Molti sostengono che nel campo della cyber-security la formazione è importante, magari con contratti milionari per formare i dipendenti delle grandi aziende. Ma abbiamo notato un livello culturale nel settore informatico veramente scadente in tutta la popolazione.

Avvocati e economisti che hanno lo smartphone e non sanno come funziona un computer nelle sue fasi basilari, cioè che per formare un carattere ci sono 8 bit di cui ognuno attiva la successiva potenza di due, partendo da destra. E'come parlare di grattacieli senza sapere che il cemento armato ha tondini di ferro dentro che lo sostengono.

Noi riteniamo che la formazione nel settore sia importante ma che deve essere estesa a tutti, nella maniera più universale ed economica possibile. Abbiamo ricevuto il manuale COMPTIA per la certificazione nel campo della sicurezza dalla società americana NETWRIX . Visionato il testo abbiamo deciso di tradurlo perché costituisce una buona base per CAPIRE il mondo informatico che ci circonda. COMPTIA riassume le conoscenze comuni del mondo della informatica e della cyber-security. Noi di ROBIONICA siamo andati avanti rispetto a queste conoscenze, abbiamo software e brevetti innovativi, quindi, in alcuni capitoli appendiamo un nostro commento che evidenziamo in maiuscolo per distinguerlo dal contesto.

Se poi qualcuno volesse conseguire la certificazione per la sua carriera, in fondo mettiamo il link al testo originale in inglese. Nella traduzione abbiamo lasciato l'intestazione dei paragrafi in inglese per agevolare lo studio. Ringrazio Elga Sansone che ha tradotto in italiano dal Googoliano. Siccome i nostri prodotti si basano sulla crittografia inespugnabile dei nodstri brevetti, in questo documento anticipiamo il dominio 6, sulla crittografia, con i nostri adeguati commenti

Questo testo si rivolge a tutti. Certe cose sono piu' difficili, ma vorrei alzare il livello di conoscenze, sia per favorire la cultura della sicurezza, sia per aiutare chi si affida a fornitori software e hardware che spiegano qualcosa del problema, ma troppo poco. Molto spesso si acquistano prodotti di informatica con scarse conoscenze e si sbaglia o si viene abilmente fregati.

Facendo un paragone, se dovete guidare una auto nuova, ma non leggete tutte le istruzioni, partite e le marce riuscite a metterle, poi i fari non sapete come accenderli, i fendinebbia e lo sbrinatore restano oscuri, e tanti altri comandi che ogni auto ha in modo diverso. Ma avete fretta e partite co stesso, con un grande rischio per voi e per gli altri. Questo succede nel campo della informatica e nel campo della sicurezza informatica. Guidate una azienda e non sapete diverse cose importanti. Il manuale

dell'autovettura in questo caso è proprio questo documento. Leggetelo e rileggetelo, i concetti vi devono essere chiari.

Riteniamo che ogni azienda di piu' di 10 persone deve avere una persona che approfondisca queste conoscenze fino ad ottenere la certificazione, cosa che aumenterebbe il suo skill e ridurrebbe la possibilità di attacco alla Azienda.

Per aziende più piccole lo stesso titolare deve studiare, nel nostro testo in italiano, magari se ha un figlio studente indurlo ad ottenere la certificazione.

Fare finta di non capire risulta deleterio per se e per gli altri, e come nel coronavirus ognuno ha la responsabilità di danneggiare gli altri.

Certe cose sono descritte per strutture grandi, ma deve essere capito il concetto, poi l'implementazione per micro-imprese può essere semplificata.

Sommario.

Dominio 1 Threats, Attacks and Vulnerabilities

Dato uno scenario, analizzare l'indicatore compromesso e
determinare il tipo di malware
Confronta e contrapponi i tipi di attacchi
Spiegare i tipi e gli attributi dell'attore di minaccia
Spiegare i concetti dei test di penetrazione
Spiegare i concetti di scansione delle vulnerabilità
Spiegare l'impatto associato ai tipi di vulnerabilità

Dominio 2 Technologies and Tools

Installa e configura componenti di rete, sia hardware che software, per supportare la sicurezza dell'organizzazione
Dato uno scenario, utilizzare strumenti software appropriati per valutare
la posizione di sicurezza di un'organizzazione
Dato uno scenario, risolvere i problemi di sicurezza comuni
Dato uno scenario, analizzare e interpretare l'output dalla sicurezza
tecnologie
Dato uno scenario, distribuire i dispositivi mobili in modo sicuro
Dato uno scenario, implementare protocolli sicuri

Dominio 3 Architecture and Design

Installa e configura componenti di rete, sia hardware che software, per supportare la sicurezza dell'organizzazione

Dato uno scenario, utilizzare strumenti software appropriati per valutare la posizione di sicurezza di un'organizzazione
Dato uno scenario, risolvere i problemi di sicurezza comuni
Dato uno scenario, analizzare e interpretare l'output dalla sicurezza tecnologie
Dato uno scenario, distribuire i dispositivi mobili in modo sicuro
Dato uno scenario, implementare protocolli sicuri

Dominio 4 Identity and Access Management

Dominio 5 Risk Management

Spiegare l'importanza delle politiche, dei piani e delle procedure correlate alla sicurezza organizzativa
Riassumi i concetti di analisi dell'impatto sul business
Spiegare i processi e i concetti di gestione dei rischi
Dato uno scenario, seguire le procedure di risposta agli incidenti
Riassumi i concetti di base di medicina legale
Spiegare il ripristino di emergenza e la continuità dei concetti operativi
Confronta e contrapponi vari tipi di controlli
Dato uno scenario, attuare pratiche di sicurezza e privacy dei dati

Dominio 6 Cryptography and PKI

Confronta e contrapponi i concetti di base della crittografia
Spiegare gli algoritmi di crittografia e le loro caratteristiche di base
Dato uno scenario, installa e configura le impostazioni di sicurezza wireless
Dato uno scenario, implementare l'infrastruttura a chiave pubblica

Gestione del rischio
Crittografia e PKI

Domande

Guida allo studio Domande per CompTIA Security +
Esame di certificazione

Introduction to certification exam

Nel testo originale in inglese ci sono le istruzioni per tentare di passare l’esame,

qui non le riportiamo perché riteniamo distraggano dallo studio, il nostro testo è rivolto a tutti, chi sosterrà l’esame sarà 1 % dei lettiri.

SICCOME INTEGRIAMO IL TESTO CON DESCRIZIONE DEI NOSTRI PRODOTTI CHE SUPERANO LE CONOSCENZE COMUNI BEN DESCRIITE IN QUESTO DOCUMENTO, PARTIAMO DAL DOMINIO 6 CHE PARLA DI CRITTOGRAFIA, DOVE NOI DI ROBIONICA SIAMO ALL'AVANGUARDI

Dominio 6. Cryptography and PKI

Compare and contrast basic concepts of cryptography. La maggior parte delle modalità di crittografia crittografano i dati un blocco di informazioni alla volta. Ci sono metodi o modalità di funzionamento per come le modalità di crittografia eseguono la crittografia.
Modes of operation . Lo scopo delle modalità operative di cifratura consistono nel mascherare i modelli esistenti nei dati crittografati.

Symmetric algorithms. Gli algoritmi a chiave simmetrica, chiamati anche crittografia a chiave privata, si basano su un segreto condiviso o chiave crittografica. Tutte le parti che partecipano a una comunicazione dispongono di una copia del documento chiave condivisa e la utilizzano per crittografare e decrittografare i messaggi: il mittente crittografa il messaggio con la chiave condivisa e il destinatario decodifica il messaggio con la chiave condivisa. La crittografia simmetrica è molto difficile da interrompere quando si utilizzano chiavi di grandi dimensioni. È principalmente usato per eseguire la crittografia di massa.
L'ALGORITMO DEL SOFTWARE CRIPTEOS 3001 E' UNA CRITTOGRAFIA A CHIAVE SIMMETRICA HA UNA DOPPIA CHIAVE DI 128 K OVVERO 131072 CARATTERI

Asymmetric algorithms. Gli algoritmi a chiave asimmetrica, noti anche come algoritmi a chiave pubblica, si basano su una chiave pubblica e a chiave privata. Tutte le parti che partecipano a una comunicazione possiedono una copia della chiave pubblica ma solo una parte possiede la chiave privata. Ciò fornisce una soluzione ai punti deboli della crittografia della chiave simmetrica poiché le chiavi devono essere utilizzate in tandem per crittografare e decifrare. Ad esempio, se la chiave pubblica crittografa un messaggio, solo la corrispondente chiave privata può decrittografare il messaggio e viceversa.
Il SISTEMA A CHIAVE PUBBLICA SI BASA SULLE PROPRIETA' DEI NUMERI PRIMI. BASE DELL'ALGORITMO E' LA GENERAZIO NE DI NUMERI CASUALI. MA IN INFORMATICA I NUMERI CASUALI NON

ESISTONO, I NUMERI CASUALI VENGONO GENERATI DA UN ALGORITMO. GIA' NEL 2012 RICERCATORI AVEVANO INDIVIDUATO L'ALGORITMO GENERATORE DEI NUMERI E DECRITTATO IL 5% DELLE CHIAVI (repubblica 15-02-2012)

Hashing. Un algoritmo di hashing è un algoritmo matematico che mappa dati di dimensioni arbitrarie su un hash di dimensioni fisse. Lo scopo è quello di essere una funzione a senso unico, impossibile da invertire. In effetti, la chiave pubblica utilizzata nella crittografia asimmetrica si basa su un valore hash: il valore viene calcolato da un numero di input di base usando un algoritmo di hashing.
L'ALGORITMO DI HASH CRTTOGRAFA MA NON DECRIPTA

Salt. Un salt è un dato casuale che viene utilizzato come input aggiuntivo per una funzione unidirezionale che esegue l'hashing dati. I caratteri casuali vengono concatenati all'inizio di una password prima dell'elaborazione. Questo è comunemente pensato per salvaguardare password o passphrase in memoria e aiuta a proteggere dal dizionario e altri attacchi pre-calcolo.

Nonce. Un nonce sono bit di dati o un numero casuale che vengono utilizzati una sola volta come input aggiuntivo per comunicazione crittografica. È comunemente usato nei protocolli di autenticazione per garantire che le vecchie comunicazioni non possono essere riutilizzate negli attacchi replay.

IV. Un vettore di inizializzazione (IV) è simile a un nonce, tranne per il fatto che il numero casuale deve essere selezionato in modo imprevedibile. In altre parole, il IV deve essere veramente casuale e non sequenziale. La randomizzazione è cruciale per gli schemi di crittografia per raggiungere la sicurezza semantica.

Elliptic curve. Un algoritmo a curva ellittica (ECC) fa affidamento sulla struttura algebrica delle curve ellittiche su campi finiti. Di conseguenza, ECC richiede chiavi più piccole rispetto ad altre crittografie per fornire sicurezza equivalente. Ad esempio, una chiave RSA a 1.024 bit è crittograficamente equivalente a chiave per sistema crittografico a curva ellittica a 160 bit.
RICORDIAMO CHE 1.024 BIT SONO 128 CARATTERI (BYTE)

Weak/deprecated algorithms. Gli algoritmi di crittografia si basano su formule matematiche. Man mano che i computer diventano più intelligenti e più veloci, gli algoritmi diventano più deboli, risultando in ambienti meno sicuri.

ECCO EL CAPITAIN , SUPERCOMPUTER EXASCALE CON CPU ZEN4 DI NUOVA GENERAZIONE. IL SUPERCOMPUTER ARRIVERA' NEL 2023 E OFFRIRA' UNA POTENZA DI OLTRE 2 EXAFLOP NEI CALCOLI NUMERICI. RICORDIAMO CHE UN EXAFLOP VALE 10 ELEVATO ALLA 18.

IL FATTO E' CHE UN COMPUTER COSI' VELOCE, CHE ESEGUE 1.000.000.000.000.000.000 OPERAZIONI AL SECONDO METTERA' IN CRISI TUTTI GLI ALGORITMI DI CRITTOGRAFIA COL SUA ATTACCO DI FORZA BRUTA (BRUTE FORCE), TRANNE IL NOSTRO CRIPTEOS 3001, DOVE LO SPAZIO DELLE CHIAVI E' ESTREMAMENTE PIU' IMMENSO, ABBIAMO 256 ELEVATO ALLA 131.072 (128 KB) . DIVIDENDO PER L'ESPONENTE 18 ABBIAMO 256 ELEVATO ALLA 131.054 . UN NUMERO SEMPRE ESTREMAMENTE IMMENSO.

Pertanto, gli algoritmi sono obsoleti e sostituiti con algoritmi più sofisticati. Per ambienti che utilizzano sistemi crittografici simmetrici, le parti precedentemente non correlate si trovano ad affrontare sfide sostanziali quando si tenta di scambiare la chiave privata per proteggere la comunicazione.
QUESTO E' UN FALSO PROBLEMA . BASTA INVIARE LA CHIAVE FUORI DALLE RETE INTERNET

Key Exchange. D'altra parte, lo scambio di chiavi per crittografia asimmetrica (o chiave pubblica) supporta comunicazioni sicure in tutto il mondo tra parti che potrebbero non conoscersi prima della comunicazione. In effetti, gli algoritmi asimmetrici offrono un comodo scambio di chiavi meccanismi e sono facilmente scalabili.
IL MECCANISMO A CHIAVE PUBBLICA SERVE SOLO PER TRASFERIRE LA CHIAVE PRIVATA, CHE E' PIU' VELOCE NELLA CRITTOGRAFAZIONE

Digital signatures. Dopo aver scelto un algoritmo di hash crittografico, un'organizzazione può implementare un sistema digitale di firma che utilizza algoritmi di firma digitale per fornire la prova che un messaggio proviene da un mittente particolare e per garantire che il messaggio non sia stato modificato mentre in transito tra il mittente e il destinatario. Gli algoritmi di firma digitale si basano su una combinazione di crittografia a chiave pubblica e funzioni di hashing.

LA NECESSITA' DELLA FIRMA DIGITALE TESTIMONIA LA SOSTANZIALE DEBOLEZZA DEL SISTEMA A CHIAVE PUBBLICA

Diffusion. Una delle due operazioni su cui si basano gli algoritmi crittografici per oscurare i messaggi di testo in chiaro è la diffusione (l'altra è la confusione). La diffusione si verifica quando si cambia un testo in chiaro che provoca più modifiche sparse nel testo cifrato. Ad esempio, se un singolo bit del testo in chiaro viene modificato, quindi la metà dei bit nel testo cifrato dovrebbe cambiare e viceversa versa. Poiché un bit può avere solo due stati, quando i bit cambiano da una posizione casuale a un altro, metà dei bit avrà cambiato stato.

TECNICA DEBOLE. DA MANO A TENTATIVI DI DECODIFICA

Confusion .L'altra operazione, un altro algoritmo crittografico basato su oscuri messaggi in chiaro è la confusione. La confusione si verifica quando ogni cifra binaria (bit) del testo cifrato dipende su diverse parti della chiave, oscurando le connessioni tra i due. Questa relazione tra il testo in chiaro e la chiave è così complicato che un attaccante non può determinare la chiave semplicemente alterando il testo in chiaro e analizzando i risultati del testo cifrato.

Collision. Si verifica una collisione se due input separati producono lo stesso valore hash. Le collisioni sono rare, ma poiché le funzioni di hash hanno una lunghezza di input e una lunghezza di output predefinite, inevitabilmente due diversi input alla fine produrranno lo stesso output di hash.

IL CONCETTO SAREBBE BUONO, MA LA TECNICA HASH HA DEI LIMITI STRUTTURALI

Steganography. La steganografia è l'arte di usare tecniche crittografiche per incorporare messaggi segreti all'interno di un altro messaggio. Gli algoritmi steganografici si basano sull'apportare modifiche al minimo, frammenti significativi di file immagine. In effetti, i cambiamenti sono così piccoli che non c'è un minimo effetto di cambiamento sull'immagine visualizzata. Ad esempio, un'organizzazione può utilizzare la steganografia per aggiungere filigrane digitali ai documenti per proteggere la proprietà intellettuale.

Obfuscation. L'offuscamento tenta di nascondere i dati in testo semplice o senza l'uso della crittografia. Ad esempio, è possibile utilizzare un metodo di sostituzione delle lettere in cui ogni lettera dell'alfabeto è assegnata a una

lettera diversa o a ciascuna lettera è assegnato un numero, oppure è possibile scrivere frasi indietro o parole nel modo sbagliato. Ci sono variazioni semplici e variazioni complesse. L'offuscamento non è considerato un metodo valido o sicuro per proteggere i dati ma può essere utile in scenari molto specifici quando i dati non sono sensibili e il caso d'uso richiede solo rendendo un po 'più difficile ottenere i dati.
VIENE UTILIZZATO OFFUSCAMENTO NEI LINGUAGGI DI PROGRAMMAZIONE DI 4 GENERAZIONE DOVE E' POSSIBILE RICAVARE IL CODICE SORGENTE DALL'ESEGUIBILE CON LA DECOMPILAZIONE

Stream cipher. Un codice di flusso è un algoritmo che crittografa un bit, o carattere, di un messaggio in chiaro in un momento. Sebbene il codice di flusso utilizzi un flusso infnite di bit pseudo-casuali come chiave, la randomizzazione dovrebbe essere imprevedibile e la chiave non dovrebbe mai essere riutilizzata.

Block cipher. Un codice a blocchi è un algoritmo che crittografa una dimensione fissa di dati (blocco) in un messaggio di testo normale; in genere, ciascun blocco è 64 bit, 128 bit o 256 bit. Il riempimento viene utilizzato negli scenari in cui i bit di testo in chiaro sono più brevi della dimensione del blocco. La maggior parte delle cifre simmetriche utilizzate oggi sono cifrari a blocchi.

L'ALGORITMO DI CRIPTEOS 3001 E' UN CODICE A BLOCCHI IN CUI I BLOCCHI SONO MOLTO GRANDI. QUESTO COMPORTA UNA ELEVATISSIMA VELOCITA' DI CRITTOGRAFAZIONE E DECODIFICA: TEST SU UN PC DI SCARSE PRESTAZIONI HANNO PORTATO A CRITTOGRAFARE MEZZO MILIARDO DI CARATTERI IN 80 SECONDI

Key strength . La lunghezza della chiave (o dimensione della chiave) è il numero di bit in una chiave utilizzata da un algoritmo crittografico.
La maggior parte degli algoritmi a chiave simmetrica sono progettati per avere una sicurezza pari alla loro lunghezza della chiave. Questo è perché la lunghezza della chiave definisce il limite superiore per la sicurezza di un algoritmo - una misura dell'attacco più veloce conosciuto contro un algoritmo basato sulla lunghezza della chiave.

RICORDIAMO CHE LE CHIAVI DI CRIPTEOS 3001 SONO DI 131072 CARATTERI

Session keys.Una chiave di sessione è una chiave simmetrica monouso generata casualmente per crittografare e decrittografare una sessione di comunicazioni sicure.

Ephemeral key. A differenza di una chiave statica, una chiave effimera è una chiave crittografica di breve durata utilizzata in processo di istituzione chiave. Di solito non sono direttamente affidabili in quanto sono generati su fly.

Secretalgorithm. Un algoritmo a chiave segreta (o algoritmo a chiave simmetrica) è un algoritmo crittografico che utilizza la stessa chiave crittografica per crittografare il testo in chiaro e decrittografare il testo cifrato.
ANCHE ALGORITMO DI CRIPTEOS 3001 E' A CHIAVE SEGRETA

Data in transit. I dati in transito o i dati in movimento si riferiscono a dati che si spostano attivamente da una posizione all'altra. Ciò include i dati trasmessi su una rete privata o su Internet.

Data at rest. I dati a riposo si riferiscono ai dati memorizzati su supporti quali dischi rigidi, unità USB esterne, backup nastri, ecc.

Data in use. I dati in uso si riferiscono ai dati che vengono elaborati (generati, aggiornati, aggiunti o cancellati) da un'applicazione. Ad esempio, potrebbero trattarsi di dati nella memoria di sistema o nella memoria temporanea buffers.

Random/pseudorandom number generation. La generazione di numeri casuali è possibile con generatori di numeri casuali hardware, ma sono molto lenti. D'altra parte, la generazione di numeri pseudo-casuali utilizza un algoritmo e un valore iniziale per generare una sequenza di numeri casuali a una velocità molto maggiore.
MENTRE LA GENERAZIONE DI NUMERI PSEUDO CASUALI HA MESSO IN CRISI L'ALGORITMO A CHIAVE PUBBLICA, NEL CASO DELLA GENERAZIONE DELLE CHIAVI PER CRIPTEOS 3001 IL FATTO CHE VI SIA UN ALGORITMO SOFTWARE PSEUDO CASUALE NON INFICIA IL FUNZIONAMENTO, LA CHIAVE E' SEPARATA

DALL'ALGORITMO

Key stretching. Il Key stretching delle chiavi è una tecnica utilizzata per trasformare chiavi deboli (per esempio una chiave di dimensione troppo piccola) più sicura contro un attacco di forza bruta. Il key stretching fa questo utilizzando una funzione di generazione di chiavi per creare una chiave allungata o migliorata basata sulla chiave debole. Per esempio, rinforzare una chiave agiungendoci una stringa lunga e segreta alla chiave debole.
INVECE DEL KEY STRETCHING ROBIONICA PROPONE IL PRODOTTO KEY-LOCK, CHE CON UN ALTRO ALGORITMO RADDOPPIA LA LUNGHEZZA DELLA CHIAVE E LA CRITTOGRAFA SUL DISCO FISSO, MENTRE LA CHIAVE CHE CI SI RICORDA APPARE SOLO SUL MONITOR DEL PC

Implementation vs algorithm selection . L'implementazione è l'atto di implementazione della crittografia, mentre la selezione dell'algoritmo è il processo di scelta dell'algoritmo giusto per la tua implementazione.

Common use cases
Perfect forward secrecy . Il segreto diretto perfetto è un protocollo che utilizza una chiave privata unica, a breve termine per ciascuno sessione sicura. Questa funzionalità garantisce che, anche se una chiave di sessione privata è compromessa, il contenuto esposto sarà limitato alla sola sessione.
QUESTA SICUREZZA NON E' NECESSARIA CON CRIPTEOS 3001

Security through obscurity .La sicurezza attraverso l'oscurità è l'atto di nascondere qualcosa che non è sicuro, invece di proteggerlo. Ad esempio, immagina di avere una console di gestione per configurare un database. Invece di costringere gli amministratori ad autenticarsi, gli dai un lungo URL che è difficile ricordare. Mentre la sicurezza attraverso l'oscurità può impedire agli utenti malintenzionati inesperti dal trovare qualcosa che non vuoi che trovino, è considerato inefficace e in genere non viene utilizzato in ambienti ad alta sicurezza.

Cryptographic service provider. Un provider di servizi crittografici (CSP) è un software libreria che fornisce servizi di crittografia e decrittazione basati su software o hardware. Ad esempio, un'applicazione potrebbe utilizzare un CSP per implementare l'autenticazione utente avanzata.

Cryptographic module. Un modulo crittografico è l'hardware o il software che esegue operazioni crittografiche all'interno di un limite fisico o logico. Il modulo potrebbe eseguire funzioni come crittografia, decrittografia, firme digitali, tecniche di autenticazione e generazione di numeri casuali.

Low-power devices. I dispositivi a bassa potenza o bassa energia hanno un'energia significativamente inferiore capacità di utilizzo e archiviazione rispetto a molti altri dispositivi standard. Di conseguenza, le organizzazioni sono costrette a utilizzare la crittografia leggera per proteggere questi dispositivi.

Low latency. Il tempo di elaborazione richiesto da un algoritmo crittografico può essere significativo. Mentre la crittografia a bassa latenza è una proprietà importante per i dispositivi standard, lo è significativamente più importante per i dispositivi a bassa potenza.
L'ALGORITMO DI CRIPTEOS 3001 E' ESTREMAMENTE VELOCE: TECNICI DEL SETTORE HANNO PARAGONATO LA SUA VELOCITA' DI CODIFICA A QUELLA DEGLI HACKER
Supporting confdentiality. Considerato uno dei principali obiettivi dei cryptosystems, la riservatezza garantisce che le informazioni o le comunicazioni siano mantenute private. Lo fa in tre diversi scenari: quando i dati sono a riposo, quando i dati sono in transito e quando i dati sono in uso.

Supporting integrity. L'integrità nella crittografia garantisce che i dati non vengano modificati senza autorizzazione. Ad esempio, l'integrità garantisce che i dati memorizzati non siano stati alterati tra l'ora in cui è stata creata e l'ora in cui è stato effettuato l'accesso. Allo stesso modo, il destinatario di un messaggio può essere certo che il messaggio ricevuto è identico al messaggio inviato dal mittente.

Supporting obfuscation. L'offuscamento è valido solo in ambienti a bassa sicurezza dove le minacce sono piccole e gli impatti sono bassi. Ad esempio, gli insegnanti potrebbero conservare i pass per le sale in una cartella etichettata "Carta bianca" per impedire ai bambini di trovarli facilmente.

Supporting authentication. Considerata una delle principali funzioni dei cryptosystems, l'autenticazione verifica l'identità dichiarata degli utenti del sistema.

Supporting non-repudiation. Fornito solo da sistemi crittografici a chiave pubblica (o asimmetrici), la non ripudio garantisce al destinatario che il messaggio è stato originato dal mittente. Impedisce al mittente di dichiarare di non aver inviato il messaggio (noto anche come ripudiare il messaggio).

Resource vs security constraints. Un vincolo di risorse è quando non hai abbastanza hardware o software per eseguire un'attività in un determinato periodo di tempo. Potrebbe anche riguardare risorse umane, come non avere abbastanza persone per gestire i tuoi server. Sicurezza i vincoli sono diversi perché potrebbero essere limiti tecnici di una soluzione o standard o vincolo integrati nelle politiche e procedure aziendali.

High resiliency. Quando si progetta una soluzione che garantisce operazioni continue anche se alcuni componenti falliscono, si progetta una soluzione altamente resiliente. L'alta resilienza si ottiene spesso con hardware aggiuntivo, software aggiuntivo e controlli di sicurezza.

DES. Il Data Encryption Standard (DES) è un algoritmo di crittografia a blocchi standard progettato presso IBM utilizzato da molti altri algoritmi. A causa della dimensione della chiave relativamente piccola (56 bit), DES è ora considerato insicuro.

AES. Advanced Encryption Standard (AES) è uno degli algoritmi di crittografia simmetrica più popolari. NIST lo ha selezionato come sostituto standard per DES nel 2001. AES ha sede sulla cifra di Rijndael ed è stato implementato in molti altri algoritmi e protocolli. Ad esempio, Microsoft BitLocker e Microsoft Encrypting File System (EFS) usa AES. Inoltre, la maggior parte dei produttori di CPU include il supporto hardware AES e gli Stati Uniti il governo ha approvato il suo utilizzo per proteggere i dati classificati. AES supporta dimensioni chiave di 128 bit, 192 bit e 256 bit.

STUDI HANNO DIMOSTRATO CHE DIVENTERA' A BREVE VIOLABILE CON GLI ATTACCHI DI FORZA BLUTA (BRUTE FORCE)

DOVE SI PROVANO TUTTE LE CHIAVI POSSIBILI FINO A TROVARE QUELLA CHE FUNZIONA

Explain cryptography algorithms and their basic characteristics . Il progetto d'esame richiama algoritmi specifici: studiali e non concentrarti sugli algoritmi non elencati. Sebbene non sia male avere familiarità con gli altri, rimanere concentrati sugli algoritmi e sulle modalità di cifratura in questa sezione.

Symmetric algorithms

3DES. Il triplo DES (3DES) è stato creato come possibile sostituto di DES. Triple DES applica l'algoritmo DES tre volte e ha una sicurezza pratica migliore rispetto a DES. Mentre il primo il design utilizza chiavi a 56 bit, le implementazioni più recenti utilizzano chiavi a 112 o 168 bit. Triple DES è utilizzato in molte carte di pagamento intelligenti.
ANCHE QUESTO E' MOLTO DEBOLE RISPETTO A CRIPTEOS 3001

RC4. L'algoritmo Rivest Cipher 4 o Ron's Code 4 (RC4) è un codice di flusso che esegue bene per la sua velocità e semplicità. Mentre RC4 è buono se la chiave non viene mai riutilizzata, è considerato insicuro da molti esperti di sicurezza.
CONSIDERATO INSICURO

Blowfsh. L'algoritmo Blowfsh è un codice a blocchi sviluppato anche come alternativa a DES. Poiché Blowfsh può utilizzare dimensioni di chiave variabili che vanno da 32 bit a 448 bit, è considerato un protocollo di crittografia avanzato. In effetti, l'applicazione bcrypt nei sistemi Linux utilizza Blowfsh per crittografare le password per proteggersi dagli attacchi delle tabelle arcobaleno (vedere di più su bcrypt più avanti in questo capitolo). Le tabelle Rainbow sono tabelle pre-calcolate che abbinano hash crittografici a una stringa di testo semplice. Sono spesso usati per decifrare le password in modo efficace.
COME SI VEDE, LA COMPLICAZIONE DELLE PASSWORD CON AGGIUNTA DI CODICI DI HASH HA LA CONTROPARTITA CHE ESISTONO TABELLE PER DECODIFICARE LA PASSWORD.
TUTTA LA CRITTOGRAFIA BASATA SU CODICI HASH E' DEBOLE.

CRIPTEOS 3001 HA UN ALGORITMO CHE NON SI BASA SUI CODICI HASH NELLA GENERAZIONE DELLE CHIAVI

Twofsh. Simile a Blowfsh, l'algoritmo Twofsh è un codice a blocchi sviluppato in alternativa a AES. Twofsh utilizza una dimensione della chiave di 128 bit, 192 bit o 256 bit. È stato progettato per essere più flessibile di Blowfsh supportando hardware aggiuntivo e utilizza due tecniche non presenti in altri algoritmi: pre-sbiancamento e post-sbiancamento.
256 BIT SONO 32 CARATTERI

CBC. Cipher Block Chaining (CBC) è una modalità operativa di cifratura a blocchi che crittografa i dati come un intero blocco. Durante la crittografia, CBC incatenerà ogni blocco di testo in chiaro con il precedente blocco di testo cifrato. Di conseguenza, la decrittazione di un blocco di testo cifrato dipende su tutti i blocchi di testo di cifratura precedenti. Un errore a bit singolo in un blocco di testo cifrato colpisce la decrittazione di tutti i blocchi successivi. Tenta di riorganizzare l'ordine del testo cifrato i blocchi causano corruzione durante la decrittazione.
COME VISTO HA DEI PROBLEMI

GCM. Galois / Counter Mode (GCM) è una modalità di funzionamento con cifratura a blocchi che utilizza l'hash su un campo binario di Galois per fornire autenticità (integrità) e riservatezza dei dati.
GCM è stato ampiamente adottato per la sua efficacia e prestazioni nell'hardware e implementazioni software.
ANCHE IN QUESTO CASO E' FIGLIO DELLA TECNICA HASH

ECB. Electronic Codebook (ECB) è una modalità operativa di cifratura a blocchi che divide i messaggi in blocchi e crittografa ogni blocco separatamente. La più semplice delle modalità di crittografia, una caratteristica chiave della BCE è che ogni possibile blocco di testo in chiaro ha un valore di testo cifrato corrispondente difeso e viceversa. In altre parole, la BCE esegue la crittografia identica, blocchi di testo in chiaro in blocchi di testo cifrati identici e non nasconde bene i modelli di dati.A causa di questa mancanza di diffusione, gli esperti di sicurezza non raccomandano l'uso della BCE nei protocolli crittografici.
COME VISTO HA DEI PROBLEMI

CTR. Counter (CTR) è una modalità di funzionamento che consente al cifrario a blocchi di funzionare come un codice di flusso. Il CTR genera bit di flusso di chiavi indipendentemente dai dati di crittografia contenuto del blocco. Lo fa crittografando i valori successivi di un contatore, che producono una sequenza che non dovrebbe mai ripetersi.

Cipher modes

Stream vs block. Mentre sia le cifrature di flusso che quelle di blocco sono cifrature simmetriche, le cifrature di flusso si basano sulla generazione di un flusso di chiavi crittografico infnito mediante la crittografia di uno po 'alla volta. D'altra parte, i cifrari a blocchi crittografano un blocco alla volta, combinando blocchi per una maggiore sicurezza. I cifrari a blocchi in genere richiedono più memoria perché crittografare blocchi di dati più grandi e utilizzerà anche i dati dei blocchi precedenti;
COSA CHE NON SUCCEDE CON CRIPTEOS3001

Stream . Le cifrature di flusso hanno meno requisiti di memoria perché crittografano un numero minimo di bit e sarà in genere molto più veloce delle cifre a blocchi.
Sebbene le cifrature di flusso siano più difficili da implementare, le cifrature a blocchi sono più suscettibili al rumore nella trasmissione – a l'errore in una parte dei dati farà sì che il resto dei dati sia irrecuperabile.
COSA CHE NON SUCCEDE CON CRIPTEOS3001
Infine, i codici di flusso non forniscono protezione o autenticazione dell'integrità, mentre alcuni blocchi le cifre forniscono protezione di integrità e riservatezza. In genere, i migliori casi d'uso per le cifre di flusso sono scenari in cui la quantità di dati è sconosciuta o continua (ad es. flussi di rete). In alternativa, i cifrari a blocchi sono più utili quando la quantità di dati sono noti in anticipo (ad esempio, un file o campi di dati).
USO PARTICOLARE SUI FLUSSI DI RETE. DATA LA VELOCITA' DI CRIPTEOS 3001 POTREBBE ESSERE STUDIATA UNA SOLUZIONE ANCHE PER FLUSSI DI RETE

RSA. L'algoritmo RSA (Rivest – Shamir – Adleman) è uno dei primi cryptosystems a chiave pubblica. Basato su un algoritmo asimmetrico, RSA pubblica una chiave pubblica che si basa su due grandi numeri primi. Mentre chiunque può utilizzare la chiave pubblica per crittografare un messaggio, solo

qualcuno con conoscenza dei numeri primi può decifrare il messaggio. Dal momento che RSA è un algoritmo relativamente lento, è meno comunemente usato per crittografare direttamente i dati dell'utente. D'altra parte, RSA viene comunemente utilizzato per la trasmissione sicura dei dati crittografando un file condiviso, chiave simmetrica che viene quindi utilizzata per eseguire la crittografia / decrittografia di massa in modo molto più veloce velocità.
IL LORO MODO PIU' VELOCE E' MOLTO LENTO RISPETTO A CRIPTEOS3001
DSA. Il Digital Signature Algorithm (DSA) è considerato uno standard per le firme digitali. La firma digitale fornisce autenticazione, integrità e non ripudio dei messaggi. DSA crea la firma digitale utilizzando funzioni matematiche uniche che coinvolgono due numeri a 160 bit. Questi numeri provengono dai digest del messaggio (stringhe di cifre creato da una formula di hashing unidirezionale) e dalla chiave privata. Mentre i messaggi sono firmati dalla chiave privata del firmatario, la firma digitale è verificata dal corrispondente del firmatario chiave pubblica. DSA utilizza la chiave pubblica solo per l'autenticazione, non per crittografare o decrittografare i messaggi.
BASATO SU CHIAVE PUBBLICA E PRIVATA

Dife-Hellman. Lo scambio di chiavi Dife-Hellman (DH) fu uno dei primi protocolli di chiave pubbliche nel campo della crittografia. Mentre la maggior parte delle comunicazioni crittografate richiede che le parti scambiano le chiavi usando un canale sicuro, DH fornisce un metodo sicuro per scambiare chiavi crittografiche su un canale non sicuro. Questa chiave può quindi essere utilizzata per crittografare le comunicazioni successive utilizzando un codice di chiave simmetrica.
ANCHE QUI CHIAVE PUBBLICA SOLO PER TRASMETTERE CHIAVE PRIVATA
Groups. I gruppi vengono talvolta utilizzati nella crittografia per formare primitivi. Primitivi sono algoritmi di basso livello spesso usati per funzioni specifiche, come l'hash a senso unico funzioni.

Asymmetric algorithms

DHE. Dife-Hellman effimero (DHE o EDH, a seconda della suite di crittografia utilizzata)è simile a DH, ma fornisce anche segretezza in avanti usando i tasti effimeri: il DH la chiave privata è temporanea e non viene

salvata dal server. DHE è comunemente usato per crittografare sessioni di trasporto (ad es. TLS).

ECDH. Curva ellittica Dife-Hellman (ECDH) è una variante del protocollo DH che utilizza la crittografia a curva ellittica per l'accordo chiave anonima. Di conseguenza, ciascuna parte dello scambio di chiavi avrà una coppia di chiavi pubblica-privata a curva ellittica.

Elliptic Curve (ECDHE). Curva ellittica Dife-Hellman effimera (ECDHE) è una variante del protocollo DHE che utilizza la crittografia a curva ellittica per generare chiavi effimere. Come un risultato, ECDHE fornisce anche segretezza diretta.

PGP. Pretty Good Privacy (PGP) è un programma di crittografia che fornisce crittografia autenticazione e privacy. Lo fa usando una combinazione di metodologie di crittografia come hash, compressione dei dati, crittografia a chiave simmetrica e chiave pubblica crittografia. PGP può essere utilizzato per firmare, crittografare / decrittografare file di testo, e-mail, file, directory e partizioni del disco. PGP è di proprietà e gestito da Symantec Corp.
CARINO, MA GLI INGREDIENTI DEL SUO MENU' SONO FUNZIONI DI HASH, CHITTOGRAFIA A CHIAVE PUBBLICA, DI CUI ABBIAMO VISTO I DIFETTI

GPG. GNU Privacy Guard (GnuPG, GnuPGP o semplicemente GPG) è non proprietario, gratuitoversione di PGP. GPG si basa sugli standard OpenPGP stabiliti dall'IETF. Inoltre, GPG prevede di integrarlo nella posta elettronica e nei sistemi operativi come Linux.
VERSIONE GRATUITA DEL PRECEDENTE

Hashing algorithms. Esistono vari algoritmi di hash crittografici che possono essere utilizzati per produrre un valore di checksum. Un valore di checksum è un piccolo pezzo di dati derivati dai dati da proteggere. Lo scopo principale del checksum è convalidare l'autenticità dei dati (ad esempio, che non è stato modificato).

MD5. L'algoritmo Message-Digest 5 (MD5) è uno dei due algoritmi di hashing più utilizzati. La funzione accetta un input di lunghezza arbitraria e produce un messaggio digest che è lungo 128 bit (ovvero un valore di hash a 128 bit), in

genere visualizzato come un numero esadecimale a 32 cifre. È noto che MD5 provoca collisioni (ovvero due messaggi distinti l'hash con lo stesso valore). Tuttavia, può ancora essere utilizzato come checksum per verificare i dati integrità, come la verifica della corruzione involontaria o la determinazione della partizione per a chiave particolare in un database partizionato.
NEGLI ALGORITMI DI HASH NON E' GARANTITO CHE DA UN INPUT ESCA UN OUTPUT UNICO, CON LA COLLISIONE DUE INPUT HANNO LO STESSO OUTPUT DI HASH

SHA. L'altro uno dei due algoritmi di hashing più utilizzati, Secure Hash Algorithm (SHA) è lo standard comune utilizzato per la creazione di firme digitali. SHA era sviluppato dalla NSA. SHA-1 accetta un input e produce un valore hash a 160 bit, in genere reso come un numero esadecimale di 40 cifre. SHA-2 può produrre valori hash che sono 224, 256, 384 o 512 bit.
FIRME DIGITALI. SEMPRE HASH …

Bcrypt. Bcrypt è una funzione di hashing della password basata sul codice a blocchi Blowfsh. Bcrypt incorpora un rinforzo per proteggersi dagli attacchi dei tavoli arcobaleno. Inoltre, bcrypt si adatta nel tempo aumentando il contatore iterativo che gli consente di resistere agli attacchi bruteforce. Bcrypt è l'algoritmo hash di password predefinito su molti Unix e Linux sistemi per proteggere le password archiviate nel file delle password shadow.

PBKDF2. La funzione 2 di derivazione delle chiavi basata su password (PBKDF2) aiuta a ridurre la vulnerabilità delle chiavi crittografate agli attacchi di forza bruta. PBKDF2 applica una funzione HMAC a una password e valore salt più volte per produrre una chiave derivata. Usando il tasto come una chiave crittografica nelle operazioni successive rende il crack delle password molto più diffcile. Numerosi algoritmi e sistemi, come WPA2, Apple iOS e Cisco operativisistemi, utilizzare PBKDF2 per aumentare la sicurezza delle password.
PARTENDO DA UNA COSA INSICURA COME LE PASSWORD SI ARRANGIANO A TENTARE DI RENDERLE SICURE

HMAC. Il codice di autenticazione dei messaggi basato su hash (HMAC) è un tipo di codice di autenticazione dei messaggi (MAC) che verifica sia l'integrità dei dati sia l'autenticazione di un messaggio. Poiché HMAC utilizza due

passaggi di calcolo dell'hash, l'algoritmo fornisce risultati migliori immunità contro gli attacchi di estensione della lunghezza.

RIPEMD.È stato sviluppato il Digest Message Review Rest (RIPEMD) di RACE Integrity da ricercatori europei; il design si basa sull'algoritmo di hashing MD5. Uno di le versioni più recenti, RIPEMD-160, è una versione migliorata di RIPEMD. La prestazione dell'algoritmo è simile a SHA. RIPEMD è disponibile nelle versioni 128, 256 e 320 bit.
ANCHE IN QUESTO CASO CHIAVI AL MASSIMO DI 40 CARATTERI

- Key stretching algorithms.
Gli algoritmi di allungamento dei tasti aumentano la forza di memorizzazione password usando i salt. Ecco due tecniche di stretching chiave comuni:

XOR. XOR è un codice additivo comunemente usato in molti algoritmi. Un testo cifrato può essere creato applicando l'operatore XOR a tutti i personaggi usando una chiave predefinita. La decodifica del testo cifrato implica semplicemente l'applicazione dell'operatore XOR con la chiave.

ROT13. La cifra di rotazione di 13 posizioni (ROT3) è una cifra di sostituzione di lettere in cui le lettere dell'alfabeto sono o 13 set (tutte le istanze della lettera "A" sono sostituite dalla lettera "N", tutte le istanze di "B" sono sostituite da "O", ecc.). Il codice ROT13 è il codice Caesar (uno dei i primi e più semplici numeri, come la sostituzione di A con B, B con C e così via) con uno spostamento di 13.
Poiché l'alfabeto latino di base contiene 26 lettere, lo stesso algoritmo è per decodificare ROT13 applicato. Sfortunatamente, il codice può essere infranto molto facilmente, quindi non fornisce praticamente alcuna sicurezza.
IL CODICE DI CESARE ADESSO E' VIOLABILISSIMO. UTILIZZAVA UNA CIFRA DELLO SPOSTAMENTO RISPETTO ALL'ALFABETO LATINO. SE CIFRA =3 QUINDI A DIVENTAVA D.
SUCCESSIVAMENTE VENNE VIGENERE CHE FECE UNA TABELLA BIDIMENSIONALE IN CUI C'ERA UNA PAROLA CHIAVE E OGNI RIGA VEDEVA SPOSTARSI L'ALFABETO LATINO PARTENDO DALLA LETTERA DELLA PAROLA CHIAVE. SE LA PAROLA CHIAVE E' VIGENERE NELLA PRIMA RIGA L'ALFABETO PARTIVA DALLA LETTERA V , NELLA SECONDA DALLA I, NELLA TERZA DALLA G E COSI' VIA.

NEL RINASCIMENTO I CODICI VIGENERE FURONO VIOLATI DALLA ANALISI DELLE FREQUENZE, SE IL MESSAGGIO ERA PRESUNTO IN ITALIANO IL CARATTERE PIU'DIFFUSO CORRISPONDEVA ALLA E, IL SECONDO ALLA A ECC. FINO A RICOSTRUIRE L'INTERO MESSAGGIO SE ABBASTANZA LUNGO.

IL SISTEMA CRITTOGRAFICO CRIPTEOS 3001 SEGUE UNO SCHEMA SIMILE A VIGENERE DOVE PERO' LA STESSA LETTERA NON VIENE MAI TRADOTTA NELLO STESSO MODO, QUINDI NON E' DECODIFICABILE CON L'ANALISI DELLE FREQUENZE.

Substitution ciphers. I codici di sostituzione sono il tipo più comune di codice e si basano sulla sostituzione di ogni lettera del testo in chiaro, inclusi segni di punteggiatura e spazi, con un'altra lettera o un simbolo casuale. In contrasto con un ROT13 o un altro codice Cesare, l'alfabeto in un codice di sostituzione è completamente confuso e non semplicemente l'alfabeto è cambiato. Esistono varie forme di cifre di sostituzione che sostituiscono singole lettere, gruppi di lettere, l'intero messaggio o varie sostituzioni in diverse posizioni nel messaggio.
L'ALGORITMO DI CRIPTEOS 3001 E' UN CODICE DI SOSTITUZIONE ESTREMAMENTE SICURO EFFICACE E VELOCE.

Obfuscation. L'offuscamento è l'arte di nascondere o oscurare qualcosa.

WPA. Il protocollo WPA (Wi-Fi Protected Access) protegge il traffico di rete wireless in transito implementando gran parte dello standard IEEE 802.11i. WPA utilizza il protocollo TKIP (Temporal Key Integrity Protocol) per verificare l'integrità dei pacchetti. WPA utilizza l'algoritmo di controllo dell'integrità dei messaggi TKIP per impedire a un utente malintenzionato di modificare e inviare nuovamente i pacchetti di dati. Tuttavia, gli esperti di sicurezza non raccomandano l'uso di WPA a causa dei maggiori flussi di sicurezza.
ECCONE UN ALTRO SCONSIGLIATO..

Given a scenario, install and configure wireless security settings
Questa è un'altra sezione hands-on. Ci si aspetta di avere familiarità con l'installazione dettagliata e la configurazione delle impostazioni di sicurezza wireless. Come parte della vostra preparazione esame, spendere un po' di

tempo esaminando i router wireless in aggiunta alla revisione di queste informazioni. I protocolli crittografici o protocolli di crittografia eseguono funzioni di sicurezza utilizzando algoritmi crittografici.

Cryptographic protocols

WPA2. La Wi-Fi Alliance ha sviluppato WPA2 in sostituzione di WPA. WPA2 fornisce supporto obbligatorio per CCMP, che è un protocollo di crittografia basato su AES.

WPA3. La Wi-Fi Alliance ha sviluppato WPA3 in sostituzione di WPA2. Questo nuovo standard utilizza la crittografia a 128 e 192 bit con segretezza diretta e mitigherà i problemi di sicurezza posto da password deboli.

TKIP. TKIP (Temporal Key Integrity Protocol) è un protocollo di crittografia wireless che utilizza gli standard definiti nella norma IEEE 802.11. TKIP è stato progettato per sostituire Wirelss Equivalent Privacy (WEP) senza richiedere la sostituzione di hardware legacy.
TKIP utilizza una chiave a 128 bit che genera dinamicamente per ciascun pacchetto, impedendo il tipi di attacchi che hanno compromesso WEP. Sebbene TKIP sia molto più forte di un controllo di ridondanza ciclico (CRC), non è così forte come l'algoritmo utilizzato in WPA2. In effetti, TKIP è no più considerato sicuro; è stato deprecato nella revisione del 2012 dello standard 802.11.

CCMP. Protocollo codice di autenticazione messaggio concatenamento blocco blocchi cifratura (CCMP) è un protocollo di crittografia wireless che utilizza gli standard definiti nell'IEEE Modifica 802.11i allo standard IEEE 802.11 originale. Progettato per affrontare le vulnerabilità in WEP, CCMP è un meccanismo di incapsulamento crittografico dei dati avanzato utilizzato per riservatezza, integrità e autenticazione dei dati. CCMP si basa sullo standard AES e utilizza chiavi a 128 bit e un algoritmo vettoriale di inizializzazione a 48 bit, che riduce al minimo la vulnerabilità agli attacchi di tipo replay.

EAP. Extensible Authentication Protocol (EAP) è un protocollo di autenticazione che è frequentemente utilizzato nelle reti wireless e nelle connessioni punto-punto; EAP non è utilizzato per reti cablate. EAP fornisce formati per altri protocolli per incapsulare i messaggi EAP (ad es. WPA,

WPA2, ecc.). Inoltre, EAP supporta più meccanismi di autenticazione, come ad esempio token card, smart card, certificati, password monouso e autenticazione con crittografia a chiave pubblica.

PEAP. Il protocollo PEAP (Protected Extensible Authentication Protocol) è una versione di EAP progettata per fornire un'autenticazione più sicura per le reti wireless 802.11 che supportano il controllo dell'accesso alla porta 802.1X. Lo fa incapsulando il traffico EAP all'interno di un tunnel TLS crittografato e autenticato. Ciò garantisce l'informazione di autenticazione del client nel tunnel protetto e al sicuro dalle intercettazioni.

EAP-FAST. L'autenticazione flessibile EAP tramite Secure Tunneling (EAP-FAST) è un protocollo che viene utilizzato nelle reti wireless per l'autenticazione della sessione. EAP-FAST è stato progettato per affrontare i punti deboli del protocollo LEAP (Lightweight Extensible Authentication Protocol) di esecuzione dell'autenticazione su un tunnel TLS. EAP-FAST utilizza le credenziali di accesso protetto (PAC) per stabilire il tunnel TLS per l'autenticazione. Il processo prevede tre fasi: I protocolli di autenticazione prevedono il trasferimento di dati di autenticazione tra due parti (ad es. Client e server).

Authentication protocols

Fase 0. Il PAC (segreto condiviso) viene fornito e fornito alle parti della connessione.
Fase 1. Il tunnel TLS viene creato utilizzando il PAC.
Fase 2. Le parti della connessione si scambiano le credenziali.

EAP-TLS. EAP Transport Layer Security (EAP-TLS) è un protocollo di autenticazione EAP che viene utilizzato per proteggere le comunicazioni su una rete wireless. EAP-TLS richiede lato client X.509 certifica l'autenticazione con il server, ma è considerato uno dei più standard EAP sicuri disponibili.
EAP-TTLS. EAP Transport Layer Security (EAP-TLS) è un protocollo di autenticazione EAP che viene utilizzato per proteggere le comunicazioni su una rete wireless. EAP-TLS richiede lato client X.509 certifica l'autenticazione con il server, ma è considerato uno dei più sicuri disponibili standard EAP.

IEEE 802.1x. IEEE 802.1x è uno standard IEEE per il controllo dell'accesso alla rete basato su porte (PNAC). Lo standard IEEE 802.1x definisce

l'incapsulamento del protocollo EAP. IEEE 802.1x
lo standard fornisce un framework per dispositivi su reti wireless o cablate.

PSK. Il metodo WPA-PSK, o chiave pre-condivisa, è progettato per reti domestiche o di piccole dimensioni. Sebbene questo metodo non richieda un server di autenticazione, ogni dispositivo di rete wireless crittografa il trafc di rete utilizzando una chiave di crittografia a 128 bit, che viene creata da una chiave condivisa a 256 bit. Il client deve inserire la chiave condivisa come passphrase da 8 a 63 caratteri ASCII o una stringa di 64 cifre esadecimali.

Enterprise. Il metodo WPA-Enterprise utilizza IEEE 802.1x ed è progettato per le reti aziendali. Questo metodo richiede un server di autenticazione RADIUS. Sebbene WPA-Enterprise richieda un'autenticazione di livello aziendale, il metodo fornisce ulteriore sicurezza, come la protezione dagli attacchi del dizionario su password brevi, ficcanaso e VLAN assegnato automaticamente e supporta Network Access Protection (NAP).
WPA offre vari metodi per l'autenticazione degli utenti. Questi variano in base al metodo di distribuzione delle chiavi e protocollo di crittografia.

Methods

RADIUS Federation. RADIUS (Remote User Authentication User Service) è un protocollo di rete usato frequentemente per l'autenticazione 802.1x. RADIUS fornisce autenticazione centralizzata, autorizzazione e gestione della contabilità per gli utenti che si connettono a un servizio di rete. RADIUS viene spesso utilizzato dagli ISP e dalle aziende per gestire l'accesso a Internet o alle reti interne, alle reti wireless e ad altri servizi. Ad esempio, i server di rete di accesso di solito includono un componente RADIUS che comunica con RADIUS server per consentire ai client di connettersi alla rete.

Open. Le reti aperte o i punti di accesso aperti non richiedono l'autenticazione per i client per connettersi. Sebbene questo metodo possa utilizzare la crittografia, è facilmente sfruttabile. Per questo motivo, gli esperti di sicurezza non raccomandano di implementare reti aperte a meno che non siano necessarie requisiti aziendali. Ad esempio, questo metodo è comunemente usato negli aeroporti, ad esempio negozi, hotel, centri commerciali e altre aree pubbliche.

WPS. Wi-Fi Protected Setup (WPS) è un metodo di distribuzione della chiave di autenticazione che è destinato a semplificare e rafforzare la sicurezza della rete. WPS è stato creato da Wi-Fi Alliance per consentire agli utenti domestici di configurare l'accesso protetto Wi-Fi utilizzando uno dei quattro metodi:

PIN, pulsante, comunicazione near-feld (NFC) o USB. Inoltre, il metodo consente agli utenti di aggiungere nuovi dispositivi a una rete esistente senza inserire passphrase lunghe. Tuttavia, è stato scoperto un importante difetto di sicurezza con il metodo PIN WPS che ha permesso accesso remoto degli aggressori.

Captive portal. Comunemente utilizzato nelle reti wireless aperte, un portale captive è un web pagina che mostra agli utenti un messaggio di benvenuto che li informa delle condizioni di accesso (ad es. porti consentiti, responsabilità, ecc.) e potrebbe richiedere autenticazione o pagamento. Prigioniero i portali sono comunemente implementati su hotspot Wi-Fi forniti in commercio, come ad esempio aeroporti, negozi, condomini, camere d'albergo e centri d'affari.

CA. Un'autorità di certificazione (CA) è un'entità fidata che emette certificati digitali basati su lo standard X.509. Simile ai servizi di autenticazione notarile per i certificati digitali, la CA agisce come una terza parte fidata tra il proprietario del certificato e la parte che si affida al certifcate. Ad esempio, la CA emette certificati utilizzati per proteggere le pagine Web (ad esempio HTTPS) e firma elettronica dei documenti.

Given a scenario, implement public key infrastructure

Questa sezione si concentra sui dettagli di implementazione. Preparati a ricevere uno scenario, potenzialmente con requisiti e informazioni sull'infrastruttura esistente, e devi spiegare come andare avanti con un'infrastruttura a chiave pubblica (PKI) in base ai requisiti.
Una PKI è composta da diversi componenti. Sono necessari alcuni componenti, ad esempio una CA. Altri sono opzionali, come un OCSP. Per preparare l'esame, dovresti essere in grado di distinguere tra i componenti e capire come vengono utilizzati.

Components

Intermediate CA. Una CA intermedia o subordinata è una variante della CA in quanto essa esegue il lavoro quotidiano di firma dei certificati e aggiorna le

informazioni di revoca dei certificati. Una CA root avrà spesso una o più CA intermedie ritenute affidabili dalla CA principale.

CRL. Una delle due tecniche utilizzate per verificare l'autenticità dei certificati e identificarli certificati revocati, un elenco di revoche certificati (CRL) è un elenco di certificati digitali che è stato revocato dalla CA emittente e non dovrebbe più essere considerato attendibile. Questo sarà in genere si verificano prima della data di scadenza pianificata del certificato. Simile a una lista nera, il CRL è utilizzato da vari client (ad es. browser Web) per verificare se un certificato è valido. Uno degli svantaggi dell'utilizzo di un elenco CRL è che i client devono scaricare frequentemente gli aggiornamenti mantenere un elenco corrente.

OCSP. L'altra delle due tecniche utilizzate per verificare l'autenticità dei certificati e identificare i certificati revocati, il protocollo di stato certificato online (OCSP) fornisce un meccanismo di richiesta / risposta per i clienti per ottenere lo stato di revoca di un certificato digitale. Questo vantaggio elimina la latenza inerente al mantenimento di un CRL fornendo verifica in tempo reale certificata.

CSR. Una richiesta di firma certificata (CSR) è un messaggio appositamente formattato inviato da un richiedente presso una CA al fine di richiedere un certificato digitale. Insieme alla CSR, il richiedente invierà la chiave pubblica per la quale dovrà essere rilasciato il certificato. Incluso nel CSR sono le informazioni identificative (ad es. nome di dominio, nome comune, amichevole nome, ecc.) e protezione dell'integrità (ad es. firma digitale, ecc.).

Certifcate. Un certificato X.509 è un certificato digitale utilizzato per verificare che una chiave pubblica appartenga a una particolare entità (ad esempio un utente, un computer o un servizio). Basato sulla chiave pubblica X.509 infrastruttura (PKI) standard, il certifcate contiene la versione, il numero seriale, la CA emittente, periodo di validità e altre informazioni sull'entità. Mentre la chiave pubblica in un server web certifcate viene utilizzato per crittografare il traffico sul sito, il certifcate identifica chi possiede il sito.

Public key. Uno dei due componenti di una coppia di chiavi asimmetriche, viene utilizzata una chiave pubblica da un mittente per crittografare un messaggio utilizzando la chiave pubblica del destinatario. Nelle firme digitali,

la chiave pubblica viene utilizzata dal destinatario per verificare i messaggi firmati con la chiave privata del mittente.

Private key. L'altro componente di una coppia di chiavi asimmetriche, una chiave privata viene utilizzata dal destinatario per decrittografare un messaggio che è stato crittografato utilizzando la chiave pubblica. Nelle firme digitali, la chiave privata viene utilizzata dal mittente del messaggio per firmare i messaggi. Questo dimostra al destinatario del messaggio che il messaggio non è stato modificato. Entrambe le chiavi nella coppia di chiavi
- la chiave privata e la chiave pubblica - devono essere create prima del CSR.

Object identifers (OID). Identificatori di oggetti (OID) è un meccanismo identificativo approvato dall'Unione internazionale delle telecomunicazioni (ITU), ISO / IEC e IETF per la denominazione standardizzata di qualsiasi oggetto, concetto o cosa utilizzando un nome non ambiguo e persistente espresso come un gruppo di caratteri. OID è usato per nominare quasi ogni tipo di oggetto in X.509 certifica (ad esempio componenti di nomi distinti, CPS, ecc.).

Online vs offline CA. La maggior parte delle autorità di certificazione sono online: elaborano attivamente CSR e forniscono dati per download CRL o risposte a richieste OSCP. Perché le conseguenze di una CA root compromessa è così enorme, gli esperti di sicurezza consigliano di proteggerli da accesso non autorizzato. Per questo motivo, la CA principale è isolata dall'accesso alla rete e lo è spesso tenuto in uno stato di spegnimento - una offline CA. Una CA offline non dovrebbe avere impatto su eventuali operazioni PKI se la CA principale ha delegato operazioni (ad esempio, emissione, distribuzione e revoca dei certificati digitali) a una o più CA intermedie. La CA principale è portato online solo quando richiesto per compiti poco frequenti, come l'emissione o la riemissione di certificati che autorizzano autorità di certificazione intermedie.
COMPLICATO ? BASTA USARE CRIPTEOS 3001

Stapling. La pinzatura OCSP è uno standard per il controllo dello stato di revoca di X.509 digitale certifcates. Sebbene le risposte OCSP siano molto più veloci di un download CRL, è possibile essere un ritardo minore all'avvio della connessione TLS (stretta di mano). Pinzatura OCSP elimina la necessità che un browser richieda la risposta OCSP direttamente da una CA aggiungendo una

risposta OCSP con data e ora firmata dalla CA alla stretta di mano iniziale. Questo elimina la necessità per i client di contattare la CA, poiché il server Web memorizza nella cache o pinza la risposta OCSP alla stretta di mano TLS iniziale. Di conseguenza, la pinzatura OCSP si riduce il carico di lavoro del 30% e migliora la sicurezza.

Concepts

Pinning. Il pinning con chiave pubblica è un meccanismo di sicurezza che aiuta i siti Web a prevenire la rappresentazione da parte di utenti malintenzionati che utilizzano certificati digitali fraudolenti. Il certificato di un sito Web viene in genere convalidato verificando la gerarchia delle firme, ma questa catena di fiducia può essere compromessa. Per combattere questo rischio, il server Web fornisce al client un elenco di pubblico bloccato hash chiave per un determinato periodo di tempo. In seguito a connessioni al server Web, il client si aspetta che il server utilizzi solo queste chiavi pubbliche nella sua catena certificata.

Trust model. PKI si basa su un modello di trust gerarchico che assegna a una terza parte il file responsabilità di stabilire un rapporto di fiducia tra due parti. Nella parte superiore è una fonte comunemente riconosciuta (CA principale) che tutte le parti utilizzano la fiducia PKI. In genere, sotto l'origine sono autorità subordinate (CA intermedie) che si basano sull'autorità di origine.

Key escrow. L'impegno chiave è un processo di scambio di chiavi in cui è una chiave utilizzata per decrittografare i dati tenuto in deposito a garanzia o archiviato da terzi. Solo una parte autorizzata può accedere alla chiave.
Se la chiave viene persa o compromessa, solo una parte autorizzata può accedere alla chiave per decrittografare i dati.

Certificate chaining. I certificati digitali sono verificati utilizzando catena certificata, che è un elenco ordinato di certificati in una gerarchia. La catena inizia in basso con il digitale certificato, e ogni certificato nella catena è firmato dal soggetto identificato dal successivo certificato nella catena. Qualsiasi certificato fra il certificato digitale ed il certificato della radice è denominato una catena o certifcate intermedio. La catena termina con un certificato CA radice, che è sempre firmato dalla CA stessa. Le firme di tutti i certificati nella catena sono verificate fino al certificato CA radice

Wildcard. Un certificato jolly è un certificato digitale che viene utilizzato con un dominio e tutti i sottodomini corrispondenti. La notazione per un certificato jolly consiste in un asterisco e un punto prima del nome di dominio.

SAN. Un nome alternativo soggetto (SAN) consente di associare nomi soggetti aggiuntivi con un certificato digitale. I nomi aggiuntivi potrebbero essere o non essere simili al nome soggetto principale del certificato. In effetti, una SAN può includere indirizzi e-mail, indirizzi IP, URI, nomi di directory o nomi DNS.

Code signing. Un certificato di firma del codice è un certificato digitale utilizzato per confrontare il software autore e assicurarsi che il codice non sia stato modificato. I certificati di firma del codice sono comunemente utilizzati dagli sviluppatori di software per firmare digitalmente app, driver e programmi software.

Self-signed. Un certificato autofirmato è un certificato digitale che viene firmato utilizzando il proprio chiave privata. Ad esempio, un certificato CA radice è considerato un certificato autofirmato. Tuttavia, i certificati autofirmati non vengono in genere utilizzati per comunicazioni multipartitiche a meno chei certificati vengono aggiunti a una whitelist di certificati attendibili (ad esempio certificati CA radice).

Types of certifcates

Machine/computer. Mentre alcuni certificati digitali sono assegnati a un utente, altri digitali i certificati sono assegnati a una macchina o un computer. In quest'ultimo scenario, i certificati possono essere utilizzato per consentire ai client di verificare l'autenticità dei server e l'autenticazione reciproca, o autenticazione a due vie. L'autenticazione reciproca si riferisce all'autenticazione di due parti
tra loro contemporaneamente.

Email. La protezione della posta elettronica mediante un certificato digitale garantisce la riservatezza e l'integrità di messaggi tra le parti. Sono disponibili più opzioni per il mittente per proteggere la posta elettronica, tra cui firma, crittografia o entrambi. Uno dei protocolli principali utilizzati è Secure /Protocollo S / MIME (Multipurpose Internet Mail Extensions), che è emerso

come standard per la posta elettronica crittografata. S / MIME utilizza l'algoritmo di crittografia RSA ed è consigliato da esperti di sicurezza.

User. È richiesto un certificato assegnato a un utente per consentire agli utenti di firmare o crittografare la posta elettronica.

Root. Un certificato radice è il certificato più alto assegnato alla CA radice. È anche il certificato più importante in un PKI. Se succede qualcosa al certificato (come è revocato o scaduto), ha un impatto su tutti i certificati emessi dalla PKI.

Dominio validated. Un certificato convalidato dal dominio (DV) è un certificato digitale in cui il nome di dominio del richiedente è stato convalidato dimostrando la proprietà di un DNS dominio. Un certificato DV viene in genere utilizzato per Transport Layer Security (TLS). La proprietà del dominio è in genere provata utilizzando le informazioni del registrar di dominio, i record DNS, l'e-mail o il account di web hosting di un dominio.

Extended validation. Un certificato di convalida estesa (EV) è simile a un certificato convalidato dal dominio ma con una verifica più rigorosa dell'identità dell'entità richiedente da una CA. Sebbene un certificato DV fornisca un livello base di verifica, il certificato EV fornisce ulteriore fiducia ai consumatori che desiderano avere la certezza di un operatore di siti Web un'organizzazione legale, consolidata con un'identità verificabile. Il controllo aggiuntivo che è richiesto ai richiedenti include controlli manuali di tutti i nomi di dominio richiesti dal richiedente, controlli contro fonti di informazione indipendenti, controlli contro fonti governative ufficiali e telefonate alla società per confermare la posizione del richiedente.
Se il certificato viene accettato, il numero di serie registrato dal governo dell'azienda e il suo indirizzo fisico sono memorizzati nel certificato EV.

DER. Un certificato di codifica distinta (DER) è un certificato codificato binario. Tutti i tipi di certificati e chiavi private possono essere codificati utilizzando il formato DER. I certificati in formato DER utilizzano comunemente le estensioni .cer e .der file.

Certifcate formats Esistono diverse estensioni di nomi di file per certificati X.509. Alcune di queste estensioni sono utilizzato anche per altri dati, come le chiavi private.

PEM. Un certificato PEM (Privacy Enhanced Electronic Mail) è una variante del certificato DER. I certificati PEM sono file ASCII codificati Base64, che sono racchiusi tra le stringhe "----- INIZIA CERTIFICATO -----" e "----- FINE CERTIFICATO -----". Certificati PEM sono il formato più comune; usano le estensioni .cer, .crt, .pem e .key file.

CER. CER è un'estensione fle per i certificati. I certificati sono di solito in forma DER binaria, ma anche i certificati con codifica Base64 sono comuni (vedi .pem sopra). Il sistema operativo Windows gestisce nativamente l'estensione fle .CER per operazioni come la visualizzazione e importazione di certificati.

P7B. I file P7B, detti anche certificati PKCS (Public-Key Cryptography Standards) n. 7, contengono solo certificati o certificati di catena ma non la chiave privata. I certificati P7B utilizzano comunemente le estensioni dei nomi di file .p7b e .p7c.

PFX. Un certificato di scambio di informazioni personali (PFX) è codificato binario. Il certificato PFX archivia il certificato server, i certificati intermedi e la chiave privata in un file crittografato. I certificati PFX utilizzano comunemente l'estensione del nome fle .pfx.

P12. Un file P12, chiamato anche PKCS (Public-Key Cryptography Standards) # 12 certifcate, contiene in genere chiavi private certificate e protette da password. Il certificato P12 è a successore del certificato PFX e utilizza comunemente l'estensione del nome del file .p12.

COMPLICATO ? NEI MITI DELL'ANTICA GRECIA IL NODO DI GORDIO ERA UN NODO INESTRICABILE LEGATO A UNA PROFEZIA. ALESSANDRO MAGNO ARRIVO' E TAGLIO' IL NODO CON LA SPADA, REALIZZANDO LA PROFEZIA.

NEL NOSTRO CASO DI GENTE COMUNE NON CI SONO IMPERATORI E SPADE: BASTA USARE LA CRITTOGRAFIA DI ROBIONICA

DELL'ALGORITMO CRIPTEOS 3001 E TUTTO DIVENTA PIU' SEMPLICE .
RIPARTIAMO ADESSO A LEGGERE DAL PRIMO CAPITOLO

Dominio 1

Viruses .Un virus è un programma dannoso progettato per replicarsi. I virus sono generalmente associati file legittimi, come documenti o programma di installazione. Non tutti i virus sono progettati per danneggiare un computer; a volte sono divertenti o scherzi, e altre volte, sono scritti da hacker che cercano di raggiungere l'infamia. Esistono molti tipi diversi di virus - virus macro, virus del settore di avvio e così via - ma non è necessario conoscere tutti i diversi tipi per questo esame.

IL VIRUS SI REPLICA COME IL CORONAVIRUS. INVECE DELLE PERSONE SONO I COMPUTER E DISPOSITIVI COLLEGATI IN RETE INTERNET CHE TRASMETTONO L?INFEZIONE

Crypto-malware. Il crypto-malware è un tipo di ransomware che utilizza la crittografia per bloccare l'accesso ai dati. È difficile da superare senza pagare il riscatto o avere un backup dei dati.
IL CRIPTO-MALVARE PUO' ESSERE FERMATO DAL PRODOTTO DI ROBIONICA RAMSES CHE IDENTIFICA I SITI CRITTOGRAFATI SU UNA LISTA PREFISSATA.

Ransomware. Il ransomware è un malware progettato per contenere un computer o un ostaggio di dati fino al pagamento del riscatto. Questo potrebbe bloccare l'accesso ai dati, cambiando il computer abbastanza da renderlo difficile per utilizzare o crittografare i dati (questo è noto come crypto-malware, che è il prossimo punto dell' elenco). Una volta che un riscatto viene pagato agli aggressori, i dati vengono generalmente rilasciati all'utente.
IL RANSOMWARE PUO' ESSERE FERMATO DAL PRODOTTO DI ROBIONICA RAMSES CHE IDENTIFICA I SITI CRITTOGRAFATI SU UNA LISTA PREFISSATA. VIENE SACRIFICATO UN SOLO SITO

Worm. Un worm è un tipo di malware il cui unico scopo è diffondersi. Spesso i worm non causano danni a un computer o dati. Tuttavia, a causa della rapida diffusione di un worm, può causare problemi su una rete (ad esempio consumando la maggior parte o tutta la larghezza di banda disponibile). Occasionalmente, un worm avrà un payload dannoso che causa problemi, come l'eliminazione dati su un computer.
LA PROPAGAZIONE WORM PERMETTE DI INFETTARE TUTTI I COMPUTER O DISPOSITIVI COLLEGATI IN RETE INTERNET

Trojan. Come un cavallo di Troia, il Trojan è un'applicazione dannosa che induce in errore gli utenti. I Trojan spesso sono nascosti nel programma di installazione - ad esempio, quando un utente installa un programma di fotoritocco, il Trojan viene installato silenziosamente in background, all'insaputa dell'utente. In generale, una volta
installati, i trojan non tentano di replicarsi o propagarsi; invece, spesso si connettono a un server di comando e controllo per eseguire il report e ottenere ulteriori istruzioni.

IL TROJAN E' UNA APPLICAZIONE DANNOSA. IL RECENTE DECRETO INTERCETTAZIONI LO HA PERMESSO NON SOLO DA PARTE DI AUTORITA' GIUDIZIARIE, MA DI TUTTI GLI INCARICATI DI PUBBLICO SERVIZIO, FERROVIERI, AUTISTI AUTOBUS, OPERATORI NETTEZZA URBANA, CREANDO UN VERO E PROPRIO "GRANDE FRATELLO" COME NEL PROFETICO ROMANZO DI ORWELL 1984

I trojan sono spesso abituati a installare backdoor (definite più avanti in questo elenco) su un computer, fornendo l'accesso remoto all'attaccante al computer. MOLTO SPESSO CON I TROJAN POSSONO ESSERE INSERITE FALSE PROVE, COME ACCESSO A SITI PEDOPORNOGRAFICI, FOTO O VIDEO COMPROMETTENTI, E VIA DICENDO. INOLTRE LE SOCIETA' DI INFORMATICA PER GESTIRE LE LICENZE ENTRANO NEL TUO COMPUTER, VIOLANDO L'ARTICOLO 15 DELLA COSTITUZIONE ITALIANA "LA LIBERTA' E LA SEGRETEZZA DELLA CORRISPONDENZA E DI OGNI ALTRA FORMA DI COMUNICAZIONE SONO INVIOLABILI"

Rootkit. Un rootkit è un tipo di malware progettato per consentire agli aggressori di connettersi e controllare un computer compromesso in remoto. Spesso, dà loro il pieno controllo del computer.

ANCHE IN QUESTO CASO VIOLIAMO LA COSTITUZIONE ITALIANA

I rootkit hanno un modo per registrare audio, video (da webcam), catturare sequenze di tasti e rubare dati.

COPRIRE LA WEBCAM DEL TELEVISORE QUANDO SEI I CAMERA IN INTIMITA'

Keylogger. Un keylogger, o registratore di battitura, cattura segretamente tutti i tasti premuti sulla tastiera e o li invia a un server remoto o li registra su un file per il successivo recupero da parte di un utente malintenzionato. Ad esempio, potrebbe

acquisire tutte le sequenze di tasti da parte di un utente che visita il proprio sito Web bancario
- include le loro credenziali. L'autenticazione a due fattori può aiutare a proteggere dai keylogger, soprattutto se si tratta di inserire un codice univoco per ogni accesso.

CON IL PRODOTTO KEY-LOCK DI CRITTOGRAFIA SICURA SI EVITANO QUESTI DANNI. NON VI E' DIGITAZIONE DI PASSWORD. UN SEMPLICE COPIA E INCOLLA PERMETTE DI SCRIVERE LA PASSWORD SUL SITO DELLA BANCA

Adware. L'adware è un tipo di malware il cui scopo principale è visualizzare annunci sul tuo computer, guadagnare soldi per i loro creatori. La maggior parte degli attacchi adware si verificano contro i browser. Nota che l'adware è diverso dalle applicazioni legittime che dispongono di pubblicità in linea perché tali applicazioni ottengono in genere l'autorizzazione da parte dell'utente, spesso sottoscrivendo tale parte dell'accordo per scaricare il software, mentre adware visualizza annunci senza il permesso dell'utente.

QUI MANCA UNA LEGISLAZIONE CHE PUNISCA SIMILI AZIONI

Spyware. Lo spyware è un malware il cui scopo principale è rubare informazioni sensibili da un computer. I metodi includono l'intercettazione di sequenze di tasti, il furto diretto dei dati e il dirottamento dei microfoni o webcam. Alcuni spyware sono progettati specificamente per ottenere informazioni bancarie.

ANCHE IN QUESTO CASO CON IL PRODOTTO KEY-LOCK DI CRITTOGRAFIA SICURA SI EVITANO QUESTI DANNI. NON VI E' DIGITAZIONE DI PASSWORD. UN SEMPLICE COPIA E INCOLLA PERMETTE DI SCRIVERE LA PASSWORD SUL SITO DELLA BANCA

Robot. I robot per computer sono disponibili in due forme: buoni e cattivi. I buoni robot svolgono compiti ripetitivi, come ad esempio attività manuali automatizzate. I robot danneggiati prendono il controllo del computer, riportano a un comando e controllare il server e attendere le istruzioni. Spesso i robot fanno parte di una botnet, un gruppo di robot collegati a un'infrastruttura di comando e controllo.

Bots. Le botnet vengono abitualmente utilizzate per eseguire attacchi denial-of-service (DoS), ma possono anche rubare dati, acquisire sequenze di tasti e inviare e-mail indesiderate.
ANCHE QUI I PRODOTTI ROBIONICA POSSONO DARE RISPOSTE EFFICACI

RAT. Un Trojan di accesso remoto (RAT) è un tipo di malware progettato per creare una backdoor e fornire controllo amministrativo su un computer. I RAT possono essere impacchettati con download legittimi (per esempio, programmi di prova) e ottenere l'accesso a un computer senza che l'utente lo sappia.

I TROJANS SONO DANNOSISSIMI E ANDREBBERO PROIBITI. LA BACKDOOR SI PUO' REALIZZARE COL PRODOTTO CRIPTEOS 3001, DOVE L'AUTORITA' GIUDIZIARIA PUO' AVERE ACCESSO ALLA CHIAVE SEGRETA. SE NON SI HA LA CHIAVE, BASTA AVERE IL SET DI TUTTE LE CHIAVI DELLA AZIENDA. ANCHE SE FOSSERO UN MILIONE SI AVREBBE POCHISSIMO TEMPO PER DECODIFICARE IL MESSAGGIO. UTILIZZARE BACKDOOR "SPIONE" E' CONTRO L'ARTICOLO 15 DELLA COSTITUZIONE ITALIANA

Questa sezione descrive in dettaglio i vari tipi di attacchi utilizzati dagli hacker per tentare di ottenere l'accesso non autorizzato a una rete o a un computer. Come minimo, devi conoscere ogni metodo di alto livello, quindi se ti viene presentato uno scenario durante l'esame, puoi determinare il tipo di attacco basato sulle informazioni fornite. Questi attacchi rientrano nelle seguenti categorie:

Cryptographic attacks

Social engineering attacks . L'ingegneria sociale è l'arte di ingannare le persone. Gli attacchi avvengono tramite e-mail, telefono e di persona. Il social engineering è uno dei tipi più pericolosi di attacchi perché ha un livello elevato tasso di successo. Ecco i tipi di attacchi di ingegneria sociale coperti dall'esame Security +:

Logic bomb. Quando il malware è progettato per creare il caos in una data e ora specifiche o quando si verifica una condizione specifica, è noto come una bomba logica. Le bombe logiche sono spesso distruttive, eliminando i dati o prendendo domande di offline. Sono spesso associati ad attacchi interni. Ad esempio, lo sviluppatore scontento potrebbe creare una bomba logica, configurandola con cura per esplodere un po 'dopo che lui o lei lascia l'azienda per ridurre il rischio di essere ritenuto responsabile per esso.

Backdoor . Una backdoor è un tipo di malware che fornisce un modo segreto per accedere a un computer. Ad esempio, supponiamo che una pagina Web richieda l'autenticazione. Una backdoor potrebbe fornire un modo per bypassare l'autenticazione manipolando l'URL o eseguendo una serie di clic nel posto giusto. Le

backdoor possono essere disponibili per chiunque , ma lo sono a volte stabilite dagli hacker per eludere il normale metodo di accesso.

LA BACKDOOR SI PUO' REALIZZARE COL PRODOTTO CRIPTEOS 3001, DOVE L'AUTORITA' GIUDIZIARIA PUO' AVERE ACCESSO ALLA CHIAVE SEGRETA. SE NON SI HA LA CHIAVE, BASTA AVERE IL SET DI TUTTE LE CHIAVI DELLA AZIENDA. ANCHE SE FOSSERO UN MILIONE SI AVREBBE POCHISSIMO TEMPO PER DECODIFICARE IL MESSAGGIO. UTILIZZARE BACKDOOR "SPIONE" E' CONTRO L'ARTICOLO 15 DELLA COSTITUZIONE ITALIANA

Social engineering attacks

Phishing. Il phishing è l'atto di cercare di ingannare qualcuno per rinunciare a informazioni personali o informazioni sensibili. Esistono tre strade per gli attacchi di phishing:

Spear phishing.Spear phishing è il phishing che prende di mira un individuo o un piccolo gruppo di persone. Tipicamente, gli attacchi di spear phishing sono più sofisticati degli attacchi di phishing di massa; gli attaccanti spesso sanno di più sui loro bersagli e spesso guadagnano di più se il bersaglio è compromesso.
La caccia alle balene è un tipo di spear phishing che si rivolge a persone di alto profilo, come i dirigenti di aziende pubbliche. Gli attaccanti di caccia alle balene spesso fanno fatica a imparare molto sui loro obiettivi e attacchi di successo possono produrre guadagni molto più alti rispetto ad altri attacchi di phishing.
IL PHISHING FUNZIONA CON OPERAZIONI DI INTELLIGENZA ZERO (APRIRE UN DOCUMENTO, CLICCARE UN LINK) CHE NESSUNA FORMAZIONE PUO' EVITARE. NELLA CONFUSIONE DI UN UFFICIO INEVITABILMENTE CLICCHI. ROBIONICA HA REALIZZATO UNA METODOLOGIA HARDWARE-SOFTWARE PER EVITARE GLI ATTACCHI DI PHISHING. VISIBILE LA DEMO SU YOUTUBE CON RICERCA "ROBIONICA"

Vishing. Vishing è phishing per telefono. Mentre alcune persone si riferiscono a questo come phishing, vishing è il termine ufficiale. Con il phishing, l'obiettivo è quello di ottenere informazioni sensibili o personali dalla persona che risponde al telefono. Spesso, il chiamante impersonerà un'altra persona, tenterà di far sembrare importante e hanno un motivo per accelerare le richieste.

MOLTO SPESSO LE TELEFONISTE, ISTRUITE SU QUESTO, BLOCCANO OGNI TELEFONATA COMMERCIALE

Le difese contro il phishing includono la formazione dei dipendenti, campagne di phishing interne da testare,educare gli utenti e le difese tecniche come scansioni anti-phishing prima che la posta elettronica venga consegnata agli utenti finali.

. ROBIONICA HA REALIZZATO UNA METODOLOGIA HARDWARE-SOFTWARE PER EVITARE GLI ATTACCHI DI PHISHING. VISIBILE LA DEMO SU YOUTUBE CON RICERCA "ROBIONICA"

Email (the most common method). Molte persone hanno familiarità con il tipico phishing, e-mail che finge di provenire dalla tua banca e ti chiede di confermare le tue informazioni o resettare il tuo account. Questi tipi di e-mail di phishing a volte sembrano legittimi e in genere utilizzano collegamenti dannosi. Dopo aver fatto clic sul collegamento dannoso, potresti essere indirizzato a un falso
sito Web della banca, il malware potrebbe essere installato di nascosto sul tuo computer o sul tuo browser e potrebbe essere dirottato. Il phishing e-mail in genere è indirizzato a molte persone alla volta perché è facile ed economico.

Telephone (the second most common method). Il phishing per telefono è simile: una persona chiama il "supporto IT" e menziona qualcosa sull'infezione del tuo computer. La persona quindi ti chiede di visitare un sito Web di supporto speciale per il tuo computer. Tuttavia, quel sito Web di supporto speciale spesso installa in modo nascosto malware sul tuo computer.

In person (the least common method). Un attacco di phishing potrebbe anche coinvolgere una persona che si presenta come un impiegato di utilità elettrica che chiede di riparare la tua infrastruttura elettrica dentro, per ottenere l'accesso non autorizzato alle tue strutture.

Tailgating . Il tailgating è quando qualcuno segue una persona autorizzata in un'area riservata, come un edificio aziendale spesso, senza fornire le proprie credenziali, come scorrere la chiave magnetica. Per le piccole aziende, è difficile per un aggressore sferrare un attacco di tailgating perché tutti si conoscono e nessuno permetterà a uno sconosciuto di entrare. Tuttavia, nelle grandi aziende con migliaia di persone, è comune non conoscere la maggior parte dei tuoi colleghi. Ma tailgating ancora si verifica abitualmente perché in molti paesi le persone considerano cortesia comune tenere la porta per la persona dietro di loro, specialmente se sono adeguatamente vestiti, sembrano avere l'età giusta e così via. Alcuni attaccanti ne trasportano una grande quantità di stuff (come una borsa per il pranzo, un drink e uno zaino) e chiedono aiuto per entrare. Gli attacchi di tailgating sono pericolosi perché

offrono agli aggressori l'accesso fisico al tuo ambiente e ai tuoi computer. Gli aggressori possono lasciare chiavette USB infette in posizioni chiave o tentare di prendere dal computer. Per ridurre il rischio, alcune aziende vietano il tailgating e richiedono che ogni dipendente faccia scorrere il badge per entrare, anche se arrivano contemporaneamente a qualcun altro.

TUTELANDO LE CREDENZIALI CON CRIPTEOS 3001 O KEY-LOC DI ROBIONICA E'DIFFICILE CHE GLI ATTACCANTI RIESCANO AD ACQUISIRE DATI. LE CHIAVETTE AZIENDALI DOVREBBERO AVERE IL LOGO E TUTTE LE ALTRE DOVREBBERO ESSERE PROIBITE

Impersonation . Un attacco di rappresentazione è un attacco in cui una persona malintenzionata tenta di impersonare una persona o entità legittima. Gli attacchi di imitazione possono verificarsi tramite e-mail, sul Web o di persona. Ad esempio, supponiamo che Company12345 abbia il dominio company12345.biz - e un utente malintenzionato registra un nome di dominio molto simile, company123456.biz; la piccola differenza
tra questi nomi potrebbe passare inosservato tramite e-mail o quando si visita un sito Web. O un attaccante potrebbe vestirsi da bidello, portando uno zaino sotto vuoto e indossando guanti; potrebbero essere in grado per girovagare facilmente per il tuo vecchio edificio senza attirare troppa attenzione.

Dumpster diving .L'immersione con cassonetto è in circolazione da prima dei computer e di Internet: semplicemente attaccanti, setacciare i cassonetti della spazzatura alla ricerca di informazioni personali o sensibili che potrebbero utilizzare per effettuare spear phishing o altri attacchi o consentire loro di rubare l'identità di qualcuno. Gli aggressori spesso cercano anche rifiuti elettronici, come unità disco, chiavette USB e nastri di backup. Per ridurre al minimo le possibilità di essere colpiti da un attacco subacqueo del cassonetto, dovresti distruggere tutti i documenti sensibili e distruggere fisicamente tutta la memoria elettronica prima di scartarla.

GIUSTO

Shoulder surfng . Quando una persona guarda segretamente lo schermo del computer o la tastiera di un altro utente, quella persona è surfing spalla. È un modo semplice per ottenere password, metodi di accesso e altro informazione sensibile. È un attacco pericoloso che spesso passa inosservato. Per proteggersi , puoi mettere un piccolo specchio sul monitor o nel tuo cubicolo.

ANCHE IN QUESTO CASO USANDO KEY-LOCK DI ROBIONICA NON CI SONO PASSWORD DA RUBARE

Hoax . Una bufala è una falsa pretesa di invogliare qualcuno a compiere l'azione desiderata. Ad esempio, un attaccante potrebbe affermare che hai vinto qualcosa o che vogliono comprare qualcosa da te così fornirai informazioni personali, come il numero di previdenza sociale o il conto bancario. Per ridurre al minimo le possibilità che una bufala sia efficace contro di te, sii scettico quando vedi o senti qualcosa che è troppo bello per essere vero o che è in qualche modo insolito.

IL SISTEMA ANTIPISHING DI ROBIONICA PROTEGGE ANCHE DA QUESTA EVENTUALITA'

Watering hole attack . Un watering hole in genere colpisce un'azienda specifica. L'attaccante viene a conoscenza di siti Web che l'azienda frequenta (watering hole) e tenta di posizionare malware su quei siti nella speranza che qualcuno nell'azienda venga infettato. Gli attacchi possono verificarsi di persona: un utente malintenzionato può posizionare chiavette USB infette presso l'helpdesk IT o area di supporto in una scatola con un cartello con la dicitura "Chiavette USB gratuite".

L'AZIENDA DEVE FARE UNA POLICY DI CONTENIMENTO DI SIMILI CASI

Authority . Quando l'attaccante trasmette autorità in un attacco di ingegneria sociale, l'attacco ha più probabilità di avere successo. Ad esempio, l'attaccante potrebbe impersonare un dirigente di alto livello o un IT persona di supporto. Le persone spesso fanno di tutto per rendere felici tali autorità, che consente all'attaccante di ottenere l'accesso a informazioni riservate.

Intimidation. Esistono diversi modi in cui gli aggressori usano l'intimidazione durante un attacco di ingegneria sociale. Essi potrebbero tentare di spaventare la vittima ("Se non mi mandi le persone, il controllo non può certificare i risultati dell'azienda ") o minacciarli (" se non si desidera convalidare la propria identità, allora registrerò il tuo rifiuto e lo segnalerò alle risorse umane "). L'intimidazione arriva spesso durante una rappresentazione di attacco, in cui l'attaccante impersona qualcuno in una posizione di alto livello di autorità.

Consensus. L'attaccante stabilisce il consenso affermando che altri stanno eseguendo l'azione richiesta. Per esempio, per ottenere informazioni di controllo sensibili da un'azienda, un utente malintenzionato potrebbe chiamare un manager di livello più basso e menzionare che il suo collega è stato in grado di fornire le informazioni richieste durante l'ultimo audit al fine di aumentare la probabilità della vittima di soddisfare la richiesta.

Scarcity . Quando qualcosa scarseggia, spesso diventa più desiderabile. Aziende di marketing spesso usano la scarsità per stimolare la domanda. Anche gli aggressori di ingegneria sociale lo usano, ad esempio durante una bufala o un attacco di phishing, un utente malintenzionato potrebbe menzionare che un premio o un omaggio ha una disponibilità limitata.
Ora che hai una buona conoscenza dei tipi di attacchi di ingegneria sociale, facciamo rivedere le ragioni principali per cui questi attacchi sono efficaci:

Familiarity. La familiarità può anche aiutare gli attacchi ad avere successo. Ad esempio, un utente malintenzionato potrebbe vestirsi come un addetto alla manutenzione e camminare per un settimana nell'edificio di una società. Solo dopo essere stato visto per una settimana l'attaccante chiede a qualcuno di dargli accesso all'armadio del telefono. Poiché l'attaccante sembra familiare ("oh, lavora qui e fxes stu ff"), i dipendenti saranno più disponibili a tenere una porta aperta per lui o di aiutarlo ad accedere alle aree riservate. Allo stesso modo, un utente malintenzionato può chiamare un dirigente di alto livello al telefono ed essere gentile e cortese con l'assistente esecutivo.Dopo un paio di settimane da queste chiamate, l'attaccante potrebbe presentarsi all'assistente in maneira amichevole e quindi tentare di sfruttare l'assistente.

ANCHE IN QUESTO CASO BASTANO POCHI SEMPLICI ACCORGIMENTI AZIENDALI E L'UTILIZZO DEI SOFTWARE ROBIONICA

Trust . Gli attacchi di ingegneria sociale a volte comportano fiducia. Ad esempio, un utente malintenzionato potrebbe ottenere un lavoro presso un'azienda target. Dopo alcuni mesi di lavoro lì, l'attaccante è in una buona posizione e effettuare attacchi di ingegneria sociale contro colleghi. L'attaccante è attendibile come "Uno di noi", che fa sì che i dipendenti scartino il loro normale scetticismo.

Urgency. Una tattica comune negli attacchi di ingegneria sociale è impartire un senso di urgenza. Per esempio,un utente malintenzionato che funge da amministratore dell'helpdesk può chiamare un utente e dire: "Ciao, Terry. Questo è Chris
finita nell'IT. Il tuo computer ha un virus. Dobbiamo installare immediatamente un FX sul tuo computer.
Posso inviarti un'e-mail adesso? " Un simile attacco può essere molto efficace perché le vittime spesso pensano che succederanno cose brutte se non agiranno in fretta.

RICORDIAMO IL SISTEMA HARDWARE-SOFTWARE ANTI PHISHING DI ROBIONICA

DoS. Un attacco denial of service tenta di sopraffare una rete, un computer o un'altra parte dell'infrastruttura IT per degradare le prestazioni o usufruire di un servizio. La maggior parte degli attacchi DoS noti hanno come bersaglio reti o servizi specifici.

DDoS. Un attacco denial of service distribuito è un attacco DoS su larga scala che sfrutta le botnet create di molti computer o dispositivi informatici, spesso migliaia di dispositivi o più. Il botnet invia richieste di rete o altre comunicazioni allo stesso servizio o rete fino a quando il servizio o la rete non saranno sopraffatti e inutilizzabili.

L'UTILIZZO DI DUE COMPUTER CON CRIPTEOS 3001 CON LA TECNICA DEL "PONTE LEVATOIO" PERMETTE DI FERMARE GLI ATTACCHI ESTERNI AL PC COLLEGATO IN RETE INTERNET, CHE CRITTOGRAFA E TRASMETTE VIA CAVO AL PC COLLEGATO COLL'OBIETTIVO SENSIBILE, CENTRALE NUCLEARE, BANCA ECCETERA. Il SECONDO PC DECRIPTA E IDENTIFICA EVENTUALI ANOMALIE DEL MESSAGGIO ISOLANDO L'OBIETTIVO. VANTAGGIOSAMENTE L'ANALISI DI MESSAGGI ANOMALI PUO' ESSERE ABBINATO AL PC ESTERNO.

Gli attacchi di applicazioni e servizi prendono di mira applicazioni o servizi specifici. Ad esempio, un attacco potrebbe colpire i server Web o tentare di riutilizzare le credenziali dell'utente e autenticarsi come qualcun altro. Come per gli altri argomenti, devi essere in grado di differenziare tra i vari tipi di attacchi e determinare il tipo di attacco in uno scenario fornito sull'esame. Il
i punti elenco seguenti descrivono in dettaglio i tipi di attacchi di applicazioni e servizi:

Application/service attacks
La comunicazione su una rete è in genere tra due parti, punto A e punto B.

man-in-the-middle . Un attacco man-in-the-middle (Uomo nel mezzo) falsifica una parte per intercettare il traffico prima di trasmettere le informazioni alla parte designata. L'attaccante potrebbe essere origliato o sta cercando di raccogliere abbastanza informazioni per aggirare successivamente i metodi di autenticazione. ANCHE IN QUESTO CASO NON AVENDO PASSWORD DIFFICILE VIOLARE I SOFTWARE ROBIONICA

Buffer overflow. Un buffer è dove un'applicazione può scrivere temporaneamente i dati. Si verifica un overflow del buffer, quando vengono scritti o archiviati più dati di

quelli assegnati allo spazio. Gli aggressori li possono causare deliberatamente per produrre errori o causare l'arresto anomalo delle applicazioni.

DOVREBBE ESSERE FATTA ANALISI DELLA MEMORIA

Injection. L'iniezione di codice è spesso associata all'iniezione SQL, ma può anche utilizzare LDAP, SMTP e altri metodi. L'attaccante aggiunge (inietta) il proprio codice dannoso in un'applicazione o servizio in fase di esecuzione. Ciò può causare una negazione del servizio, perdita di dati o acquisizione completa da parte dell'attaccante.
Cross-site scripting . Cross-site scripting (XSS) è una vulnerabilità dell'applicazione Web che consente agli aggressori di iniettare script nel sito Web o nell'applicazione. Lo script ha come target una vulnerabilità nell'app Web, il server su cui è in esecuzione l'app o un plug-in associato all'app. Un attacco XSS sfrutta la fiducia di un utente per un sito Web o un'applicazione.

INIEZIONE SQL E' UNA TECNICA CHE' E' STATA PER 15 ANNI IN TESTA ALLE CLASSIFICHE OWASP DI VULNERABILITA' PIU' PERICOLOSE,

BASTAVA L'UTILIZZO DELLA SEMANTICA "PREPARE STATEMENT" NEL CODICE HTML PER BLOCCARE IL FENOMENO. ANCHE IN QUESTO CASO ABBANDONARE L'AUTENTICAZIONE CON UTENZA E PASSWORD RISOLVE IL PROBLEMA

Privilege escalation . Il processo di attacco a un sistema per ottenere l'accesso a quel sistema o ad altre risorse che sono tipicamente protette è l'escalation dei privilegi. Esistono due tipi di escalation di privilegi: orizzontale e verticale. L'escalation orizzontale è il punto in cui un utente accede a sistemi o risorse sono pensati per altri sistemi o utenti. L'escalation verticale è il punto in cui un utente accede ai sistemi o risorse che utilizzano un account di livello superiore, come l'accesso amministrativo o root.

DICONO CHE IN WINDOWS10 E' FACILISSIMO DIVENTARE AMMINISTRATORI DI SISTEMA

ARP poisoning . Il Address Resolution Protocol aiuta un sistema a identificare l'indirizzo hardware (MAC) di un dispositivo. L'avvelenamento da ARP è il processo di spoofing o modifica di tali dati in modo che le informazioni vengano trasmesse a un altro dispositivo, in genere di proprietà dell'attaccante, piuttosto che al destinatario previsto.

Amplifcation . Un attacco di amplificazione è un tipo di attacco DDoS che di solito prende di mira i servizi di rete come NTP e DNS. L'attaccante tenterà di sopraffare il servizio di destinazione con un grande quantità di traffico UDP per rendere inaccessibile il servizio e l'infrastruttura.

Cross-site request . Un attacco di falsificazione delle richieste tra siti (XSRF) colpisce un sito Web o un'applicazione di un utente attendibile sessione del browser. L'utente può (consapevolmente o inconsapevolmente) trasmettere comandi o script per attaccare un'applicazione. Contrariamente a un attacco XSS, un attacco XSRF sfrutta la fiducia di un utente che ha nell'accesso ai dati di una applicazione web.

DNS poisoning . Un Dominio Name System assiste un sistema traducendo nomi descrittivi in indirizzi IP. DNS l'avvelenamento è il processo di spoofng o modifica dei record DNS in modo che quando un nome descrittivo sia cercato, viene restituito un indirizzo IP errato. Questa tattica può essere utilizzata per reindirizzare il traffico in una negazione di attacco di servizio o per inviare il traffico al sito Web dell'attaccante anziché al sito corretto.

Dominio hijacking. Tutti i nomi di dominio sono registrati tramite un registrar ufficiale IANA, che controlla i domini di primo livello disponibili. Se la registrazione di un nome di dominio viene rubata o compromessa, vale a dire dirottamento del dominio. L'attaccante ha quindi il pieno controllo del dominio e quindi può cambiare i server dei nomi, le informazioni di contatto e altro ancora.

Man-in-the-browser. Un attacco man-in-the-browser è un tipo di attacco man-in-the-middle in cui un browser web viene attaccato da un codice su un sito Web. Il risultato è che l'attaccante prende il controllo del web browser e consente al browser di inserire codice, apportare modifiche all'applicazione o modificare il contenuto del sito Web senza che l'utente o il sito Web lo sappiano.

Zero day. Se un utente malintenzionato identifica una nuova vulnerabilità e la sfrutta nello stesso giorno, si tratta di un zero day attacco. Un attacco zero day è pericoloso perché se hai anche le ultime patch di sicurezza, gli aggiornamenti non ti proteggeranno da vulnerabilità sconosciute. L'attacco si verifica prima che qualcuno sia consapevole che esiste l'exploit e il fornitore può emettere un fx.

IMPORTANTE CREARE SOFTWARE A ERRORE ZERO, METTERE SUL MERCATO SOFTWARE INCOMPLETI DAL PUNTO DI VISTA DELLA SICUREZZA PORTA A GROSSI PROBLEMI. TECNICHE DI MERCATO DI

FAR TESTARE SOFTWARE E SISTEMI OPERATIVI AI CLIENTI E' ESTREMAMENTE DANNOSO

Pass the hash. Un passaggio d'attacco hash evita la necessità di conoscere le credenziali di un account utente passando l'hash dell'utente precedentemente autenticato per la risorsa desiderata. Questi tipi di attacchi sono utili se le password non vengono cambiate frequentemente e le risorse non richiedono autenticazione a più fattori.

LA CRITTOGRAFIA HASH NON E' SICURA

Replay. Un attacco replay è una trasmissione ripetuta (ripetuta) di una comunicazione valida. L'obiettivo è accedere a risorse o dati rinviando una trasmissione valida. Utilizzando i timestamp sulla comunicazione può aiutare a minimizzare o bloccare gli attacchi di replay. Inoltre, utilizzando una sola volta chiavi o password per la comunicazione puo' anche essere utile.

RICORDIAMO MEGLIO NON USARE PASSWORD. LE CHIAVI CHE DURANO UNA SOLA VOLTA POSSONO ESSERE VIOLATE

Hijacking and related attacks

Clickjacking. I siti Web sembrano in genere bidimensionali, ma gli attaccanti possono nascondere contenuti cliccabili sotto un collegamento ipertestuale legittimo o un'immagine cliccabile. Quando un utente fa clic su quelo che pensano che sia un link legittimo, fanno anche clic sul link nascosto, che esegue codice dannoso.

Session hijacking. La maggior parte dei siti Web utilizza i cookie per identificare le singole sessioni che hanno autenticato sul sito web. Questi cookie possono contenere una chiave di sessione. Gli aggressori possono accedere alla sessione rubando la chiave di sessione.

ATTUALMENTE C'E' UNA NORMATIVA DEL CODICE DELLA PRIVACY CHE IMPONE AL SITO WEB DI CHIEDERE SE SI ACCETTANO I COOKIES, ANCHE DI TERZE PARTI, CHE SERVONO A PROFILARE L'UTENTE.

OVVIO CHE SI RISPONDE "ACCETTO". E' UN PO' COME IL MEDIOEVALE "RICORDATI CHE DEVI MORIRE", UNO RICORDA E VA AVANTI..

URL hijacking. Il dirottamento degli URL (noto anche come errore di battitura) si basa sul fatto che gli utenti effettuino errori di battitura e altri errori durante l'accesso a un sito Web; vengono presentati con un sito falso che sembra essere il vero sito.

Driver manipulation Shimming. Gli spessori vengono utilizzati nella programmazione per consentire il funzionamento di diverse versioni API in un ambiente. Ciò può anche creare vulnerabilità di sicurezza quando possono essere API meno recenti usati per manipolare l'hardware.

Refactoring. In un attacco refactoring, l'attaccante cambia il codice sorgente sottostante per ottenere pieno accesso all'hardware su cui è in esecuzione, consentendo all'autore dell'attacco di utilizzare il hardware per altri attacchi.

QUESTO PUO' AVVENIRE DECOMPILANDO UN PRODOTTO E CREANDONE UNA COPIA FASULLA, PERFETTAMENTE FUNZIONANTE MA COL CODICE MALEVOLO SOTTOSTANTE

MAC spoofng.Tutti i dispositivi collegati a una rete hanno un indirizzo fisico o MAC. MAC, spoofing è il processo di modifica dell'indirizzo fisico di un dispositivo. Questa tattica potrebbe essere usata per intercettare il traffico destinato al dispositivo originale.

IP spoofng. Se un dispositivo è collegato a una rete di livello 3, utilizza gli indirizzi IP con cui comunicare con altri dispositivi. Per intercettare il traffico, un utente malintenzionato può utilizzare lo spoofing IP per agire come un altro dispositivo sulla rete.

Replay. Come un attacco denial of service, un attacco di riproduzione trasmette ripetutamente i dati. Tuttavia, i dati di riproduzione sono in genere dati validi per acquisire informazioni sulla sessione o altri dati da utilizzare in un attacco.

Wireless attacks .Gli attacchi wireless sono specifici delle reti wireless. Per lo più questi attacchi tentano di ottenere un accesso non autorizzato a una rete wireless. Questi attacchi sono particolarmente pericolosi perché spesso provengono dall'esterno della tua attività (ad esempio nel parcheggio o da attività vicine).

IV. Un attacco vettoriale di inizializzazione (IV) è un metodo per decrittografare il traffico wireless. Un aggressore impara il testo in chiaro di un singolo pacchetto wireless e quindi calcola la chiave rimanente del flusso dell'hash RC4. Tutti i traffici wireless che utilizzano lo stesso vettore di inizializzazione possono quindi essere decifrato dall'attaccante.

Evil twin. Un gemello malvagio è un punto di accesso dannoso che sembra essere legittimo (ad esempio, la rete è denominata "Visitatore Wi-Fi") ma è stata configurata

per intercettare e intercettare il traffico wireless. Il punto di accesso (AP) può rubare password, chiavi di rete e altre informazioni che vengono inviate attraverso la rete.

Rogue AP. Un punto di accesso non autorizzato è un AP che è stato aggiunto alla rete senza autorizzazione. Questo viene in genere fatto dai dipendenti che desiderano un accesso più semplice o la propria rete Wi-Fi.
Questi punti di accesso possono bypassare i requisiti di sicurezza dell'azienda e interferire con i canali wireless disponibili in un'area fisica.

ANCHE IN QUESTO CASO LA CRITTOGRAFIA HASH E' IL PUNTO DEBOLE

Jamming .Le reti wireless funzionano su canali specifici di frequenze wireless. Il numero di i canali sono determinati dalle specifiche della rete wireless. Questo numero limitato di canali rende facile per un attaccante attaccare quel raggio di segnale, come un denial-of-service, attacco per bloccare la rete.

WPS. La configurazione protetta Wi-Fi (WPS) fornisce un modo semplice per aggiungere nuovi dispositivi a una rete wireless: in molte implementazioni, non è necessario inserire la password wireless; è sufficiente premere un pulsante sull'AP e un pulsante (o pulsante virtuale) sul dispositivo e far sì che il dispositivo si unisca automaticamente alla rete. Tuttavia, questa comodità vanifica
un flusso di sicurezza - un attacco di forza bruta ai numeri PIN utilizzati per aggiungere un dispositivo può consentire ad altri dispositivi di autenticarsi sulla rete.

Bluejacking. Il bluejacking è il processo di utilizzo del Bluetooth per inviare messaggi a dispositivi abilitati Bluetooth in un raggio immediato. Bluejacking si basa sul fatto che il Bluetooth rilevabile sia abilitato con dispositivi nelle vicinanze.

Bluesnarfng. Bluesnarfng è il processo di utilizzo del Bluetooth per connettersi e rubare dati da un altro dispositivo. Questo attacco si basa su implementazioni Bluetooth vulnerabili. Per ridurre al minimo le possibilità di essere vittima,

disattiva il Bluetooth nei luoghi pubblici e tieni aggiornato il tuo dispositivo gli ultimi aggiornamenti di sicurezza.

BUONI CONSIGLI

RFID . L'identificazione a radiofrequenza (RFID) è un tipo di tecnologia wireless che consente la comunicazione a corto raggio, come il Bluetooth. Diversi attacchi

possono essere eseguiti specificatamente per RFID per falsificare o disabilitare le comunicazioni.

NFC. La comunicazione near-feld (NFC) è un tipo di tecnologia wireless che consente la vicinanza comunicazione, come RFID e Bluetooth. Alcuni attacchi possono essere eseguiti specificatamente per NFC per falsificare o disabilitare le comunicazioni.

Disassociation. Quando un client wireless si disconnette da una rete, esegue una dissociazione con il punto di accesso. Un utente malintenzionato può disconnettere di proposito altri dispositivi sulla rete fingendo di essere tali dispositivi e dissociandoli dal punto di accesso. Gli altri dispositivi non sono quindi connessi alla rete e devono essere nuovamente uniti manualmente.

Birthday. Una forma di attacco a forza bruta, un attacco di compleanno usa la teoria della probabilità. I tentativi di attacco per generare e identificare porzioni di un hash, cercando di trovare una corrispondenza.

Known plain text /cipher text. Quando un utente malintenzionato ha già accesso sia al testo in chiaro sia al testo cifrato crittografato, queste informazioni possono essere utilizzate per identificare anche le chiavi segrete utilizzate per creare il file testo crittografato e li usa per decrittografare altro testo crittografato.

Rainbow tables. Le tabelle Rainbow sono tabelle pre-assemblate per invertire hash crittografati, in genere hash di password. Le tabelle Rainbow sono particolarmente efficaci quando il target in testo semplice ha una lunghezza dei caratteri nota o limitata, ad esempio un numero di carta di credito.

Dictionary. Un attacco con dizionario è un attacco a forza bruta in cui viene trovata la chiave di decrittazione o la password provando ogni stringa in un dizionario personalizzato.

QUESTI ATTACCHI NON SONO EFFICACI CONTRO LA CRITTOGRAFIA SUPER-RESISTENTE DEL SOFTWARE CRIPTEOS 3001 DI ROBIONICA

Cryptographic attacks. Gli attacchi crittografici colpiscono tecnologie che si basano su funzioni crittografiche. Ad esempio, gli attacchi crittografici spesso prendono di mira le password, che vengono spesso archiviate utilizzando la crittografia.

QUESTI ATTACCHI NON SONO EFFICACI CONTRO LA CRITTOGRAFIA SUPER-RESISTENTE DEL SOFTWARE CRIPTEOS 3001 DI ROBIONICA

Brute force. Gli attacchi di forza bruta sono ripetuti tentativi di violare la crittografia di una password, file o sistema. Gli attacchi di forza bruta online attaccano un sistema che è attivo e potrebbe avere altra sicurezza protocolli e controlli abilitati. Gli attacchi di forza bruta offline vengono eseguiti, come contro un set calcolato di hash di password.

GLI ATTACCHI DI FORZA BRUTA, CIOE' RIPETERE TUTTE LE CHIAVI FINO A TROVARE QUELLA GIUSTA NON FANNO NIENTE CONTRO L'ALGORITMO DI CRIPTEOS 3001, DOVE DEVONO FARE 256 ELEVATO ALLA 131072 TENTATIVI. CRIPTEOS 3001 SARA' IMMUNE ANCHE QUANDO CI SARANNO I VELOCISSIMI COMPUTER QUANTICI, CHE INVECE DI AVERE IL BIT CON VALORI ZERO E UNO AVRANNO GLI STATI DI PROPBABILITA' DEFINITI DALLA TEORIA DI HEISENBERG, MOLTEPLICI IN CONTEMPORANEA MA NON INFINITI

Collision. Quando due diversi ingressi producono lo stesso valore di hash, questo è noto come una collisione. Una collisione tenta di trovare due diversi valori di input che generano lo stesso hash.

LA CRITTOGRAFIA HASH NON E' SICURA

Downgrade. Un attacco di downgrade utilizza volutamente un protocollo meno recente e meno sicuro per comunicare. Spesso, quando i clienti comunicano con i server, negoziano il metodo di comunicazione e sicurezza. In un attacco di downgrade, un cliente negozia per la minima sicurezza possibile.

Replay/playback. Un attacco di ripetizione ripete o ritarda una comunicazione di rete precedentemente valida. Ripetendo le informazioni possono consentire a un utente malintenzionato di ricevere informazioni da un server. Ritardare la comunicazione può avere lo stesso effetto di un attacco denial of service.

Finora abbiamo esaminato i tipi di malware e i tipi di attacchi. Ora guarderemo al tipo di persone coinvolte in attacchi. Durante l'esame, devi essere in grado di identificare il tipo di attaccante in base ai metodi e al livello di sofisticazione in un determinato scenario.

Explain threat actor types and attributes

Weak. Esistono diversi algoritmi e protocolli crittografici che possono essere utilizzati per crittografare i dati e traffici . Sfortunatamente, la maggior parte di loro ha conosciuto vulnerabilità e flussi, debole le implementazioni di un protocollo rendono la sua vulnerabilità più importante. Ad esempio, PPTP è un protocollo VPN che si qualifica come un'implementazione debole di una VPN; ha conosciuto la sicurezza problemi, sebbene possa ancora funzionare per la connettività VPN.

RICORDIAMO LA ESTREMA VALIDITA' DELL'ALGORITMO DI CRIPTEOS 3001 CON CHIAVI LUNGHE 128 KB

implementations
Types of actors . Di seguito sono gli attori comuni in un attacco:

Script kiddies .I kiddie degli script sono nuovi agli attacchi. Usano gli script e gli strumenti esistenti per attaccare i sistemi; spesso non hanno la capacità di creare il proprio o addirittura capire come funziona l'attacco.

Hacktivist/hacktivism. Un hacktivista usa un attacco per promuovere un messaggio politico o un'agenda sociale. Questi attacchi sono più cosmetici che dannosi.

Organized crime. Gruppi gli hacker possono riunirsi con un obiettivo o un'idea comune in mente come parte di uno sforzo organizzato. . Alcuni anelli del crimine organizzato esistenti si stanno trasformando in phishing e hacking come un altro modo per produrre reddito.

Nation states/APT. Paesi e nazioni in tutto il mondo stanno diventando sempre più attivi negli attacchi altri paesi.

Le minacce persistenti avanzate (APT) sono attacchi a lungo termine, spesso con uno stato nazionale che dirige o sponsorizza l'attacco. Questi attacchi possono essere sofisticati e pericolosi, non solo a causa della minaccia della guerra fisica, ma anche perché così tante risorse possono essere messe dietro gli attacchi.

TORNIAMO A RIPETERE: I PRODOTTI ROBIONICA SERVONO PER DIFENDERSI EGREGIAMENTE DAGLI ATTACCHI APT, SE POI LE NAZIONI USANO ALTRE TECNICHE, COME GUERRA CHIMICO- BATTERIOLOGICA NON C'E' SOFTWARE CHE TENGA. QUESTO PER CORRETTEZZA

Attributes of actors. Per aiutare a capire il tipo di attore in un determinato scenario, puoi usare le informazioni su come operano:

Insiders. La minaccia più comune e pericolosa per reti e sistemi viene dagli addetti ai lavori (dipendenti, appaltatori, venditori). Gli addetti ai lavori hanno accesso a risorse o strutture e quindi abusare di quella fiducia utilizzando l'accesso maliziosamente.

Competitors. Le organizzazioni possono utilizzare phishing o altri attacchi per trovare informazioni su un concorrente e i suoi prodotti, come funzionalità pianificate, date di rilascio o altre informazioni privilegiate che potrebbero aiutarli a competere contro l'obiettivo. Il livello di accesso di un utente malintenzionato può aumentare notevolmente le possibilità di successo.

Internal/external. Gli hacker esterni in genere hanno il vantaggio di essere anonimi ma devono ottenere l'accesso attraverso un attacco, che può essere difficile e comporta altri rischi. Gli aggressori interni sono persone fidate di un'organizzazione , in modo che abbiano il vantaggio di cose come badge porta agli edifici, accesso fisico e wireless alla rete e accesso alle risorse.

Level of sophistication, Il livello di sofisticazione di un attacco può aiutare a determinare chi potrebbe esserci dietro. Per esempio, il targeting di un vecchio exploit noto con semplici script o strumenti potrebbe indicare uno script Kiddy. Tuttavia, lo sfruttamento di vulnerabilità relativamente sconosciute può indicare un attacco più sofisticato, che potrebbe indicare il crimine organizzato o uno stato nazionale.

Resources/funding . Sebbene non tutti gli attacchi siano motivati dal punto di vista finanziario, i soldi possono svolgere un ruolo in un attacco. Quando usi più denaro e risorse per un attacco, di solito puoi produrre attacchi sofisticati.

Intent/motivation .La motivazione dietro gli attacchi può variare. Se un attacco è di un attore interno, potrebbe essere un atto di sabotaggio o vendetta, o essere correlato a un disprezzo dell'organizzazione. Gli attori esterni sono tipicamente motivati dal denaro, ma potrebbero anche far parte di un'organizzazione hacktivista, o attaccare perché credono che il bersaglio sia immorale.

.Types of intelligence. Esistono due tipi principali di intelligenza:

Open-source intelligence (OSINT).OSINT è raccolto da fonti pubblicamente disponibili, come documenti pubblici o dai social media.

Closed-source intelligence (CSINT)

CSINT è raccolto da fonti segrete.

reconnaissance . Penetration testing (pen testing) comporta il test dei controlli di sicurezza di un'organizzazione. Come i test vengono spesso eseguiti da società esterne senza alcuna conoscenza interna della rete. Ecco i concetti pen testing che dovresti conoscere:

IL PENETRATION TESTING VIENE PRESCRITTO ANCHE DAL GDPR, NORMATIVA EUROPEA SULLA PRIVACY. MA IL PROBLEMA E' CHE I PENETRATORI USANO TECNICHE HACKER, QUINDI PERICOLOSE SE USATE IMPROPRIAMENTE, E CIO' COMPORTA, PER IL GDPR, LA STIPUULA DI CONTRATTI TRA AZIENDA CLIENTE E AZIENDA DI PENETRATION TESTING CON FIORE DI AVVOCATI E ASSICURAZIONI.

SONO COSTI CHE SOLO LE AZIENDE MEDIO-GRANDI POSSONO SOSTENERE. VANTAGGIOSAMENTE IL PRODOTTO DI ROBIONICA VULNER FA IN 5 MINUTI IL LAVORO DI UN PENETRATION TESTER SENZA DANNI E PUO' ESSERE UTILIZZATO ANCHE DA PERSONALE DIGIUNO DI INFORMATICA, DATA LA ESTREMA SEMPLICITA' DI FUNZIONAMENTO

1.4 Explain penetration testing concepts

Active . La ricognizione attiva verifica i controlli di un'infrastruttura di sicurezza, ad esempio, provando differenti variabili e metodiva per restituire di proposito errori e altre informazioni sull'obiettivo.

Passive. La ricognizione passiva raccoglie informazioni sull'obiettivo senza ottenere l'accesso alla rete o risorse, come informazioni sull'edificio fisico o nomi e informazioni demografiche sul personale che vi lavora. Gli aggressori si rivolgono spesso ai social
media e motori di ricerca su Internet per ottenere ulteriori informazioni.
Un pen testing potrebbe essere necessario per accedere a reti o host diversi per continuare i test, per istanza a causa di segregazione di rete, frewalls o altre disconnessioni logiche tra dispositivi. Il processo di bypassare queste disconnessioni si chiama pivot.
I test con penna spesso utilizzano più exploit per ottenere l'accesso alle risorse di destinazione. L'iniziale sfruttamento mira ad ottenere l'accesso alla rete. Quindi, exploit o tecniche aggiuntive potrebbero essere necessarie per aumentare i privilegi o spostarsi all'interno della rete.

reconnaissance
Pivot
Initial exploitation
21
Persistence. Alcuni pen testing prevedono la scansione e il test delle risorse una volta per assicurarsi che sono aggiornati sulle ultime patch e hanno una solida configurazione di sicurezza. I Pen testing persistenti estendono questi test nel tempo, il che può aiutare a identificare le lacune delle procedure nelle organizzazioni.

Ad esempio, un server Web potrebbe apparire sicuro durante il primo passaggio di pen testing , ma non viene patchato per due mesi; un test successivo rivelerà il patch mancanti.

Escalation of privilege. L'escalation dei privilegi è uno dei metodi più comuni per ottenere l'accesso alle risorse. Gli aggressori cercano di risalire da un account ospite con pochi diritti a un account utente a un account con accesso amministrativo completo.

Il pen testing a blocchi quadrati imita ciò che un vero aggressore deve affrontare:

Black box. . il tester della scatola nera non è a conoscenza del sistema di destinazione e non è dotato di ulteriori informazioni sull'organizzazione, sull'architettura o sugli obiettivi.

Pertanto, i pen testing test a scatola nera si basano fortemente su risorse e informazioni rivolte al pubblico. Se il tester non è in grado di violare i dispositivi pubblici, allora i dispositivi interni non sono testati.

White box. Il test su scatola bianca è l'opposto del test su scatola nera: al tester viene dato pieno accesso a un intero ambiente per eseguire test, incluso potenzialmente il codice sorgente delle applicazioni.
Questo fornisce il set più completo di test ma può anche essere il più lungo e complicato.

Gray box. Il test della scatola grigia è come un attacco di un attore interno. Il tester ha una conoscenza minima di architettura e il livello di accesso di un account utente standard. Il test della scatola grigia consente test di risorse interne ed esterne.

Scanning. La scansione delle vulnerabilità è un atto più passivo dei test di penetrazione. Ad esempio, una scansione potrebbe determinare solo se una porta è

aperta su un frewall, mentre un test di penetrazione tenterà di sfruttare una porta aperta e connettersi alle risorse.

Penetration testing vs vulnerability. Rispetto ai test con pen testing , le scansioni di vulnerabilità sono un approccio passivo per garantire che dispositivi e sistemi siano aggiornati. Queste scansioni possono identificare porte aperte su dispositivi e frewalls, valutare se le regole di segregazione di rete e frewall funzionano come previsto e verificare se i sistemi dispongono delle ultime patch installate. Ecco i concetti di scansione delle vulnerabilità che dovresti conoscere:

1.5 Explain vulnerability scanning concepts

Passively test. Come indicato dal nome, il test passivo dei controlli di sicurezza tenta solo di identificarne i punti deboli o vulnerabilità nell'obiettivo da scansionare. A differenza di un test di penetrazione, che tenta di sfruttare una debolezza, un test passivo raccoglie semplicemente informazioni sul bersaglio.

Identify vulnerability. Diversi tipi di obiettivi presentano diverse vulnerabilità. I server Web potrebbero presentare vulnerabilità nell'esecuzione del codice e nell'accesso ai dati. Le vulnerabilità del firewall possono includere errori di configurazione in segregazione o vulnerabilità di accesso ai controlli di amministrazione del frewall.

Identify lack of security controls. Parte della scansione delle vulnerabilità consiste nell'identificare tutti i componenti che potrebbero mancare di controlli sicurezza. Un esempio è una rete Wi-Fi ospite aperta a tutti ma presente su una rete non è completamente separato dalle risorse di un'organizzazione. Un altro esempio è una cartella condivisa che tutti possono leggere e scrivere.

Identify common Misconfgurations. La scansione delle vulnerabilità può anche aiutare a trovare errori di configurazione comuni per i frewalls e altri dispositivi su una rete. Le configurazioni errate sono spesso semplici, come lasciare aperto l'account amministratore predefinito o non limitare Desktop remoto solo a coloro che richiedono l'accesso.

Intrusive vs non-intrusive. Nel cloud, è anche possibile configurare una posizione di archiviazione come pubblica quando deve essere privata, un errore di configurazione comune. In genere, le scansioni delle vulnerabilità non sono invadenti perché tentano solo di identificare un punto debole, non di sfruttarlo. Tuttavia, a seconda del sistema di destinazione, la scansione può inavvertitamente diventare invadente. Ad esempio, se il sistema di destinazione è in ascolto su una porta per una connessione, il

la scansione delle vulnerabilità potrebbe vedere la porta aperta e ritardare o negare la connessione di una risorsa legittima. Inoltre, il traffico aggiuntivo di scansioni di vulnerabilità può aggiungere alla quantità di dati i dispositivi di rete che devono lavorare, causando problemi per una rete già congestionata.

Credentialed vs non-credentialed. Come i test di penetrazione della scatola nera e della scatola grigia, è possibile eseguire una scansione delle vulnerabilità con o senza credenziali. Una scansione senza credenziali è la più semplice e veloce; riporta solo indietro
i servizi aperti sulla rete. Una scansione con credenziali va oltre tentando di connettersi a una risorsa con un set o un elenco di credenziali fornite prima della scansione. Questa scansione richiede di ottenere un elenco accurato di credenziali ma fornisce una migliore comprensione degli attacchi interni.

Poiché le scansioni delle vulnerabilità tentano di identificare solo se esiste un rischio, il tasso di falsi positivi può essere elevato. Ad esempio, se la scansione identifica le porte aperte utilizzate per un'applicazione critica, la scansione potrebbe segnalare che il dispositivo è vulnerabile. Tuttavia, perché l'applicazione
richieda che tali porte siano aperte e l'organizzazione ha adottato altre misure per mitigare il rischio delle porte aperte, il rapporto potrebbe essere un falso positivo.

False positive

Ogni vulnerabilità può avere diversi rischi o impatti associati. Non tutte le organizzazioni tratteranno ogni vulnerabilità allo stesso modo, altrimenti - diversi team di sicurezza potrebbero classificarli ciascuno con rischio separatamente e pianificare di mitigare il rischio o documentare il motivo per cui hanno scelto di non farlo.

Explain the impact associated with types of vulnerabilities

Race conditions . Una condizione di competizione si verifica quando un processo produce un risultato imprevisto a causa dei tempi. I flussi di condizioni Gara sono rari e sono difficili da testare perché sono spesso difficili da riprodurre su richiesta. Le vulnerabilità delle condizioni di gara possono spesso non essere rilevate per lunghi periodi di tempo, lasciando le organizzazioni a rischio.

ANCHE IN QUESTO CASO RIPORTIAMO LA PRESENZA DEI SOFTWARE RIAN E GO-DRY CHE TENDONO A CREARE CODICE SORGENTE A ERRORE ZERO. ERRORE ZERO SIGNIFICA ZERO VULNERABILITA' E ZERO RISCHI

Vulnerabilities due to:

End-of-life systems. I sistemi che superano la data di scadenza del fornitore in genere non ricevono più aggiornamenti di sicurezza o funzionalità. Quando una vulnerabilità o exploit in un'operazione di sistema o hardware identificato, potrebbe non essere possibile mitigarlo in dispositivi meno recenti e quindi le organizzazioni potrebbero dover tentare di aggiornare i sistemi o sostituire quelli vecchi hardware. Il rischio aumenta nel tempo.

IL FATTO CHE I SISTEMI NON PIU' SUPPORTATI SIANO FONTI DI RISCHIO SERVE SOLO A FAR VENDERE I SISTEMI NUOVI, CHE, PER ESEMPIO DEI SISTEMI OPERATIVI DEI COMPUTER, COMPORTANO L'ABBANDONO DI SOFTWARE FUNZIONANTI ANCHE DI TERZE PARTI, MENTRE, ESSENDO I SISTEMI OPERATIVI LANCIATI SUL MERCATO COLL'OBIETTIVO DI FARLI TESTARE AI CLIENTI, NON COSTITUISCONO UN VANTAGGIO DAL PUNTO DI VISTA DELLA SICUREZZA

Embedded systems. I dispositivi integrati in altri sistemi possono essere difficili da aggiornare. Per esempio, un dispositivo di produzione che ha un sistema operativo integrato potrebbe non essere sullo stesso programma di aggiornamento come altri sistemi gestiti dal team di sicurezza. Le organizzazioni potrebbero doverlo fare mettere in atto altre misure di sicurezza per mitigare i problemi, come il controllo o la disabilitazione della funzionalità.

Lack of vendor support. Se un'applicazione o un dispositivo non è più supportato o raramente riceve patch o aggiornamenti da parte del venditore, anche se non è alla fine della sua vita, diventerà di più nel tempo è più rischioso utilizzarlo man mano che vengono scoperte più vulnerabilità. Le organizzazioni potrebbero aver bisogno sostituire tali sistemi per ridurre il rischio.

IL FATTO CHE I SISTEMI NON PIU' SUPPORTATI SIANO FONTI DI RISCHIO SERVE SOLO A FAR VENDERE I SISTEMI NUOVI, CHE, PER ESEMPIO DEI SISTEMI OPERATIVI DEI COMPUTER, COMPORTANO L'ABBANDONO DI SOFTWARE FUNZIONANTI ANCHE DI TERZE PARTI, MENTRE, ESSENDO I SISTEMI OPERATIVI LANCIATI SUL MERCATO COLL'OBIETTIVO DI FARLI TESTARE AI CLIENTI, NON COSTITUISCONO UN VANTAGGIO DAL PUNTO DI VISTA DELLA SICUREZZA

Improper input handling. Le applicazioni e i siti Web che non gestiscono correttamente l'input dell'utente possono rendere il sito Web e i dati dietro di esso vulnerabili. Ad esempio, se un sito Web che utilizza un database SQL consente caratteri speciali senza prima analizzarli, è possibile eseguire un attacco di iniezione SQL per ottenere o eliminare i dati dal database.

SOLO LA MANCANZA DI INFORMAZIONE DEI CREATORI DI SITI HA PERMESSO CHE LA SQL-INJECTION FOSSE IN CIMA ALLA CLASSIFICA DEGLI ATTACCHI PER 15 ANNI COME RILEVATO DA OWASP. BASTAVA UTILIZZARE LA TECNICA DEL PREPARE STATEMENT IN CUI LA QUERY E' GIA' PRECOMPILATA E UTENTE E PASSWORD SONO SOLO DEI PARAMETRI, NON PERMETTENDO DI INSERIRE COMANDI DIVERSI

Improper error handling. Come per la gestione degli input, la gestione errata degli errori può influire sulla disponibilità di un'applicazione o sito Web. Gli errori ripetuti possono causare una perdita di memoria, un sovraccarico di flusso o altri problemi potrebbe causare tempi di inattività.

Misconfguration/weak confguration. L'errata configurazione o la debole configurazione di un dispositivo possono avere risultati drastici. Se un attaccante può ignorare un controllo di sicurezza a causa di una cattiva configurazione, quindi l'attaccante potrebbe essere in grado di assumere l'intera rete.

Default confguration. L'uso di una configurazione predefinita in genere ha lo stesso effetto di non avere alcun controllo di sicurezza posto a tutti. Le password e le informazioni di accesso predefinite per qualsiasi dispositivo o sistema possono essere trovate attraverso una rapida ricerca sul web.

Resource exhaustion. Gli attacchi di esaurimento delle risorse tentano di sfruttare un bug del software o un flusso di progettazione o inondare a sistema con un gran numero di richieste per arrestare il sistema o renderlo non disponibile per il tempo necessario per riavviarlo. Ad esempio, un utente malintenzionato può scaricare un file da un Web sito, non solo una volta, ma migliaia di volte, potenzialmente da migliaia di diversi client (clienti legittimi o fasulli).

Untrained users. Meno gli utenti sono consapevoli dei controlli di sicurezza, più è probabile che utilizzino il software impropriamente, innamorarsi degli attacchi di ingegneria sociale e fare altri errori.

PER QUESTO PUBBLICHEREMO QUESTO TESTO SUL NOSTRO SITO E CERCHEREMO DI PUBBLICIZZARLO CON OPPORTUNE AZIONI DI

MARKETING. LA CULTURA DELLA SICUREZZA DEVE ALLARGARSI A MACCHIA D'OLIO, ANCHE SE NON PROVOCA IMMEDIATAMENTE UN BUSINESS: I RITORNI CI SARANNO PER TUTII QUELLI CHE OPERANO CON COMPETENZA NEL SETTORE DELLA SICUREZZA

Improperly confgured accounts. Come le configurazioni predefinite, gli account che hanno password deboli o più privilegi del necessario sono vulnerabilità dei sistemi a cui possono accedere.

Vulnerable business processes. Anche la scarsa gestione dell'account utente, gli aggiornamenti di sicurezza, il controllo delle modifiche e altri processi aziendali possono essere una vulnerabilità. Anche una semplice lista di controllo può aiutare a prevenire un sistema diventando obsoleto e vulnerabile agli ultimi exploit.

Weak cipher suites and implementations. L'implementazione di suite di crittografia deboli in genere ha lo stesso effetto di non utilizzare alcuna sicurezza. Deboli le implementazioni di cifratura, potrebbero essere facilmente identificate da un utente malintenzionato e presentare vulnerabilità e exploit noti. I dati crittografati con queste cifre potrebbero quindi essere decifrati dagli aggressori.

CRIPTEOS 3001 HA UNA CRITTOGRAFIA SUPER-FORTE COME GIA' DETTO

Architecture/design weaknesses. Più l'espansione esiste nella progettazione di un sistema, più è facile dimenticarsene componenti o sistemi che non sono gestiti correttamente.

System sprawl/ undocumented assets
Inoltre, non documentando le risorse rendono difficile la pianificazione di aggiornamenti, pen test e valutazioni di vulnerabilità. Un'architettura o un progetto debole dietro un processo o un sistema può tradursi in ulteriori vulnerabilità.

New threats/zero day. Nuove minacce e attacchi zero-day sono difficili da pianificare. Anche i sistemi che sono gestiti e le patch aggiornate regolarmente sono vulnerabili a queste minacce.

Improper certificate and key management. Molti certificati e le loro chiavi proteggono i dati crittografati, sia che siano archiviati su un disco o in transito. La mancata corretta gestione di questi certificati e chiavi critiche può comportare che un aggressore possa avere pieno accesso ai dati.

I CERTIFICATI, CONNESSI ALLA CRITTOGRAFIA A CHIAVE PUBBLICA, DI CUI ABBIAMO VISTO I DIFETTI, POSSONO ESSERE FALSIFICATI E TUTTO IL CASTELLO DI CARTE CROLLA

Memory/buffer vulnerabilities

Memory leak. Una perdita di memoria provoca in genere un'applicazione che inizia a funzionare lentamente e infine si arresta in modo anomalo quando il sistema esaurisce la memoria disponibile.

MENTRE NEL LINGUAGGIO DI PROGRAMMAZIONE C LA MEMORIA VENIVA ALLOCATA E LIBERATA CON ISTRUZIONI MESSE DAL PROGRAMMATORE, NEI LINGUAGGI DI IV GENERAZIONE CI SONO IGLI "SPAZZINI COMUNALI" DEL GARBAGE COLLECTOR CHE LIBERANO LA MEMORIA IN AUTOMATICO QUANDO VOGLIONO LORO, QUESTO PUO' CREARE PROBLEMI. PIU' FACILE A PROGRAMMARE MA INSICURO

Integer overflow. Nelle applicazioni che usano numeri interi, è possibile sovraccaricare una variabile calcolando un numero superiore o inferiore a quello accettato dalla variabile. Come altre vulnerabilità delle applicazioni, ciò può causare il blocco o l'arresto anomalo del sistema se non era previsto l'overflow.

Buffer overflow. Come un overflow del numero intero, se un buffer di dati trabocca con più dati di quanto è stato dimensionato , può causare il blocco o l'arresto anomalo di un'applicazione. Il buffer overflow può essere prevenuto validando qualsiasi dato prima che venga scritto in memoria.

Pointer dereference. I puntatori all'interno del codice dell'applicazione sono proprio questo: puntare alla variabile che memorizza i dati. Una vulnerabilità che può de-referenziare il puntatore può far sì che la variabile memorizzi il tipo errato di dati, sia un valore nullo o che ne abbia altri l'impatto può causare un errore nell'applicazione.

DLL injection. Le DLL sono generalmente considerate affidabili dal sistema su cui sono in esecuzione. Iniettando una DLL, gli aggressori possono eseguire il loro codice all'interno dello spazio degli indirizzi di un processo attendibile, che consente loro di assumere facilmente il controllo del sistema sotto le sembianze del processo affidabile.

ADESSO LE DLL SONO SOSTITUITE DAI FRAMEWORK, ENCICLOPEDIE LIBRERIA CON TUTTO LO SCIBILE INFORMATICO DISPONIBILE PER QUEL LINGUAGGIO DI PROGRAMMAZIONE. A PARTE CHE FRAMEWORK

SUCCESSIVI SONO INCOMPATIBILI IN AMBIENTE MICROSOFT, LA NECESSITA' DI ACCEDERE A QUESTE LIBRERIE, INSTALLATE SUI COMPUTER, HA OBBLIGATO A COMPILARE NON PIU' NEL BLINDATO LINGUAGGIO OGGETTO, MA IN UN LINGUAGGIO CHE PUO' RIPORTARE AL CODICE SORGENTE UTILIZZANDO DECOMPILATORI ANCHE GRATUITI. PER OPPORSI A QUESTO USANO TECNICA OFFUSCAMENTO

2. Technologies and Tools

2.1 Install and confgure network components, both hardware-and software-based, to support organizational security

Questa è una sezione pratica, quindi dovrai installare e configurare le risorse. Non è necessario gestire le decisioni di progettazione ma è necessario conoscere i dettagli dell'implementazione della tecnologia data. Naturalmente, queste tecnologie sono indipendenti dal fornitore, quindi non è necessario acquisire familiarità con tutte le varie implementazioni del fornitore.

Firewall Un firewall è un dispositivo hardware o una soluzione software che controlla e quindi consente o rifiuta comunicazioni di rete. Conoscere i seguenti concetti di firewall:

ACL. Un elenco di controllo di accesso (ACL) è una singola voce in un firewall che determina se specifica la comunicazione è consentita (consentita) o negata (bloccata).

Application-based vs network-based. Un firewall basato su applicazioni è specializzato a proteggere le vulnerabilità specifiche dell'applicazione. Ad esempio, un firewall basato sull'applicazione è in grado di proteggere i server di database dagli attacchi SQL injection. Se configurato in modalità attiva, i firewalls basati su applicazioni possono bloccare il traffico dannoso; in modalità passiva, registrano solo attività dannose. Un firewall basato su rete è un firewall generale che si trova a livello di rete e ispeziona il traffico di rete senza conoscenza specifica dell'applicazione. Permette o nega traffico basato su regole predefinite.

Stateful vs stateless. Un firewall con stato controlla le comunicazioni e mantiene la conoscenza delle connessioni. Un firewall con stato eccelle nell'identificare il traffico malevolo ma non può gestire tanto il traffico quanto un firewall senza stato. Un firewall senza stato consente o nega comunicazione basata su origine, destinazione, protocollo o porta. Un firewall senza stato eccelle nella gestione di grandi volumi di traffico. Implicit deny. Un rifiuto implicito è una dichiarazione in un firewall che impone che tutto il traffico non lo sia consentito o negato in ACL esistenti è negato (o trattato come sospetto).

VPN concentrator Un concentratore VPN è un dispositivo che facilita le connessioni VPN. Ascolta le connessioni da client, autentica le connessioni e quindi fornisce l'accesso alla rete.

Remote access vs. site-to-site. Una VPN di accesso remoto consente agli utenti di connettersi a rete dell'organizzazione da una postazione remota. Una VPN da sito a sito consente a due siti di connettersi l'un l'altro. Ad esempio, una VPN da sito a sito potrebbe connettersi a una filiale con un asso principale.

IPSec. Una VPN IPSec utilizza IPSec per le connessioni. I dispositivi richiedono un client VPN per connettersi la rete (che è il principale svantaggio). Una volta connessi, i client sono solo un altro dispositivo sulla rete e non si rendono conto che sono diversi da un dispositivo connesso localmente.

Split tunnel vs full tunnel. Un tunnel diviso consente agli utenti di connettersi a una VPN e accedere risorse su quella rete mantenendo anche la connettività a Internet o altra Rete. Ad esempio, se sei a casa, puoi VPN alla tua rete aziendale mentre mantenendo comunque l'accesso a Internet tramite la connessione Internet domestica. Un tunnel completo è uno che invia tutte le comunicazioni tramite la VPN. Ad esempio, se si è connessi a una VPN tunnel completa e vai a un sito Web basato su Internet, la richiesta verrà inviata la rete VPN, non la rete locale.

TLS. Una VPN TLS funziona tramite la porta TCP 443 e può essere connessa tramite un browser (come attraverso un portale) o tramite un client VPN. Una VPN TLS semplifica la configurazione del firewall perché è necessaria una sola porta. Può anche essere utile per le organizzazioni che lo desiderano utilizzare solo un portale ed evitare l'implementazione e la manutenzione del software client VPN.

Always-on VPN. Storicamente, le connessioni VPN sono state avviate su richiesta: quando si voleva connettersi alla rete aziendale, ci si connetteva manualmente. Con una VPN sempre attiva, il tuo computer è sempre connesso alla tua rete aziendale. Succede automaticamente quando il computer è connesso a Internet. Una VPN sempre attiva fornisce un esperienza migliore per l'utente e può aumentare la produttività mantenendo le persone sempre connesse.

Tunnel mode. La modalità tunnel è la modalità VPN IPSec predefinita. Con questa modalità, l'intera comunicazione è protetta da IPSec.
Transport mode. La modalità di trasporto viene utilizzata principalmente per le comunicazioni peer-to-peer, come quando un dispositivo client si connette in remoto a un server (come l'utilizzo di RDP). La modalità di trasporto può migliorare la comunicazione peer-to-peer crittografandola.

Authentication Header (AH). Questo protocollo prevede l'autenticazione dell'intero pacchetto. Non fornisce la riservatezza dei dati.

Encapsulating Security Payload (ESP). Questo protocollo prevede la riservatezza dei dati e autenticazione. L'autenticazione avviene solo per la parte del datagramma IP.

NIPS. Un sistema di prevenzione delle intrusioni di rete (NIPS) è un tipo di IDS che si trova all'interno della rete per proteggere la rete dal traffico dannoso. È una soluzione attiva che può bloccare alcuni tipi di comunicazioni dannose. Un sistema di rilevamento delle intrusioni di rete (NIDS) è un tipo di ID che vengono inseriti all'interno della rete per monitorare le comunicazioni di rete per rilevare eventuali comportamenti malware . È una soluzione passiva che fornisce rilevamento e allerta.

Signature-based. Quando si monitora il traffico di rete, è comune un approccio basato sulla firma. Le firme sono pre-create sulla base di schemi di attacco noti. Mentre questo approccio è comune ed efficace, ha dei limiti. Ad esempio, non è in grado di rilevare attacchi zero-day.

Anomaly. Con il rilevamento basato su anomalie, la soluzione crea la base organizzativa. Quando la tratta è troppo lontana dalla linea di base, è possibile intraprendere azioni o può essere genrato un avviso. Le linee di base sono di fondamentale importanza per rilevare anomalie. Le linee di base sembrano spesso a schemi di traffico, utilizzo della larghezza di banda e dettagli di comunicazione (protocolli e porte).

Heuristic/behavioral. Come il rilevamento basato sull'anomalia, il rilevamento basato sull'euristica sembra per traffico al di fuori della norma, basato su modelli di utilizzo stabiliti nella propria organizzazione. Ma invece di fare affidamento su baseline, il rilevamento euristico prende in considerazione il comportamento
fattori come la velocità con cui si svolgono le attività, la posizione da cui le attività si verifica e il tipo di hardware o software utilizzato in una richiesta.
Inline vs. passive. Una soluzione inline è situata sulla rete, spesso tra due chiavi punti di distribuzione. Una soluzione inline controlla il traffico in tempo reale. Una soluzione passiva riceve traffico tramite il mirroring o un altro metodo e viene spesso utilizzato solo a scopo di rilevamento.

In-band vs out-of-band. In-band è sinonimo di inline. Fuori banda è anche sinonimo con passivo.

Rules. Le regole vengono utilizzate per determinare se il traffico è dannoso o deve essere consentito e se genera un avviso. Le regole sono precise e dettagliate. Puoi

includere fonti, destinazione, porti e altre opzioni. Una regola può attivare un avviso o un'altra azione. Per ad esempio, potresti decidere di non agire su ogni scansione delle porte. Ma potresti agire se vedi un indirizzo IP interno che comunica tramite FTP a un Paese in cui non si svolgono attività commerciali.

Analytics. Le soluzioni IPS e IDS possono generare molti avvisi. Spesso ci sono informazioni sovraccarico e avvisi vengono ignorati. Le soluzioni utilizzano l'analisi per dare un senso al grande influsso di dati con l'obiettivo di mostrare ai team di sicurezza solo ciò che vogliono o devono vedere. Due i concetti chiave sono:

False positive. I falsi positivi sono avvisi che indicano che si sta verificando un attacco quando non ce n'è uno. Avere troppi di questi può essere pericoloso perché le squadre iniziano ignorandoli e poi perdere un vero avviso.

False negative. Un falso negativo è quando il traffico dannoso è considerato benigno. I falsi negativi sono pericolosi perché il traffico malevolo viene spesso ignorato e ritenuto sicuro.

NIPS/NIDS

Router. Un router è un dispositivo basato su hardware o software che consente la comunicazione tra diverse reti. Nelle reti odierne, molti router basati su hardware sono multiuso dispositivi ed eseguire anche operazioni di commutazione e firewall.

Switch. Uno switch è un dispositivo basato su hardware o software che collega insieme computer o altri switch. Gli switch possono essere dispositivi autonomi che forniscono solo funzionalità di switching o possono essere abbinati a funzionalità di routing e frewall.

Proxy. Un proxy è un'appliance hardware o un software utilizzato per effettuare richieste per conto di utenti, indipendentemente dal fatto che gli utenti passino da una rete interna a Internet o da Internet a una risorsa interna.

ACLs. Gli ACL su un router forniscono meno funzionalità degli ACL su un firewall, sebbene essi può bloccare o consentire parte della stessa tratta. Gli ACLS sui router possono essere utilizzati per gli apolidi decisioni di ispezione per bloccare il traffico specifico quando necessario ma non sono destinate a farlo sostituire la funzionalità firewall.

Antispoofng. Gli aggressori a volte provano a mascherare il loro vero indirizzo di origine tramite spoofng altri indirizzi. I router possono bloccare i tentativi di spoofng

utilizzando gli ACL. Mentre è comune usare ACL per l'antispoofng, sarebbe in aggiunta all'antispoofng su un frewall.

Port security. Per impostazione predefinita, è possibile connettere qualsiasi computer a qualsiasi porta su uno switch. Con sicurezza della porta, si configura lo switch per accettare connessioni solo da client noti. Per esempio, una porta può essere configurata per consentire solo un client con un indirizzo MAC specifico. Se un client con un diverso indirizzo MAC tenta di connettersi alla porta, la connessione è negata. È possibile configurare tutte le porte su uno switch per la sicurezza delle porte (whitelist dei client noti).

La sicurezza delle porte è una funzione opzionale che migliora la sicurezza della rete

Layer 2 vs. Layer 3. La commutazione tradizionale opera sul livello 2, che si basa sulla destinazione Indirizzi MAC. Il routing di livello 3 si basa sugli indirizzi IP di destinazione. La maggior parte degli switch oggi forniscono funzionalità a livello 2 e livello 3, con ogni livello che gestisce i compiti appropriati (per esempio, livello 3 che gestisce la comunicazione da VLAN a VLAN).

Loop prevention. In una rete di livello 2, hai un ciclo se ci sono più percorsi tra due endpoint. In un tale scenario, i pacchetti vengono reindirizzati e possono verificarsi tempeste di trasmissione. I metodi principali per prevenire i loop sono l'utilizzo di Spanning-Tree Protocol (STP) e Rapid Spanning Tree Protocol (RSTP).

Flood guard. Un inondazione può verificarsi quando una tabella MAC viene forzata fuori da uno switch. Senza la Tabella MAC, gli switch devono inviare i pacchetti su tutte le porte invece che solo a una porta prevista.
Per ridurre al minimo le possibilità di inondazione, è possibile implementare la sicurezza delle porte.

Forward and reverse proxy. Un proxy forward viene spesso utilizzato per il proxy delle richieste Web per client su una LAN. Tutto il traffico Internet passa al proxy. Il proxy serve le richieste tramite cache o esce su Internet per richiedere il sito Web. Per i server Web, tutte le richieste dalla tua azienda sembrano provenire da un singolo computer, il proxy forward. Inoltrare i proxy migliorano la sicurezza perché possono essere configurati con filtri per siti dannosi, per siti basati su categorie e per comunicazioni non valide. I proxy inversi ti consentono di rendere disponibili risorse interne a Internet. Ad esempio, potresti usare un proxy contrario per consentire agli utenti di accedere al tuo sito Intranet o di controllare la posta elettronica da casa. Un proxy inverso migliora la sicurezza controllando le richieste valide, eseguendo

l'autenticazione opzionale degli utenti prima di passare la richiesta a una risorsa interna e di utilizzare funzionalità anti-malware.

Transparent. Un proxy trasparente si trova in linea sulla rete ed esegue le funzioni di proxy senza che tu o il tuo dispositivo ne siate a conoscenza. Con un proxy non trasparente, i browser è configurato per contattare il server proxy (e tali configurazioni possono essere applicate). Con un proxy trasparente, il proxy si verifica senza una configurazione del browser.

Application/multipurpose. Un proxy applicazione è un proxy specializzato, spesso utilizzato per distribuzioni basate su scenari anziché scenari di navigazione Web o di pubblicazione Web generici.
Alcuni proxy dell'applicazione offrono funzionalità Single Sign-On (SSO), altri forniscono funzionalità proxy reverse e alcune sono legate a soluzioni software specifiche.

Scheduling. La pianificazione del bilanciamento del carico è il metodo mediante il quale le richieste vengono indirizzate a server back-end. Esistono 2 metodi comuni: Un bilanciamento del carico è un dispositivo di rete (basato su hardware o software) che ascolta le richieste in entrata e quindi indirizza tali richieste ai server di back-end, spesso in modo tale bilancia le richieste su più server back-end in modo uniforme. Ad esempio, se hai un bilanciamento del carico di fronte a 5 server Web, la prima richiesta potrebbe essere indirizzata a Server1, la seconda richiesta a Server2 e così via.

Load balancer

Afnity. Supponiamo di avere 3 server Web e un bilanciamento del carico. Invio in entrata la richiesta a un server Web casuale potrebbe creare problemi per alcune applicazioni Web. Per esempio, se la connessione iniziale ha un utente accede all'applicazione web e a quella dell'utente la richiesta successiva viene inviata a un altro server Web, tale server Web non sarà a conoscenza dell'utenteche accede e richiederà all'utente di accedere nuovamente. Afnity risolve questo problema mantenendo l'utente su un singolo server per tutta la durata dell'utilizzo dell'applicazione Web. Puoi fare questo per indirizzo IP di origine (sebbene ciò abbia dei limiti, ad esempio un'intera azienda potrebbe utilizzare un proxy o NAT e tutti finiranno sullo stesso server quando accederanno all'applicazione web). Esistono anche altri metodi afnity, come l'uso dei cookie.

Round-robin. Il round robin è uno dei metodi di bilanciamento del carico più semplici. Si inoltra la prima richiesta al primo server, la seconda richiesta al secondo server, ecc. Quando raggiunge l'ultimo server, ricomincia da capo. Altre

implementazioni round robin ponderato: ai server back-end viene assegnato un peso per bilanciare più uniformemente le richieste attraverso di loro.

Active-passive. Con il bilanciamento del carico attivo-passivo, un bilanciamento del carico esegue il carico di bilanciamento e uno separato è in standby. Il bilanciamento del carico in standby esegue il bilanciamento del carico solo se il bilanciamento del carico primario non è disponibile o presenta problemi di prestazioni.

Active-active. Nel bilanciamento del carico attivo-attivo, ci sono due o più bilanciatori del carico e tutti loro partecipano attivamente al bilanciamento del carico, ciascuno gestendo una parte delle richieste.
Una configurazione attivo-attiva offre prestazioni migliori rispetto a una configurazione attivo-passiva; tuttavia, si perde flessibilità per la manutenzione. Ad esempio, se vuoi aggiornare il software su uno dei sistemi di bilanciamento del carico, è necessario innanzitutto scaricarlo (ovvero consentire clienti attuali per perfezionare senza problemi le loro sessioni esistenti mentre le nuove sessioni sono dirette ad altri nodi), mentre con una strategia attiva-passiva è possibile aggiornare il passivo bilanciamento del carico, passare ad esso il trafc e quindi aggiornare il bilanciamento del carico primario.

Virtual IPs. Nel bilanciamento del carico, un indirizzo IP virtuale viene utilizzato per indirizzare tutte le richieste. Per esempio potresti avere una voce DNS per il nome di dominio completo del tuo sito Web che punta a un IP virtuale sul bilanciamento del carico. Il bilanciamento del carico è configurato per il bilanciamento del carico agli IP privati sull'individuo server web. I singoli server Web non sono configurati con l'IP virtuale.

SSID. Service Set Identifer (SSID) è il modo in cui viene identificato un punto di accesso wireless. È un identificatore univoco che facilita la comunicazione sulla rete. Può contenere un testo ed essere di lunghezza massima di 32 caratteri.

MAC fltering. Una funzione opzionale di molti punti di accesso wireless è quella di filtrare per indirizzo MAC. Con il MAC fltering, è possibile specificare gli indirizzi MAC che possono unirsi alla rete.
Questo è stato originariamente introdotto come funzionalità di sicurezza, ma ne offre una quantità molto limitata di sicurezza. Molti sistemi operativi ti consentono di impostare il tuo indirizzo MAC; impostandolo su indirizzo di un client valido, potresti potenzialmente ottenere l'accesso alla rete (presumendo il

passphrase era anche noto). Gli indirizzi MAC vengono trasmessi con ogni pacchetto, quindi è possibile trovare facilmente gli indirizzi MAC anche catturando il traffico.

Signal strength. La potenza di un segnale wireless viene misurata in decibel milliwatt (dBm). Un segnale più forte fornisce prestazioni migliori. Se il segnale è troppo debole, potresti non essere in grado di connetterti o le prestazioni potrebbero essere spaventose.

Band selection/width. Le reti wireless spesso offrono più bande. Per esempio tu potresti avere una banda a 2,4 GHz e una banda a 5,2 GHz. La banda da 2,4 GHz è adatta per portata maggiore ma offre meno prestazioni. La banda da 5,2 GHz è adatta per spazi aperti e offre le migliori prestazioni della categoria. A volte, puoi cambiare banda se uno è pesante, congestionato.
Un punto di accesso è un dispositivo (di solito hardware, sebbene possa essere un software) che viene utilizzato per fornire l'accesso a una rete (di solito una rete wireless). Ci sono molti importanti articoli di configurazione in un punto di accesso:

Access point
Antenna types and placement. Esistono alcuni tipi di antenne, ognuna con differenti caratteristiche. Ad esempio, un'antenna omnidirezionale fornisce una copertura a 360 gradi;
questi sono i più comuni in uso nelle case e spesso. Installazioni più grandi, come ad esempio su un campus, potrebbe utilizzare più antenne direzionali che puntano tutte verso un'antenna centro omnidirezionale. Il posizionamento delle antenne è importante per la copertura e l'importanza complessiva. Per un ambiente universitario, si desidera massimizzare la linea di visuale tra le antenne. In una casa a due piani, vuoi centralizzare l'antenna il più possibile. In un grande edificio spesso, dovresti posizionare le antenne sul soffitto e distanziate per garantire una copertura adeguata.

Fat vs thin. I punti di accesso sottili sono entry-level e hanno set di funzionalità limitati o non possono essere configurati perché fanno parte di un sistema più grande gestito centralmente o scaricato altrove attività chiave. Gli access point offrono altre funzionalità avanzate che si vedono in genere negli ambienti aziendali. Anche i punti di accesso completamente autonomi sono punti di accesso importanti.

Controller-based vs standalone. Le reti wireless semplici hanno un punto di accesso autonomo ; non richiede altri dispositivi e altri dispositivi non lo richiedono. Ambienti più grandi richiedono molti punti di accesso wireless. Ad esempio, un edificio con 250 punti di accesso wireless può richiedere molto tempo per la gestione; l'utilizzo di un sistema di controllo centralizzato semplifica la gestione di tutti i punti

di accesso. Ad esempio, se si desidera effettuare una configurazione
cambiare tra tutti gli AP, puoi farlo da un sistema di gestione centrale.

Aggregation. L'aggregazione è una funzionalità di base delle soluzioni SIEM. Una soluzione SIEM raccoglie tutti i file di registro; l'obiettivo è avere tutto nel SIEM.

Correlation. Quando la tua soluzione SIEM ha informazioni da una varietà di fonti, è necessario un modo per correlare gli eventi. Ad esempio, se un utente accede alla propria stazione di lavoro client, per scaricare un file da un sito Web e quindi trasferirlo in un servizio di archiviazione basato su cloud, è necessario un modo per collegare quegli eventi in un singolo incidente o catena di azioni.
Senza correlazione, è difficile vedere il quadro generale di ciò che è emerso. Molti soluzioni SIEM per la correlazione. Alcune altre correlazioni usando l'apprendimento automatico e intelligenza artificiale; e altre correlazioni anche basate sul cloud.

Automated alerting and triggers. Oltre ad essere un repository di informazioni, un soluzione SIEM può anche generare avvisi basati su trigger o attività specifiche di cui informare i team attività quasi in tempo reale (anche se a causa di problemi di prestazioni, gli avvisi a volte sono in ritardo di alcuni minuti).
Una soluzione di sicurezza delle informazioni e di gestione degli eventi (SIEM) è un repository centralizzato dei tuoi registri e attività. Ad esempio, potrebbe contenere i log degli eventi del server, i log di accesso e avvisi generati da un fornitore cloud. Molte soluzioni SIEM offrono una ricerca avanzata, reportistica e analisi dei dati.

SIEM

Time synchronization. La sincronizzazione dell'ora è importante su una rete. Dal punto di vista SIEM, è di fondamentale importanza, soprattutto per la correlazione. Se l'orologio su un server Web è avanti di qualche minuto rispetto all'orologio su un server di database, potresti avere problemi correlati agli eventi.

Event deduplication. La deduplicazione aiuta a migliorare l'efficienza della memorizzazione delle informazioni. Esso è comunemente usato dalle piattaforme di archiviazione. Viene anche utilizzato dalle soluzioni SIEM per unire identici avvisi e per ridurre la quantità di memoria richiesta per archiviare i dati di registro.

Logs/WORM. In un ambiente ad alta sicurezza, è possibile utilizzare write once read many (WORM) archiviazione per garantire che i dati non vengano mai sovrascritti, sia accidentalmente che intenzionalmente. A volte, è necessario farlo per motivi di conformità o di controllo. Altre volte, potresti farlo
questo per motivi di sicurezza. Senza l'archiviazione WORM, è necessario disporre di un solido backup in atto per assicurarti di non perdere i dati.

USB blocking. Molte soluzioni DLP possono bloccare l'uso di porte USB per supporti rimovibili. Ciò elimina la possibilità che un utente prenda dati sensibili al di fuori dell'azienda su un unità portatile. Il blocco dell'uso di USB è importante, soprattutto se non hai modo di farlo monitorare e bloccare la copia di dati potenzialmente sensibili su unità portatili.

Cloud-based. Mentre le soluzioni DLP inizialmente proteggevano solo i dati locali, lo sono espandendosi rapidamente nel cloud. Man mano che le organizzazioni trasferiscono i dati nel cloud, hanno bisogno di stesse protezioni DLP che hanno in loco; in alcuni casi, le organizzazioni desiderano una protezione estesa per il cloud. Le soluzioni DLP basate su cloud si integrano con il cloud pubblico i fornitori di scansionare e proteggere i loro servizi di archiviazione e altri servizi compatibili.

CON CRIPTEOS3001 I DATI NEL CLOUD SONO SICURI, I GESTORI DEL CLOUD NON HANNO LA CHIAVE PER DECRIPTARLI. COSI' PUO' ESSERE SCELTO IL TIPO DI CLOUD E DI FORNITORE PIU' VANTAGGIOSO ECONOMICAMENTE

Email. DLP, come riferito alla posta elettronica, è un servizio che controlla la posta in entrata e in uscita per dati specifici, in particolare dati privati o personali che la tua organizzazione non desidera inviare via email o non desidera essere inviato a Internet. Quando rileva e-mail specifiche, la soluzione DLP può bloccare l'e-mail, registrare violazioni, informare il team di sicurezza o accettarne altre azioni. Gli elementi comuni che vengono controllati includono numeri di previdenza sociale, carta di credito, numeri di conto e altre informazioni di identificazione personale.

La prevenzione della perdita di dati (DLP) è un servizio che verifica l'uso improprio dei dati, spesso concentrandosi sui dati abbandono dell'azienda tramite e-mail, trasferimento tramite fle o altri metodi. DLP è più comunemente associato con la posta elettronica, ma viene utilizzato anche per database e intranet. Molte tecnologie DLP può bloccare l'uso improprio dei dati (come l'inserimento di informazioni identificative personali dei clienti in SharePoint). Inoltre, le soluzioni DLP possono spesso proteggere automaticamente le informazioni crittografandole o l'applicazione di altri metodi di protezione dei dati, ad esempio mediante la gestione dei diritti digitali.

DLP

Dissolvable vs permanent. Un agente dissolvibile viene scaricato e installato quando l'utente tenta di accedere alla rete; l'agente esegue i controlli e quindi viene rimosso. Un agente permanente (o persistente) è un agente tradizionale che è installato e

rimane su un computer indefinitamente. È necessario gestire la distribuzione e la manutenzione di agenti permanenti, il che è un aspetto negativo.

Host health checks. Come parte dell'accesso a una rete protetta da NAC, il dispositivo deve superare un controllo dello stato dell'host. I controlli sono configurabili. Controlli semplici potrebbero comportare la verifica se l'host ha gli ultimi aggiornamenti di sicurezza e un prodotto antivirus in esecuzione. I controlli avanzati potrebbero apparire più approfonditi, ad esempio se il computer ha l'ultimo definizioni antivirus, patch di sicurezza specifiche o una voce di registro specifica di Windows, oppure se un utente specifico ha effettuato l'accesso.

Agent vs agentless. Alcune soluzioni NAC non utilizzano agenti. Ad esempio, Microsoft ha offerto una soluzione NAC integrata con Active Directory e in grado di eseguire controllo senza un agente. Con un agente, è spesso possibile eseguire controlli più approfonditi. Inoltre, il controllo iniziale può essere più rapido rispetto alla necessità di installare un agente dissolvibile o di avere un agente senza agente scansione eseguita. Tuttavia, gli agenti richiedono un sovraccarico di gestione per la distribuzione, gli aggiornamenti e la manutenzione.

Spam flter. Un filtro antispam è un servizio che controlla la posta elettronica in entrata e in uscita per verificare la presenza di spam.
Esistono molti metodi di rilevamento anti-spam e molti filtri di spam utilizzano diversi metodi per massimizzare la loro efficacia. Un filtro antispam di solito si trova nella DMZ in modo che lo spam non raggiunge la rete interna.

DLP. DLP, in relazione a un gateway di posta elettronica, controlla i messaggi di posta elettronica in entrata e in uscita per dati specifici, in particolare dati privati o personali che l'organizzazione non desidera inviare tramite la posta elettronica o non desidera essere inviata a Internet. Una soluzione DLP al gateway di posta spesso controlla solo le e-mail in uscita su Internet e le e-mail in entrata da Internet ma potrebbe non controllare la posta elettronica interna (da utente a utente).
Il controllo dell'accesso alla rete (NAC) è un servizio che garantisce che i client di rete soddisfino i requisiti minimi prima di essere autorizzati sulla rete. Ad esempio, una soluzione NAC potrebbe controllare un computer per vedere se ha un software antivirus aggiornato, ha le ultime patch di sicurezza o è in esecuzione una versione legacy di un sistema operativo. Se tutto è andato a buon fine, il client può unirsi alla rete. In caso contrario, al client viene negato l'accesso alla rete o viene indirizzato a una rete di riparazione per il download patch di sicurezza, ottenere gli ultimi aggiornamenti antivirus o installare il software di sicurezza necessario.
Un gateway di posta è un dispositivo che invia e riceve e-mail. Spesso, sul gateway

viene utilizzato un gateway di posta bordo di una rete per migliorare la sicurezza dell'ambiente di posta elettronica. Può autenticare e convalidare il traffico prima che il traffico raggiunga i server di posta interni.
NAC
Mail gateway
EncryptionServer e gateway di posta elettronica possono crittografare le comunicazioni. Mentre l'impostazione predefinita la configurazione tra diversi host di posta elettronica non crittografa le comunicazioni, è possibile scegliere di crittografare la comunicazione con partner specifici o domini specifici o di crittografare tutto quando possibile. La crittografia può anche essere richiesta. Ad esempio, alcuni i gateway supportano la crittografia della posta elettronica quando un messaggio di posta elettronica soddisfa criteri specifici, come contenere una parola come "privato" nell'argomento).

Un bridge è un dispositivo di rete che collega due o più reti insieme. Quando un router collega le reti insieme, quelle reti rimangono separate. Ma quando un ponte collega reti, diventano un'unica rete. Uno switch è un bridge multiporta con alcuni potenziali caratteristiche che un semplice bridge non offre, come la separazione hardware delle porte.

Acceleratori SSL / TLS. Gli acceleratori SSL e TLS sono dispositivi che mirano a migliorare le prestazioni dei server Web trasferendo le operazioni crittografiche all'acceleratore. Inoltre, molti acceleratori possono ispezionare il traffico in entrata e bloccare il traffico dannoso.

Decifratori SSL. I decodificatori SSL decodificano il traffico crittografato e spesso lo ispezionano e bloccano il traffico dannoso. Questi sono come acceleratori SSL ma spesso non sono progettati per migliorare il web server prestazione come obiettivo primario.

Gateway multimediale. Un gateway multimediale è un dispositivo che traduce in genere flussi multimediali diversi su una rete di telefonia.
Modulo di sicurezza hardware (HSM). Un modulo di sicurezza hardware è un dispositivo dedicato alla creazione e gestione delle chiavi digitali utilizzate in infrastrutture a chiave pubblica, infrastrutture cloud e altri scenari. Un HSM è considerato un must per le organizzazioni in cui la sicurezza è massima importanza. Un HSM viene in genere utilizzato nelle grandi aziende e raramente viene utilizzato in piccoli ambienti a causa della complessità e dei costi.
Bridge
SSL/TLS accelerators

SSL decryptors
Media gateway
Hardware security
module (HSM)

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization

Questa sezione dell'esame si concentra sul test della sicurezza di una rete esistente. Dovresti conoscere gli strumenti e i metodi in modo da poter scegliere uno strumento o un metodo appropriato in base ai requisiti e agli obiettivi.

Network scanners

Protocol analyzer .Un analizzatore di protocollo, spesso chiamato sniffer o utilità di acquisizione di pacchetti, è uno strumento per catturare e analizzare le comunicazioni di rete. È possibile eseguire un analizzatore di protocollo su un computer, telefono cellulare o molti altri dispositivi. È inoltre possibile utilizzare un analizzatore di protocollo per analizzare i pacchetti catturati, come pacchetti di una sessione precedente.

Wireless scanner .Uno scanner di rete esegue la scansione di una rete o di una serie di dispositivi per individuare porte e tipi specifici delle applicazioni Web, scoprire se i dispositivi rispondono e individuare le vulnerabilità.
Gli scanner wireless cercano reti wireless nel raggio d'azione, siano esse nascoste o tutti visibili. Riportano informazioni di alto livello sulle reti, come gli SSID, il segnale forza, produttore, indirizzo MAC e canale.

Cracker wireless. Un cracker è uno strumento che tenta di ottenere l'accesso a una rete wireless senza autorizzazione, ad esempio, tentando di decifrare le chiavi o forzare la passphrase.

Rogue system detection. Un dispositivo canaglia è un dispositivo sconosciuto e non autorizzato che è collegato alla rete. Essere in grado di rilevarli e rimuoverli è essenziale perché possono essere dannosi o creare problemi sulla rete. Molti scanner possono aiutare a rilevare sistemi canaglia con funzionalità speciali. Altre volte, è possibile farlo manualmente confrontando informazioni sul sistema operativo, versioni e servizi in esecuzione.

Network mapping. La mappatura di una rete implica la ricerca di tutti i dispositivi sulla rete e il modo in cui sono collegati. Spesso, un esercizio di mappatura della rete termina con una serie di diagrammi che mostrano tutti i dispositivi e la connettività.

Steganography tools
Honeypot
Password cracker .Un cracker di password tenta di convertire le password con hash in testo normale. Può funzionare contro sistemi operativi, directory, database o altri sistemi che memorizzano le password nel formato hash. I cracker di password vengono generalmente utilizzati in un modello offline, in esecuzione per un lungo periodo di tempo contro gli hash.

CON CRIPTEOS 3001 NESSUNO VIOLA LA CHIAVE

Vulnerability scanner . Uno scanner di vulnerabilità viene utilizzato per individuare patch mancanti, vulnerabilità note e configurazioni insicure su una rete, su un host o su una serie di dispositivi. Viene aggiornato regolarmente a espandere il numero di vulnerabilità che può rilevare. Gli scanner vengono spesso utilizzati nei pen testing e I team IT interni a volte li usano per verificare la vulnerabilità della rete.

Confguration compliance scanner. Uno scanner di conformità della configurazione è come uno scanner di vulnerabilità, ma invece di cercare vulnerabilità, cerca le impostazioni di configurazione specifiche dettate dall'utente. Per esempio, uno scanner di conformità della configurazione può determinare se i server web di un'organizzazione sono configurati in conformità con i suoi standard.

Exploitation frameworks. I framework di sfruttamento sono strumenti per facilitare gli exploit. Ti consentono di scegliere l'exploit e cosa succede dopo aver ottenuto il controllo del dispositivo tramite l'exploit. Ad esempio, un framework potrebbe tentare di sfruttare una vulnerabilità di flusso noto oltre il flusso. Questi strumenti sono utili per hacker ma anche per team di sicurezza IT interni per testare i loro sistemi.
Quando è necessario smaltire i dispositivi di archiviazione, è necessario un modo per cancellare in sicurezza i dati.

Data sanitization tools . Gli strumenti di disinfezione dei dati possono cancellare in modo sicuro i dati in modo che non possano essere recuperati. Molti degli strumenti sovrascrivono i dati in più passaggi, a volte con dati casuali. Con ogni ulteriore passaggio di sovrascrittura, la cancellazione diventa più permanente e quindi più sicura. Oltre a disinfettare i dati, puoi anche sterilizzare interi dischi rigidi.

Steganography tools . Con uno strumento di steganografia, è possibile nascondere i dati all'interno di altri file (file carrier). Comunemente, i file di immagini e video vengono utilizzati per nascondere i dati. È buona norma scegliere un vettore aereo con dimensione appropriata per i dati che si desidera nascondere. Ad esempio, se si desidera nascondere 500 KB di dati, dovresti avere un file di almeno 5 MB. Se si tenta di nascondere 500 KB di dati in un operatore File che era originariamente di 10 KB, potrebbe sollevare sospetti. Ad esempio, se apri un video di grandi dimensioni fuggito solo per scoprire che il video dura pochi secondi, sembrerebbe strano, perché ci si aspetterebbe che il video sia più lungo poiché il file è grande.
Un honeypot è un sistema informatico configurato per attirare gli aggressori. Puoi usare un honeypot per capire se una rete è sotto costante sorveglianza o attacco. Distribuire un honeypot può fornire informazioni sui tipi di attacchi che la rete sta affrontando.

Backup utilities. Le utility di backup eseguono copie dei dati, in genere su un dispositivo di archiviazione separato, come un nastro o in un'altra rete, come un cloud pubblico. Alcuni backup non sono crittografati. A volte, i backup sono memorizzati sul sito. Quando si valuta la sicurezza di un ambiente, è necessario rivedere le procedure di backup per vedere se i dati di backup sono a rischio durante il backup, l'archiviazione o trasportati.

MEGLIO BACKUP NON IN RETE. SI COLLEGA I DRIVE DI BACKUP, SI FA IL BACKUP E POI LO SI SCOLLEGA.

Banner grabbing. Quando ci si connette in remoto a un server FTP, server di posta elettronica o altro servizio, il servizio spesso risponde con un banner che indica quale software è in esecuzione, la versione del software e le funzionalità supportate. Alcuni utenti malintenzionati utilizzano strumenti di acquisizione di banner per afferrare tutti i banner di una rete e quindi scansionano i banner per cercare versioni software precedenti o software vulnerabile.

Mentre alcuni servizi consentono la modifica del banner, questo spesso non riduce il rischio perché esistono altri modi per identificare il software e le versioni che prendono il banner. Ad esempio, a volte è possibile utilizzare SNMP per eseguire query su un dispositivo informazioni hardware e software, utilizzare strumenti di fingerprinting (che si basano sui dettagli delle risposte ping, porte aperte e altri metodi proprietari) o ottenere l'accesso fisico ai dispositivi (che spesso hanno informazioni identificative sul retro o sul fondo).

Passive vs. active. Un dispositivo passivo si trova al di fuori del percorso diretto della comunicazione o è in standby, pronto per diventare attivo su richiesta. I dispositivi passivi sono talvolta a rischio a causa di un aggressore che potrebbe bersagliarli senza essere notato. I dispositivi attivi sono in genere attivi sulla rete, nel percorso diretto delle comunicazioni o la partecipazione attiva a un servizio. Passivo e attivo entrare anche in gioco nella scansione. La scansione attiva è la scansione che si collega ai servizi e ottiene quante più informazioni possibili. La scansione attiva può spesso essere rilevata da un IDS o altre soluzioni di sicurezza. La scansione passiva è più lenta e talvolta non ottiene così tante informazioni, ma la scansione passiva può essere più difficile da rilevare, quindi un attaccante potrebbe essere in grado di farlo scansionare passivamente un ambiente senza che nessuno se ne accorga.

Command-line tools. Gli strumenti da riga di comando vengono eseguiti senza un'interfaccia utente grafica. Puoi eseguirli su una varietà di computer e talvolta anche su smartphone.

Ping. Il comando Ping è un'utilità multipiattaforma, originariamente scritta per UNIX, che utilizza ICMP per comunicare con host remoti. Viene spesso utilizzato per vedere se il telecomando degli host sono raggiungibili sulla rete, se gli host remoti sono in esecuzione e fino a che punto sono lontani gli host remoti (vedendo quanto tempo impiega la restituzione dei pacchetti ICMP).

Netstat. Il comando Netstat consente di esaminare le comunicazioni di rete correnti su un host. Puoi usarlo per cercare porte in ascolto e connessioni stabilite. È un buon strumento per la risoluzione dei problemi, specialmente quando stai cercando di scoprire se un host è in ascolto su una porta specifica.

Tracert. Il comando Tracert, spesso chiamato "traceroute", è uno strumento utilizzato su più piattaforme mostra il percorso dall'host corrente a un host remoto, misurando anche i ritardi il percorso lungo la strada. Si basa su ICMP e non funziona bene su tutti i frewalls (a seconda della configurazione).

Nslookup/Dig. Se si desidera eseguire una query su un server DNS, è possibile utilizzare il comando Nslookup su Windows o il comando Dig su Linux. È possibile eseguire una query per singoli record DNS. Per esempio, puoi chiedere l'indirizzo IP di www.google.com. Puoi anche usarlo per chiedere tutti i record DNS in un dominio, sebbene ciò sia spesso bloccato a causa di problemi di sicurezza.

Arp. Il comando Arp viene utilizzato per visualizzare la tabella ARP su un host. Può anche essere usato per eliminare le voci ARB in una tabella.

Ipconfg/ip/Ifconfg. Per ottenere le informazioni di rete su un host, è possibile utilizzare un comando Ipconfg su Windows o comando Ifconfg su Linux. I comandi faranno visualizzare l'indirizzo IP, la maschera di sottorete, il gateway, i server DNS e altri dettagli sulla tua configurazione di rete. Puoi anche utilizzare questi comandi per cancellare la cache DNS dell'host.

Tcpdump. Tcpdump è un analizzatore di pacchetti a riga di comando in grado di acquisire comunicazioni sulla rete. È uno strumento multipiattaforma molto utile per la risoluzione dei problemi.

Nmap. Nmap è uno scanner di sicurezza open source. Puoi usarlo per scansionare gli host alla ricerca di vulnerabilità, cercare porte aperte o host remoti fingerprint per scoprire quale sistema operativo esegue. Questo strumento è molto utile per analizzare un ambiente.

Netcat è uno strumento di rete che può essere utilizzato per eseguire la risoluzione dei problemi di rete, esplorare reti o cercare porte aperte. È flessibile e può essere utilizzato in molti modi. Nella sua forma più semplice, può essere utilizzato per avviare una connessione a qualsiasi porta utilizzando UDP o TCP. Per esempio, è possibile avviare una connessione a un server di posta elettronica sulla porta TCP 25.

2.3 Given a scenario, troubleshoot common security issues

Per questa sezione, ti verrà presentato uno scenario e dovrai risolvere il problema problema o problemi. Dovresti anche avere familiarità con una buona prima fase di risoluzione dei problemi come e cosa fare se la prima o la seconda procedura di risoluzione dei problemi tipica sono già state eseguite ma non ha prodotto risultati.

Unencrypted credentials/clear text. Per risolvere i problemi relativi a credenziali non sicure, è necessario utilizzare uno strumento di acquisizione dei pacchetti. Puoi catturare alla fonte, a destinazione o entrambi. Il più delle volte, è necessario acquisire a destinazione perché si desidera convalidare che le credenziali vengano trasmesse sulla rete non sicura. Ad esempio, se si sospetta che un'applicazione si integri con Active Directory convalida le password in modo non sicuro, procedere come segue:

Log and event anomalies. Quando si notano eventi insoliti o voci di registro, è necessario verificare se il problema è già stato registrato rivedendo i registri e cercando di correlare le voci con qualsiasi interruzione o degradazione note. Se hai più server che eseguono lo stesso servizio, dovresti controllare gli altri server per vedere se stanno anche ricevendo gli eventi o le voci del registro. Puoi utilizzare

anche un motore di ricerca per cercare ID evento o informazioni univoche registrate nell'evento.

Permissions issues. Per risolvere i problemi relativi alle autorizzazioni, è necessario identificare i metodi di autorizzazione usati. Ad esempio, per una cartella condivisa, esistono sia permessi di sistema che permessi di condivisione. Quando gli utenti sono locali sul server con la cartella condivisa, solo il file system le autorizzazioni sono applicabili, ma quando gli utenti si connettono in remoto alla cartella condivisa, il file le autorizzazioni di sistema e le autorizzazioni di condivisione sono entrambe applicabili. Altra risoluzione dei problemi i passaggi includono l'attivazione della registrazione dettagliata, il controllo per vedere se altri utenti stanno riscontrando lo stesso problema e provare la connessione da un altro dispositivo.
Configura l'app in modo che punti a un singolo controller di dominio. Spesso le app puntano al carico bilanciato nomi virtuali, quindi è necessario riconfigurare l'app per assicurarsi che vengano inviate tutte le autenticazioni un controller di dominio singolo in modo da poter acquisire tutti i pacchetti.
Installare uno strumento di acquisizione di pacchetti sul controller di dominio o preparare il controller di dominio per l'acquisizione di pacchetti se si dispone di uno strumento di acquisizione di pacchetti centralizzato.
Inizia a catturare i pacchetti. Esegui accessi all'applicazione.
Analizzare le acquisizioni di pacchetti per scoprire se le credenziali vengono inviate in chiaro.

SI RISOLVONO TUTTI I PROBLEMI DI AUTORIZZAZIONI CON L'UTILIZZO DI CRIPTEOS 3001 IN CUI OGNI UTENTE HA LA SUA CHIAVE SEGRETA. UN PC GESTIONALE TROVA LA CHIAVE CON MINI ATTACCO DI FORZA BRUTA E MANDA IL DOCUMENTO AL COLLEGA CHE LO DEVE LEGGERE.

SE QUESTO DEVE AGGIORNARLO ASSEGNA UNA NUOVA CHIAVE PER L'UTENTE B. SERVE UN SOFTWARE GESUIONALE AD HOC.

Access violations .Le violazioni dell'accesso si verificano quando un utente accede a una risorsa o ai dati a cui non è autorizzato accesso. L'utente potrebbe aver accesso alla risorsa o ai dati per errore o l'azione potrebbe avere stato malizioso.

Misconfgured devices. Per risolvere i problemi, è necessario tenere traccia dell'attività dell'utente per un'ora prima dell'accesso con violazione e prova a rispondere a domande chiave come: quando l'utente ha inizialmente effettuato l'accesso? L'utente ha fatto accedi a più computer? Quali risorse o dati l'utente ha avuto accesso appena prima dell'accesso violazione? Cosa ha fatto l'utente subito

dopo la violazione di accesso? Il tuo obiettivo è scoprire l'intento dell'utente e scoprire se si sono verificate altre attività non autorizzate. Ad esempio, accedendo ai dati non autorizzati, l'utente si è connesso a un indirizzo IP sconosciuto su Internet?

Data exfltration. Quando i dati vengono rimossi da un dispositivo aziendale senza autorizzazione, vengono chiamati estrapolazione dei dati. Questa è una delle attività chiave che gli utenti malintenzionati tentano di eseguire. Innanzitutto, scopri quali dati fu estrapolato. È stato protetto con la gestione dei diritti digitali (DRM)? Quanti dati erano exfiltrated? Altri dati sono stati precedentemente estratti? È necessario tenere traccia dell'account utente finale indietro di diversi giorni per cercare altre attività non autorizzate. Un dispositivo configurato in modo errato è uno che si trova nel suo stato predefinito o che presenta una configurazione, ciò mette a rischio l'organizzazione. Esistono alcuni problemi di certificazione comuni che è necessario conoscere:

Data exfltration. I certificati scaduti non possono essere utilizzati. Gli avvisi di certificato scaduti vengono generalmente visualizzati e le comunicazioni spesso diventano non sicure (come da HTTPS a HTTP).

Untrusted certifcates. I sistemi operativi di solito dispongono di negozi di fiducia certificati che forniscono un trust incorporato per determinati emittenti certificati. Quando vai su un sito web con un certificato di un emittente di fiducia, il tuo browser consente la connessione. Se vai su un sito web con un certificato rilasciato da un emittente non attendibile, il tuo browser ti avviserà il pericolo e consentirti di scegliere cosa fare dopo.

Mismatched certifcates. Supponiamo che un utente vada su https://www.google.com ma che il certificato usato è stato rilasciato per un altro nome di dominio; è un certificato non corrispondente. La maggior parte dei browser lo faavviserà di certificati non corrispondenti perché spesso sono indicativi di malware o di una configurazione errata.

Firewall. Se un firewall non è configurato correttamente, potrebbe consentire il traffico dannoso nella rete. Puoi rivedere le più recenti modifiche alla configurazione del firewall per vedere se una modifica recente è la causa. Altrimenti, puoi rivedere il numero di hit sulle regole del frewall per qualsiasi cosa fuori dal comune. Infine, puoi confrontare la configurazione corrente con un backup di qualche giorno fa per cercare le modifiche.

Content flter. Se si utilizza un filtro per i contenuti ma non è configurato correttamente, potrebbe non filtrare tutto . È utile confrontare la configurazione con un altro dispositivo o con un backup.

Access points. Molte organizzazioni hanno più punti di accesso. Se si sospetta che uno non sia configurato correttamente, è possibile confrontare la versione del software e la configurazione con un punto di accesso che ha la giusta configurazione.

Weak security confgurations .Deboli configurazioni di sicurezza mettono a rischio la tua organizzazione. Esempi comuni di deboli configurazioni di sicurezza sono password predefinite, servizi di gestione non crittografati (come un'interfaccia Web per l'amministrazione tramite HTTP), servizi non sicuri (ad esempio Telnet), vecchie versioni di software o software, software senza patch e mancanza di rispetto del principio del privilegio minimo. È possibile risolvere questi scenari con uno scanner di vulnerabilità, a port scanner e una soluzione di gestione della configurazione.

Personnel issues. Le questioni relative al personale riguardano problemi con persone, in genere dipendenti o appaltatori.

Unauthorized software .Quando i dipendenti installano software non autorizzato, possono mettere a rischio l'organizzazione. Il software potrebbe contenere malware incorporato o essere instabile e causare problemi di sistema. Puoi impedire ai dipendenti di installare software sui propri computer. Inoltre, puoi usare una soluzione di gestione della configurazione per la scansione di software non autorizzato su computer e rimuoverlo automaticamente.

Policy violation. Quando si verifica una violazione della politica, la persona che ha violato la politica deve essere notificato e l'incidente deve essere registrato. Perché le violazioni delle politiche possono in ultima analisi portare alla risoluzione, le violazioni delle norme devono essere registrate con dettagli specifici, come la data, violazione del tempo e specifica e un piano d'azione dovrebbe essere sviluppato per garantire che non lo faccia succedere di nuovo.

Insider threat. Una minaccia interna è una persona all'interno della tua organizzazione che ha malevole intenzioni. Tali minacce possono essere difficili da rilevare. Aderendo al principio del privilegio minimo aiuta a limitare l'accesso degli addetti ai lavori e può essere utile disporre di controlli e registrazioni completi individuare attività dannose.

Social engineering. Un modo chiave per limitare l'efficacia del social engineering è testare regolarmente i dipendenti con false campagne di social engineering. Ad

esempio, potresti inviare un'e-mail di phishing falsa ai dipendenti, tenere traccia di chi fa clic e disporre di una terza parte, la compagnia tenta di ottenere l'accesso alla propria struttura facendo apparire qualcuno come lavoratore elettrico di utilità. L'istruzione è la chiave. I dipendenti devono comprendere le minacce e conoscere cosa fare se ne vedono uno o non sono sicuri.

IL SOFTWARE KEY-LOCK BLOCCA IL SOCIAL ENGINEERING DI CHI METTE COME PASSWORD NOMI E DATE DI FAMILIARI

IL METODO DI ARGINAMENTO DEL PHISHING, DESCRITTO ANCHE SU YOUTUBE, PERMETTE DI RESTRINGERE IL PERIMETRO DA DIFENDERE,

VEDI SU YOUTUBE CON PAROLA CHIAVE ROBIONICA

Social media. I social media possono essere negativi in un paio di modi: i dipendenti potrebbero passare troppo tempo lì durante l'orario di lavoro o potrebbero esserci informazioni riservate accidentalmente condivise. Le organizzazioni spesso limitano l'accesso ai social media o hanno specifiche politichesi utlizzo. È possibile utilizzare i filtri dei contenuti, il controllo e la registrazione per tenere traccia dei social media tassi di utilizzo e cercare anomalie.

Personal email. Come i social media, l'e-mail personale può danneggiare ed essere la produttività dei dipendenti utilizzatata per estrapolare i dati. È possibile limitare l'accesso ai servizi di posta elettronica personali, utilizzare un server proxy per controllare e registrare l'utilizzo e utilizzare una soluzione DLP per proteggersi dall'estrazione dei dati.

Baseline deviation . Una soluzione di gestione della configurazione ha spesso agenti distribuiti ai dispositivi, che controllano confgurazioni ad orari prestabiliti. Quando vengono rilevate deviazioni dalla linea di base, possono essere riparate automaticamente o registrate e segnalate. Per massimizzare la sicurezza, è necessario correggere automaticamente le deviazioni della linea di base.

License compliance violation (availability/ integrity)
. Molte organizzazioni utilizzano soluzioni di gestione delle licenze di terze parti per gestire le proprie licenze. Tali soluzioni ti aiutano a capire se hai bisogno di più licenze e se sei conforme a requisiti di licenza. Senza tale soluzione, è possibile utilizzare una gestione della configurazione, soluzione per contare il numero totale di licenze o installazioni e confrontarlo con la proprietà della tua licenza.

Asset management. La gestione patrimoniale comporta la gestione di hardware (computer, telefoni, ecc.) E software (ad esempio come licenze). È possibile

utilizzare una soluzione di gestione delle risorse per tenere traccia delle risorse. Avrà un database e probabilmente usano codici a barre per tutte le risorse fisiche, che possono essere scansionate da uno scanner portatile.

Authentication issues. Le organizzazioni più piccole possono utilizzare un foglio di calcolo per tenere traccia di tutte le risorse. Per risolvere i problemi di autenticazione, è possibile utilizzare uno strumento di acquisizione dei pacchetti (per esaminare i metodi di connettività e autenticazione e verificare la presenza di errori di crittografia), registri eventi e registro voci (per verificare la presenza di password errate o altri problemi di autenticazione) e tentativi ed errori (per esempio, se un utente non è in grado di autenticarsi su un server Web, puoi verificare se può eseguire l'autenticazione altrove per determinare se il nome utente / la password sono validi).
IL FOGLIO DI CALCOLO E' VULNERABILE ALLA SICUREZZA.

ROBIONICA HA CREATO PER LE ESIGENZE DEL GDPR UN FOGLIO DI CALCOLO IN CUI LE VOCI IN CHIARO SONO SOLO SUL MONITOR E SUL DISCO FISSO TUTTO E' CRITTOGRAFATO CON L'ALGORITMO GIA' UTILIZZATO CON IL SOFTWARE KEY-LOCK

2.4 Given a scenario, analyze and interpret output from security technologies

Per questa sezione dell'esame, ti verranno presentati i risultati e diverse descrizioni di quell'uscita; devi selezionare la descrizione più appropriata. Avere esperienza pratica per questa sezione è utile, soprattutto se non lavori regolarmente con questo tipo di output.

HIDS/HIPS Gli avvisi provenienti da HIDS o HIPS indicano in genere una potenziale intrusione o tentata intrusione che è stata bloccata. Si tratta di avvisi importanti che devono essere attuati rapidamente, in genere da un centro operativo di sicurezza.

Antivirus .L'output del software antivirus di solito indica informazioni sulle recenti scansioni antivirus, rilevamento di un virus o altro malware e avvisi su altri problemi (come l'antivirus il servizio viene arrestato o disabilitato). È possibile utilizzare queste informazioni per correggere i problemi.

File integrity check. Se un controllo di integrità del file non riesce, verrà spesso visualizzato un messaggio relativo a una mancata corrispondenza del checksum o qualcosa di simile. Non dovresti fidarti dei file che non superano i controlli di integrità perché potrebbero essere dannosi.

Host-based frewall Un frewall basato su host genera in genere tre cose: avvisi, notifiche di aggiornamento e registri.

Gli avvisi ti dicono che è entrato un qualche tipo di comunicazione; potresti dover agire o no, potrebbe essere stato bloccato automaticamente. Le notifiche di aggiornamento indicano che ha aggiornamenti firewall da eseguire. I registri sono i registri dal firewall. In genere, i registri predefiniti tengono traccia del servizio avvio e spegnimento, eventi di aggiornamento e altri eventi non critici. Puoi alzare il livelli di registrazione per acquisire ulteriori dettagli, ad esempio ogni volta che viene utilizzata una regola firewall o la comunicazione è bloccata.

Application whitelisting. Quando si autorizza un'applicazione, la si contrassegna come sicura per l'esecuzione. Le applicazioni autorizzate in genere non passano attraverso un controllo di sicurezza all'avvio. In alcuni casi, possono essere eseguite solo le applicazioni autorizzate. L'output dalla whitelisting dell'applicazione si riferisce alle app che hanno tentato di eseguire ma non sono autorizzati o hanno problemi con un'app autorizzata (forse è stata aggiornata e non funziona correttamente con la whitelisting).

Removable media control. I supporti rimovibili possono essere utilizzati per estrarre i dati o introdurre malware. Molte organizzazioni preferiscono limitare o disabilitare l'uso di supporti rimovibili. Alcuni sistemi operativi dispongono di strumenti integrati per aiutare a limitare o disabilitare i supporti rimovibili. Le soluzioni di terze parti sono state migliorate opzioni e rapporti. Si desidera controllare l'uso di supporti rimovibili (per valutare se i controlli funzionano) esaminando i file di log e impostando avvisi.

Advanced malware tools. Gli strumenti malware segnalano se trovano malware e se sono in grado di farlo rimuovere, bloccare o mettere in quarantena il malware. Questo output è importante perché potresti dover intraprendere azioni manuali per rimuovere il malware.

Patch management tools.L'output degli strumenti di gestione delle patch indica in genere se le patch sono state eseguite correttamente installate. Quando non vengono installati correttamente, è necessario analizzare il registro dettagliato delle voci per vedere il motivo (ad esempio spazio su disco insufficiente o mancanza di autorizzazioni).

UTM. Una soluzione di gestione unificata delle minacce (UTM) combina alcune funzionalità di rete in un'unica soluzione, dispositivo che fornisce sicurezza basata su rete (come proxy, reverse proxy e firewall).
È possibile attivare la registrazione dettagliata, rivedere i file di registro e risolvere le regole come parte del proprio scenari di risoluzione dei problemi.

DLP. I sistemi DLP forniscono avvisi, il che è configurabile. Puoi avere una soluzione DLP che ti avverte in caso di sospetta perdita di dati o infrazione di regole DLP. Anche i file di log DLP acquisiscono tali eventi e questi devono essere inviati a una soluzione SIEM.

DEP Data execution .prevention. La prevenzione dell'esecuzione dei dati (DEP) è una tecnologia che aiuta a proteggere la memoria da malware . Esistono DEP basati su hardware e DEP basati su software. È possibile proteggere singole applicazioni con DEP oppure è possibile proteggere un intero computer. È possibile risolvere DEP per configurarlo per una singola applicazione e quindi passare attraverso i test. Puoi anche aumentare il livello di registrazione per ottenere ulteriori informazioni su uno scenario di risoluzione dei problemi.

Web application firewall.
Un web application frewall (WAF) aiuta a proteggere le applicazioni da attacchi dannosi. A WAF può ispezionare le richieste di app a livello di app per bloccare gli attacchi avanzati basati sul web. I WAF hanno regole, come un firewall. È possibile verificare se le regole vengono utilizzate e acquisire il traffico con un'acquisizione di pacchetti o un comando di debug incorporato.

2.5 Given a scenario, deploy mobile devices securely
Il mondo dell'informatica mobile sta crescendo: nuove funzionalità vengono introdotte regolarmente e le persone stanno facendo di più sui propri dispositivi mobili. Pertanto, è necessario comprendere come proteggere l'uso dei dispositivi mobili. Come altre sezioni dell'esame, questa si concentra sugli scenari. Essere sicuro di essere a tuo agio nel raccomandare una o più tecnologie basate sui requisiti di uno scenario.

RITENIAMO DIFFICILE DIFENDERE I DISPOSITIVI MOBILI. MEGLIO DIFENDERE IL CORE BUSINESS CON LA TECNICA DEL PONTE LEVATOIO CON DUE COMPUTER, UNO COLLEGATO ALL'ESTERNO E L'ALTRO AL CORE BUSINESS CHE COMUNICANO CON LA CRITTOGRAFIA CRIPTEOS 3001

Connection methods. Gli smartphone hanno una varietà di modi per comunicare. Alcuni facilitano le comunicazioni vocali mentre altri sono destinati al trasferimento di dati o ad usi di nicchia.

Cellular. Gli smartphone si connettono alle reti cellulari tramite onde radio. Una rete cellulare è suddivisa in celle, con torri cellulari che forniscono la copertura radio per un'area geografica designata. Alcune delle comuni reti cellulari sono GSM e CDMA.

WiFi. WiFi è una tecnologia di rete wireless locale che utilizza la tecnologia radio per comunicare. Esistono molti standard WiFi, tra cui 802.11n, 802.11ac e 802.11ay.

SATCOM. Satellite Communications (SATCOM) è una tecnologia che utilizza i satelliti per comunicare. SATCOM può fornire accesso a Internet e comunicazioni vocali ai dispositivi, case e aziende.

Bluetooth. Bluetooth è uno standard di comunicazione dati che utilizza una tecnologia wireless oltre 100 metri o meno (spesso, molto meno). Il Bluetooth è utilizzato in una varietà di dispositivi tra cui cuffie, mouse e tastiere. Non fornisce lo stesso livello di prestazioni e la larghezza di banda fornita dal WiFi, ma spesso è sufficiente per i comuni usi periferici.

NFC. Near Field Communications (NFC) è una tecnologia di comunicazione wireless che fornisce comunicazioni fino a 3 piedi. Viene utilizzato principalmente per i sistemi di pagamento mobili o trasferimenti di dati di piccole dimensioni da cellulare a cellulare, come la condivisione di contatti. Le prestazioni sono abbastanza limitato, con velocità massime fino a 424 kb / s.

ANT. ANT è una tecnologia di rete wireless proprietaria utilizzata principalmente da dispositivi indossabili intelligenti come cardiofrequenzimetri, smartwatch e tracker del sonno. È orientato verso l'utilizzo con sensori e consente comunicazioni fino a 30 metri.

Infrared. La comunicazione a infrarossi è una tecnologia wireless che si basa sulla luce che gli umani non possono rilevare con i loro occhi. Viene utilizzato principalmente in dispositivi consumer come il telecomando controlli per televisori e altri dispositivi.

USB. USB è uno standard di comunicazione cablata per la trasmissione di dati tra dispositivi che supporto USB. L'ultima versione è la 3.2 che fornisce velocità massime fino a 20 Gb / s. USB viene utilizzato principalmente per collegare periferiche come tastiere, mouse e stampanti ai computer.

Mobile device management concepts

Esistono molti modi per gestire i dispositivi mobili. Ad esempio, è possibile utilizzare un dispositivo mobile soluzione di gestione (MDM). Qualunque sia il metodo utilizzato, ci sono alcuni concetti che sono comunemente utilizzati in tutte le soluzioni di gestione. Avere familiarità con loro che si potrebbe consigliare sulla base di uno scenario con requisiti o un elenco di sfide da risolvere.

Application management. Quando un dispositivo è gestito, soprattutto da un MDM soluzione, può gestire le sue applicazioni. Ad esempio, un'organizzazione potrebbe distribuire 3 o 4 app interne utilizzando la soluzione MDM. Oppure la soluzione MDM potrebbe essere configurata per bloccare alcune app.

Content management. La gestione dei contenuti si concentra sulla gestione del ciclo di vita dei dati su smartphone. Generalmente, questo include l'archiviazione di file file (come il modo in cui i file vengono archiviati in un file dispositivo), trasferimento file (come il modo in cui i file si spostano dallo smartphone ad altri repository), e la condivisione dei file (come la possibilità di condividere un fle con un altro utente). Dal punto di vista della sicurezza, la gestione dei contenuti è importante. Se non riesci a fornire una buona esperienza utente e livello di sicurezza aziendale, la soluzione potrebbe non essere ampiamente accettata o utilizzata.

Remote wipe. La cancellazione remota è la capacità di eliminare in remoto i contenuti di un telefono - app, dati e configurazione. La cancellazione remota potrebbe includere solo dati aziendali o potrebbe includere tutti i dati. La cancellazione remota è una funzione chiave che può aiutare a ridurre al minimo le possibilità di smarrimento dati in caso di smarrimento o furto di un telefono.

Geofencing. Il geofencing è una tecnologia che consente azioni basate su una posizione smartphone . Ad esempio, se uno smartphone viene portato fuori dal Paese della tua organizzazione, tu può disabilitare il Bluetooth e inviare un avviso al telefono avvisando l'utente del Bluetooth essere disabilitato. Il geofencing può essere utilizzato per scopi di produttività (come il monitoraggio di un driver di consegna) o per il marketing (come un'app mobile che invia un coupon quando si accede a un negozio).

Geolocation. La maggior parte dei telefoni ha il GPS integrato; questo consente alle app e al telefono di tracciare la sua posizione geografica. La geolocalizzazione può essere utilizzata per l'accesso. Ad esempio, se il telefono è al di fuori del tuo paese di origine, un'app potrebbe essere configurata per negare l'accesso.

Screen locks. I blocchi dello schermo vengono utilizzati per proteggere i dati sui telefoni, soprattutto in caso di un telefono smarrito o rubato. I blocchi dello schermo vengono spesso distribuiti automaticamente dopo un periodo di inattività, ad esempio 5 minuti. I blocchi dello schermo sono un'opzione di sicurezza chiave che dovresti usare su tutti i telefoni.

Push notifcation services. Le notifiche push sono avvisi che un'app può inviarti in base a una varietà di attributi, azioni o posizioni ambientali. Un semplice esempio è

un gioco che invia una notifica push quando è il tuo turno di giocare. Le notifiche push sono utili anche negli affari. Ad esempio, un servizio di allarme di emergenza potrebbe inviare una notifica push ai dipendenti durante un disastro naturale. Molte soluzioni MDM offrono una funzionalità notifica push funzionalità e abilitare la gestione delle impostazioni di notifica push sugli smartphone.

Passwords and PINs. Password e PIN vengono spesso utilizzati per sbloccare telefoni e app e sono anche utilizzati nelle app per una maggiore sicurezza. Sebbene le password e i PIN siano più vecchi della biometria, sono comunque considerati più sicuri in determinati scenari. In qualche Paese, le persone non sono tenute a fornire alle autorità password e PIN.

Biometrics. Sui dispositivi mobili, la biometria si riferisce in genere a impronte digitali, scansioni del viso e scansioni della retina. Queste soluzioni biometriche vengono spesso utilizzate per sbloccare telefoni e app e vengono utilizzati anche nelle app per una maggiore sicurezza.

Context-aware authentication. L'autenticazione legacy si basa su password. Stili più recenti dell'autenticazione richiede più fattori di autenticazione (come un'app mobile o dati biometrici). L'autenticazione basata sul contesto utilizza le informazioni sulla transazione di autenticazione per decidere se autenticare un utente. Ad esempio, l'autenticazione basata sul contesto potrebbe controllare il dispositivo utilizzato per l'autenticazione per vedere se si tratta di un dispositivo noto, se mai lo è stato usato prima o se si tratta di un dispositivo di proprietà dell'azienda. Un'autenticazione sensibile al contesto potrebbe anche guardare la posizione della richiesta di autenticazione - proviene da una rete nota?
La persona ha mai autenticato da quella posizione prima? Molti fattori possono entrare in gioco, in base alle tue esigenze. Un'applicazione sensibile al contesto può richiedere un secondo fattore di autenticazione se la richiesta di autenticazione di un utente è considerata a rischio più elevato (nuovo dispositivo, nuova posizione o insolita ora del giorno, ad esempio).

Containerization. Molte soluzioni MDM sfruttano la containerizzazione. La containerizzazione è il processo di creazione e utilizzo di contenitori per isolare app e dati aziendali app e dati personali. Ad esempio, è possibile archiviare tutti i dati aziendali in un contenitore sicuro lasciando tutti i dati personali in uno stato predefinito. In questo scenario, gli amministratori possono farlo cancellare da un telefono ma influire solo sui dati aziendali (ad esempio quando un dipendente viene licenziato).

Storage segmentation. La segmentazione dello storage è come la containerizzazione, ma la segmentazione dello storage si concentra strettamente sulla segmentazione dello storage, mentre la containerizzazione offre una maggiore ambiente di isolamento per dati, app e servizi.

Full device encryption. La crittografia completa del dispositivo è la crittografia dell'intero disco. In tale scenari, è necessario sbloccare la crittografia al riavvio, in genere con un passcode o passphrase. Il rovescio della medaglia è che i servizi del tuo telefono (come allarmi o telefonate) non sono disponibili fino a quando non si sblocca il disco all'avvio. Alcuni smartphone si stanno muovendo verso la crittografia basata su fle, che crittografa i file su richiesta. È possibile utilizzare la crittografia dei file, diverse chiavi e metodi per la crittografia, mentre la crittografia completa del disco è limitata a una sola chiave e metodo. Molte organizzazioni richiedono almeno la crittografia dei dati dell'utente. Come le organizzazioni di solito applicano la crittografia attraverso la loro piattaforma MDM.

Enforcement and monitoring for Third-party app stores. Molti dei grandi fornitori, come Apple e Google, offrono a app store dedicato per i loro dispositivi. Per impostazione predefinita, i dipendenti possono scaricare e installare qualsiasi app da app store. Alcuni di questi potrebbero essere dannosi e alcuni potrebbero non essere adatti per un ambiente di lavoro. Le organizzazioni possono utilizzare il software di gestione dei dispositivi mobili per bloccare l'installazione di determinate app o determinate categorie di app. Questo può ridurre il rischio che i dipendenti scarichino software dannoso senza accorgersene.

Rooting/jailbreaking. Molte soluzioni di gestione di dispositivi mobili hanno una funzione integrata per rilevare radicato (rilevanti per Android) o jailbreak (rilevanti per iOS). Tali dispositivi hanno bypassato la sicurezza del sistema operativo mobile e sono a rischio di vulnerabilità o malware perché l'utente può installare applicazioni da qualsiasi fonte, come una fonte al di fuori dell'applicazione del venditore store. . Molte organizzazioni bloccano l'accesso alla rete di dispositivi rooted o jailbreak.

Sideloading. Il sideload si riferisce all'installazione di app esterne all'app store. Mentre molti venditori di app preferiscono lavorare solo all'interno degli app store dei fornitori, a volte loro o un'app esterna agli app store. Tuttavia, le app offerte al di fuori degli app store non passano attraverso il rigoroso processo di verifica che farebbero in un app store del fornitore. Questo pone rischi aggiuntivi per la tua organizzazione. Le soluzioni MDM possono bloccare il sideload.

Custom frmware. Alcuni smartphone, in particolare quelli basati sulla piattaforma Android, supporto per firmware personalizzato. In alcuni casi, firmware

personalizzato apre funzionalità non disponibili con il software Android predefinito. Tuttavia, frmware personalizzato può presentare ulteriori rischi per un'organizzazione. Spesso, le organizzazioni bloccano i dispositivi con firmware personalizzato.

Carrier unlocking. Molti smartphone sono bloccati in uno o un paio di gestori. Ma puoi spesso sbloccare uno smartphone e cambiare operatore. Per gli scenari BYOD, questo non è una preoccupazione per un'organizzazione. Ma con dispositivi di proprietà aziendale, questo potrebbe non essere uno scenario desiderato.

Firmware OTA updates. Molti rivenditori di smartphone forniscono aggiornamenti su frmware tramite aria (OTA). Generalmente, gli aggiornamenti di firmware sono importanti perché spesso includono sicurezza patch e aggiornamenti. Ma alle organizzazioni spesso piace testare gli aggiornamenti di frmware per garantire stabilità e compatibilità prima che supportino ufficialmente il software.

Camera use. In ambienti ad alta sicurezza, le organizzazioni a volte bloccano l'accesso della fotocamera. Ciò garantisce che i dipendenti non possano scattare foto di documenti o di documenti sensibili o aree riservate.

SMS/MMS. La messaggistica di testo tramite SMS / MMS è una funzione comune disponibile sulla maggior parte degli smartphone. Alcune organizzazioni devono limitare l'uso di SMS / MMS (come solo per uso aziendale)
o disabilitare l'uso di SMS / MMS (come un'organizzazione ad alta sicurezza che richiede solo sicurezza meccanismi di comunicazione).

External media. Supporti esterni. La messaggistica tramite SMS/MMS è una caratteristica comune disponibile sulla maggior parte degli smartphone. Alcune organizzazioni devono limitare l'uso di SMS/MMS (ad esempio solo per uso aziendale) o disattivare l'uso SMS/MMS (ad esempio un'organizzazione ad alta sicurezza che richiede solo sicuro meccanismi di comunicazione).

USB OTG. USB on-the-go (USB OTG) consente ai dispositivi compatibili di leggere i dati da USB unità senza passare attraverso un computer. Nella maggior parte dei casi, è necessario un convertitore per la conversione la connessione USB a un tipo di connessione compatibile, ad esempio micro-USB o USB-C.

Recording microphone. Praticamente tutti gli smartphone hanno microfoni integrati che possono essere usato per registrare l'audio. Sono stati segnalati malware dannosi per i microfoni di accendendoli e registrando l'audio. Alcune organizzazioni

preferiscono bloccare la registrazione dal microfono per garantire che i dipendenti non registrino segretamente o illegalmente persone o riunioni.

GPS tagging. In molti smartphone, le foto acquisite vengono automaticamente taggate con Informazioni GPS. Ciò consente a qualcuno di guardare le coordinate GPS di un'immagine e deduci dove è stato portato. In alcuni ambienti, questo potrebbe essere un rischio per la sicurezza.
Le organizzazioni possono scegliere di disabilitare la codifica GPS delle foto in alcune implementazioni MDM.

WiFi direct/ad hoc. WiFi direct è una tecnologia che consente a due dispositivi wireless di connettersi tra loro. Una volta connessi, i dati possono essere condivisi. Ridurre al minimo le possibilità di perdita dati, alcune organizzazioni scelgono di bloccare il WiFi diretto.

Tethering. Quando un dispositivo wireless condivide la sua connessione Internet con altri dispositivi, gli altri dispositivi sono collegati al dispositivo di condivisione. Il tethering è conveniente perché puoi connettere dispositivi a Internet che non dispongono di accesso a Internet integrato.

Payment methods. I metodi di pagamento per smartphone includono soluzioni di pagamento come Apple Pay, Android Pay e Samsung Pay. Questi metodi di pagamento si basano su NFC per abilitare perfettamente gli acquisti in vari luoghi, come distributori di benzina, distributori automatici e mercati. Per i dispositivi di proprietà dell'azienda, alcune organizzazioni disabilitano il pagamento mobile metodi per impedire agli utenti di archiviare le informazioni di pagamento sui dispositivi.

Modelli di distribuzione. Per distribuire efficacemente i dispositivi, è necessario definire i metodi supportati, mettere in atto i processi e documentare tutto.

BYOD. Utilizzare il proprio dispositivo (BYOD), le persone accedono alla rete utilizzando i dispositivi che possiedono e gestiscono. La tua organizzazione installa software di gestione dei dispositivi e garantisce che i dispositivi soddisfino i requisiti dell'organizzazione. Il vantaggio di BYOD è che tutti possono ottenere il dispositivo supportato di loro scelta e possono eseguire l'aggiornamento tutte le volte che vogliono. Inoltre, la tua organizzazione non deve procurarsi dispositivi
o gestire i dispositivi, risparmiando tempo e denaro per l'organizzazione. Il rovescio della medaglia è che le organizzazioni spesso devono supportare una pletora di tipi di dispositivi, che possono diventare diffcili. Ad esempio, l'organizzazione potrebbe voler distribuire una nuova app, ma se ha requisiti di dispositivo, come i requisiti di

versione del sistema operativo, potrebbe non essere in grado perché l'organizzazione non può forzare upgrade, aggiornamenti o modifiche ai dispositivi sui dispositivi BYOD.

COPE. Di proprietà dell'azienda, abilitato personalmente (COPE) è un modello in base al quale le organizzazioni acquistano e gestiscono dispositivi. Tuttavia, l'organizzazione consente agli utenti di utilizzare i dispositivi per uso personale, come navigare sul web, scattare foto, utilizzare i social media e giocare. Con COPE, le opzioni del dispositivo sono in genere più limitate di BYOD. Tuttavia, è più facile supportare il reparto IT e il reparto IT mantiene un maggiore controllo.

CYOD. Con scegli il tuo dispositivo (CYOD), le organizzazioni o i dipendenti possono scegliere tipi di dispositivo supportati e il dipendente paga per il dispositivo e possiede il dispositivo. Le organizzazioni distribuiscono software di gestione dei dispositivi. Questo modello riduce i costi hardware per l'organizzazione. CYOD si trova a metà strada tra BYOD (pensa a questo come un "selvaggio west") e COPE (pensa a questo come a un modello più bloccato).

Corporate-owned. Il modello di proprietà dell'azienda è un modello tradizionale in base al quale l'organizzazione acquista e mantiene l'hardware. Spesso, questo modello non consente ai dipendenti di utilizzare i dispositivi per uso personale. In uno scenario del genere, i dipendenti ne trasportano abitualmente due dispositivi: il dispositivo di proprietà dell'azienda e il dispositivo personale. Mentre alcuni utenti useranno questo modello, molti non lo fanno a causa del fastidio di trasportare due dispositivi. Gli aspetti negativi sono rilevanti sia che tu stia parlando di smartphone o computer portatili.

VDI. Un'infrastruttura desktop virtuale (VDI) è quella che fornisce desktop virtuali agli utenti. Questo non è un modello valido per la distribuzione di smartphone ma può essere efficace in sostituzione per la distribuzione di laptop. I dipendenti in genere ottengono un desktop virtuale a cui possono connettersi dal proprio dispositivo (in genere un computer portatile). La connessione è spesso a schermo intero, quindi è come lavorare su un dispositivo aziendale. Tuttavia, uno smartphone non è un buon modo per connettersi a un VDI per più di un compito veloce o due.

2.6 Given a scenario, implement secure protocols

VDI. Un'infrastruttura desktop virtuale (VDI) è quella che fornisce desktop virtuali agli utenti. Questo non è un modello valido per la distribuzione di smartphone ma può essere efficace in sostituzione per la distribuzione di laptop. I dipendenti in genere ottengono un desktop virtuale a cui possono connettersi dal proprio dispositivo (in genere un computer portatile). La connessione è spesso a schermo

intero, quindi è come lavorare su un dispositivo aziendale. Tuttavia, uno smartphone non è un buon modo per connettersi a un VDI per più di un compito veloce o due.

Protocols Molti dei protocolli nei seguenti elenchi puntati sono protocolli comuni usati abitualmente. Tuttavia, se la tua esperienza è limitata a un'area (rete o server o desktop), potresti non avere familiarità con tutti loro. Assicurati di poter differenziare tra loro per l'esame.

DNSSEC. Dominio Name System Security Extensions (DNSSEC) è una specifica per la protezione delle informazioni DNS. DNSSEC richiede la firma dei dati per garantire che i dati siano validi.
DNSSEC non è stato ampiamente adottato ma è considerato lo standard per la protezione di un DNS ambiente, soprattutto da attacchi dannosi.
SSH. Secure Shell (SSH) è un protocollo utilizzato per proteggere le comunicazioni di rete. È ampiamente utilizzato dagli amministratori di server per mantenere server basati su Linux. SSH utilizza la crittografia a chiave pubblica. Per impostazione predefinita, funziona tramite la porta 22. Si utilizza SSH per accedere a una shell protetta un server remoto, ma il protocollo viene utilizzato anche altrove, ad esempio con SFTP.

S/MIME. Le estensioni di posta Internet sicure / multiuso (S / MIME) definiscono uno standard che puoi comunicare in modo sicuro tra due o più parti tramite e-mail. S / MIME si basa sulla crittografia a chiave pubblica, con le parti che si scambiano il proprio certificato pubblico prima di una comunicazione sicura. La maggior parte dei client di posta elettronica supporta S / MIME, ma non è adatto per e-mail basata sul web.

SRTP. Secure Real-Time Transport Protocol (SRTP) è un protocollo per proteggere le comunicazioni, in genere su una rete di telefonia o basata su comunicazioni.

LDAPS. LDAPS (Lightweight Directory Access Protocol Secure) è un protocollo utilizzato per comunicare in modo sicuro con un server LDAP (una directory centralizzata che contiene informazioni su utenti, gruppi, computer e altre risorse di rete). È uno standard aperto ed è implementato su un'ampia varietà di prodotti. Ad esempio, Active di Microsoft Directory Dominio Services (Servizi di dominio Active Directory e spesso solo "Active Directory") fornisce LDAP e
Funzionalità LDAPS.

FTPS. File Transfer Protocol (FTP) ha una versione protetta, FTPS (File Transfer Protocol Secure). FTPS è FTP con estensioni utilizzate per aggiungere TLS o SSL alla connessione.

SFTP. FTP sicuro (SFTP) è diverso da FTPS: SFTP utilizza il protocollo SSH per il trasferimento file, mentre FTPS utilizza FTP. SFTP è più comunemente usato di FTPS.

Voice and video. Voce e video sono due forme di comunicazione. La voce si traduce in telefonate mentre il video si traduce in videochiamate o videoconferenze. Per questo caso d'uso, SRTP è appropriato. Inoltre, verrebbe probabilmente utilizzato TLS per parti della comunicazione.

Time synchronization. Per la sincronizzazione dell'ora, il servizio principale è Network Time Protocollo (NTP).NTP è un protocollo per sincronizzare gli orologi tra due dispositivi in rete. Funziona tramite UDP sulla porta 123. Esistono altri servizi temporali, basati su NTP ocompatibile con NTP, come SNTP e Windows Time Service (W32Time).

Email and web. Per la posta elettronica, i protocolli principali sono SMTP (porta 25, per l'inoltro della posta elettronica), POP / IMAP (per il recupero della posta elettronica utilizzando client di posta elettronica legacy), S / MIME (per la posta elettronica crittografata), HTTPS (per l'amministrazione e la posta elettronica basata sul Web) e SSL / TLS (per proteggere varie comunicazioni). Per il web, HTTP (porta 80) e HTTPS (443) sono i protocolli primari.

File transfer. Per il trasferimento fle, puoi scegliere di utilizzare FTP (veloce, facile, privo di sicurezza), FTPS (come FTP ma aggiunge la crittografia) o SFTP (trasferimento sicuro di file tramite SSH). In alternativa, puoi utilizzare HTTPS per i trasferimenti fle basati sul web.

Use cases Oltre a conoscere il significato generale e la funzionalità dei protocolli, è necessario conoscere gli scenari in cui li distribuiresti. Di seguito sono riportati alcuni dei casi d'uso più comuni.

SNMPv3. Il protocollo SNMP (Simple Network Management Protocol) è un protocollo basato su standard per la gestione o il monitoraggio di dispositivi in rete. È comunemente usato nel monitoraggio degli strumenti per ottenere informazioni sul dispositivo come numero di modello, versioni di software e frmware e informazioni di configurazione. La versione 3 aggiunge funzionalità crittografiche, ovvero un grande miglioramento perché SNMPv1 e SNMPv2 sono considerati non sicuri.

SSL/TLS. Secure Sockets Layer (SSL) e Transport Layer Security (TLS) sono protocolli che forniscono comunicazioni sicure su una rete. SSL, ora deprecato, era l'implementazione iniziale ma è stata successivamente sostituita da TLS (anche se è

ancora possibile trovare un po 'di SSL su Internet). TLS è più recente e più sicuro e offre funzionalità aggiuntive SSL, come la segretezza diretta.

HTTPS. Hypertext Transport Protocol Secure (HTTPS) è un'estensione di HTTP che incorpora TLS (e talvolta il vecchio SSL) per crittografare le comunicazioni. HTTPS è il il protocollo sicuro più utilizzato su Internet.
Secure POP/IMAP. Post Office Protocol (POP) e Internet Message Access Protocol (IMAP) sono protocolli utilizzati dai client di posta elettronica per comunicare con i server di posta elettronica. Entrambi gli altri un'implementazione sicura tramite SSL o TLS. POP3, la terza versione del protocollo, è il più ampiamente usato, mentre IMAP è sulla versione 4. POP3S è una versione sicura di POP3. IMAPS è un'implementazione sicura di IMAP.

Directory services. Per i servizi di directory, il protocollo più comune è LDAP e LDAPS. Active Directory e altri servizi di directory basati su standard supportano LDAP e LDAPS.

Remote access. Per l'accesso remoto ai dispositivi, HTTPS è il protocollo più comune. Per accesso remoto a server, SSH (principalmente per computer basati su Linux) e RDP (remoto vengono comunemente utilizzati il protocollo desktop, principalmente per computer basati su Windows.

Dominio name resolution. Per DNS, DNSSEC è il protocollo di sicurezza più comune. Sebbene non sia ampiamente implementato, è lo standard per proteggere il DNS quando hai requisiti per la sicurezza DNS.

Routing and switching. Per l'instradamento e la commutazione, esistono diversi protocolli. RIP, IGRP, OSPF e BGP sono esempi comuni. Il protocollo RIP (Routing Information Protocol) è un protocollo legacy che utilizza il routing a distanza vettoriale. Interior Gateway Routing Protocol (IGRP) è un'eredità protocollo di Cisco che utilizza anche il routing vettoriale a distanza. Apri prima il percorso più breve (OSPF) è un protocollo gateway interno che offre più robustezza del RIP. Border Gateway Il protocollo (BGP) è un protocollo di routing complesso che fornisce la funzionalità backbone di Internet. A fini amministrativi, vengono comunemente utilizzati SSH e HTTPS.

Network address allocation. Per distribuire in modo efficiente e automatico gli indirizzi IP a dispositivi su una rete, il protocollo DHCP (Dynamic Host Configuration Protocol) è più comunemente usato. Il DHCP funziona inizialmente tramite trafc broadcast.

Subscription services. Network News Transfer Protocol (NNTP) è un protocollo legacy utilizzato per comunicare con Usenet, che ospita forum e trasferimento fle. Con NNTP, ti iscrivi ai gruppi desiderati, sia per la discussione che per il trasferimento fle. Quindi, recupera un client messaggi su richiesta o su base programmata. Tradizionalmente, NNTP operava sulla porta 119 (non sicuro) o porta 563 (sicuro). Oggi, NNTP opera spesso su HTTPS.

3. Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure confguration guides

Industry-standard .A volte architetti, ingegneri e amministratori vogliono elaborare i propri progetti, sulla base della propria esperienza e conoscenza. Ma di solito questo non è il percorso migliore. Ognuno ha una diversa esperienza e diversi livelli di conoscenza. Spesso, lavorando in grande ambiente aziendale significa un ritmo più lento di integrazione tecnologica e non essere all'altezza velocità con le ultime soluzioni e pratiche. È una buona pratica rivedere e considerare pubblicamente frameworks disponibili, best practice (soprattutto da parte dei fornitori) e guide di configurazione sicure (sia da venditori che da esperti in materia). Prendi le tue idee, esigenze e lavoro con informazioni pubblicamente disponibili per fornire la migliore architettura e design disponibili.
Questa sezione è focalizzata a un livello superiore rispetto alle operazioni quotidiane. Le aspettative per questa sezione è che capisci le implicazioni di una tecnologia o regolamento, i professionisti e contro di alcune tecnologie e scelte progettuali e di come le tecnologie si integrano con altre tecnologie o in un ambiente per la massima sicurezza. Ci sono 9 sezioni in Architettura e Design.

Industry-standard frameworks and reference architectures

Frameworks. Assicurati di avere familiarità con i frameworks più popolari e comprenderne il valore o necessità di aderire ai quadri (frame works). Le architetture di riferimento non sono specificate di seguito. Le architetture di riferimento sono generalmente pubblicate dai fornitori con l'obiettivo di mostrare design altamente disponibili e ad alte prestazioni dei loro prodotti. Un componente chiave di riferimento l'architettura è supportabilità - le architetture di riferimento sono sempre un'implementazione supportata, che è una considerazione importante quando si decide di architettura e design.

Regulatory. Con i quadri normativi, stai cercando di soddisfare un regolamento specifico in un settore, come parte del lavoro con una tecnologia specifica o come

parte di un governo organizzazione. Un esempio è il PCI (Payment Card Industry Data Security Standard DSS), che regola le organizzazioni che archiviano, trasmettono ed elaborano carta di credito e credito dati del titolare della carta. L'obiettivo di PCI DSS è garantire che le organizzazioni elaborino il credito le carte soddisfano un livello minimo di sicurezza nel modo in cui gestiscono le transazioni con carta di credito.
Le organizzazioni devono essere controllate e certificate in modo indipendente.

MOLTO SPESSO QUELLO CHE E' CERTIFICATO E' GIA' SUPERATO DAL RAPIDO EVOLVERSI DELLA TECNOLOGIA

Non-regulatory. quadri non normativi sono sviluppati con obiettivi simili a quelli regolamentari frameworks: migliorare la sicurezza fornendo informazioni e linee guida alle organizzazioni. Tuttavia, i quadri non regolamentari non sono applicabili. Invece, sono volontari; le organizzazioni possono scegliere di adottarle o meno. Un esempio è la sicurezza informatica NIST Frameworks (vedi https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

National vs international. Molti paesi hanno i loro quadri. Spesso, tali quadri si applicano solo alle agenzie governative o alle organizzazioni che lavorano direttamente con il governo agenzie. Un esempio è il programma americano FedRAMP, che delinea una serie specifica di requisiti per le agenzie governative statunitensi. Vedere https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

per dettagli.

L'International Organization for Standardization (ISO) fornisce quadri in un'ampia varietà di settori, comprese le informazioni di tecnologia. ISO / IEC 27000 ha diversi framework pubblicati per uso internazionale.

Industry-specifc frameworks. I frame per l'industria sono di solito molto specifici alla stessa industria. Un quadro ampiamente noto è la Healthcare Information Portability and Accountability Act (HIPAA), che ha l'obiettivo di proteggere le informazioni di identificazione personale e le informazioni sulla salute personale dei pazienti. Gli operatori sanitari devono dimostrare conformità con l'HIPAA per evitare infortuni e persino sanzioni penali in alcuni scenari.

Benchmarks/secure /confguration guides. Oltre alle architetture di riferimento, i fornitori forniscono spesso documentazione aggiuntiva relativa ai parametri di riferimento delle prestazioni e alla configurazione sicura. Queste non sono

necessariamente guide passo-passo da usare durante un'implementazione, ma una guida di alto livello che offre informazioni per aiutarti a fare delle scelte in base alle tue esigenze. Per l'esame, non è necessario saperlo su singole guide o memorizzare le informazioni in esse contenute.

Platform/vendor-specifc guides:
Web server. I server Web sono altamente suscettibili agli attacchi, quindi molti fornitori di server Web forniscono linee guida per ridurre al minimo il rischio di compromissione. Ad esempio, Apache pubblica suggerimenti sulla sicurezza all'indirizzo https://httpd.apache.org/docs/2.4/misc/security_tips.html.

Operating system. Molti fornitori di sistemi operativi forniscono guide, linee guida o addirittura script per aiutare a proteggere il sistema operativo. Ad esempio, Microsoft pubblica una sicurezza guida per Windows Server 2016 all'indirizzo

https://download.microsoft.com/download/5/8/5/585DF9E9-D3D6-410A-8B51-81C7FC9A727C/Windows_Server_2016_Security_Guide_EN_US.pdf.

Application server. I fornitori di applicazioni pubblicano anche guide e best practice relative all'indurimento e alla configurazione. Un esempio è Oracle; Oracle Middleware Administrator di Oracle è la guida, disponibile all'indirizzo https://docs.oracle.com/cd/E21764_01/core.1111/e10105/toc.htm.

Network infrastructure devices. Molti fornitori forniscono guide per l'implementazione delle loro soluzioni. Ad esempio, NetApp pubblica una guida di rafforzamento della sicurezza per il sistema operativo ONTAP utilizzato nei dispositivi di archiviazione. Vedere https://www.netapp.com/us/media/tr-4569.pdf for the NetApp Security Hardening Guide for NetApp ONTAP 9.

LE GUIDE PER IL CORRETTO FUNZIONAMENTO DEI PRODOTTI ROBIONICA SONO VISIBILI DALLO STESSO PRODOTTO, DOVE, CON LA SELEZIONE DI “read me” COMPARE SULLA GRIGLIA DI OUTPUT LA SERIE DI ISTRUZIONI DA SEGUIRE, AL MASSIMO 2 SCHERMATE SULLA GRIGLIA. LA SEMPLICITA’ OPERATIVA DEI SOFTWARE ROBIONICA, CHE NASCONDE UNA PROFONDA INTELLIGENZA NEGLI ALGORITMI, NON HA BISOGNO DI PESANTI MANUALI

General-purpose guides. Esistono molte guide di uso generale, alcune delle quali esperti in materia, alcuni dei professionisti IT in base alla loro esperienza nel campo, e alcuni da altre fonti. Una guida per scopi generici è lo sviluppatore OWASP di

OWASP Guida, che può aiutare gli sviluppatori a creare applicazioni Web sicure. Vedere https://www.owasp.org/index.php/OWASP_Guide_Project for details.

UNA LETTURA FAREBBE BENE ANCHE A CHI NON E' SVILUPPATORE

Vendor diversity. Affidarsi a un singolo fornitore può mettere a rischio la tua organizzazione, soprattutto quando si ha a che fare con il cloud o un componente chiave dell'infrastruttura. Alcune organizzazioni scelgono di mescolare intenzionalmente i fornitori nella loro infrastruttura IT per garantire che a il problema del singolo fornitore non può interrompere l'intera rete. La diversità dei fornitori offre anche maggiore leva finanziaria nella negoziazione di contratti di licenza e manutenzione.

ANCHE NOI DICIAMO CHE VOGLIAMO ESSERE IN SINERGIA CON GLI ALTRI FORNITORI. CERTO LA NOSTRA GAMMA DI PRODOTTI E' UNICA E PUO' GARANTIRE IL FUNZIONAMENTO SENZA BISOGNO DI SUPPORTO.

NON ABBIAMO BISOGNO DI CONTRATTI DI MANUTENZIONE, SE DECIDIAMO DI CAMBIARE ATTIVITA' POSSIAMO FORNIRE I CODICI SORGENTI AI CLIENTI PIU' AFFEZIONATI. DATO CHE SI TRATTA DI SOFTWARE CON 1000 – 2000 RIGHE DI CODICE (righe pensanti) TECNICI DEL SETTORE QUALIFICATI POSSONO TRANQUILLAMENTE GESTIRE IL PROGETTO E LE EVENTUALI EVOLUZIONI. QUESTO PUO' ESSERE MESSO NEL CONTRATTO DI ACQUISTO DI LICENZE

Control diversity. Per ridurre al minimo il rischio, è necessario utilizzare i controlli IT da diverse aree. Per esempio, è possibile combinare controlli fisici (porte bloccate) con controlli tecnici (autorizzazioni a livello di risorsa). Puoi scegliere di sovrapporre altri controlli. Diversificare il tuoi controlli è una buona pratica per garantire che non si faccia affidamento su un singolo tipo e quindi suscettibile a problemi se quel tipo di controllo fallisce o si degrada.

Defense-in-depth/layered security. Gli esperti concordano sul fatto che l'approccio migliore per proteggere l'ambiente è una difesa a più livelli. Anziché affidandoti a un'unica soluzione di sicurezza (come un edge frewall), costruisci la sicurezza a strati – al bordo, nel mezzo e sui dispositivi client.

QUESTO APPROCCIO E' COMPATIBILE CON I PRODOTTI ROBIONICA

User training. Un approccio a più livelli offre più livelli di protezione e rende più difficile per gli aggressori ottenere l'accesso al proprio ambiente. Come parte di una strategia di sicurezza a più livelli, è necessario formare gli utenti a comprendere le

loro responsabilità, capire dove sono i rischi ed essere in grado di identificare minacce come phishing e Ingegneria sociale. Se disponi di sistemi di sicurezza all'avanguardia ma non formi i tuoi utenti, i tuoi l'organizzazione è a rischio.

FORMARE SUI PRODOTTI ROBIONICA E' SEMPLICE ED ECONOMICO,

INTANTO LEGGETE E CAPITE QUESTO MANUALE

Administrative. I controlli amministrativi sono politiche e procedure che l'organizzazione stabilisce di ridurre il rischio complessivo nel proprio ambiente. Potresti avere un ruolo amministrativo, controllo che garantisce che i dipendenti non si seguano in un edificio chiuso senza scorrere un badge o identificarsi altrimenti con l'altra persona che entra nella porta.

Technical. controlli tecnici sono quelli che usi nella tua configurazione. Per esempio potresti utilizzare le autorizzazioni del sistema fle per limitare l'accesso o potresti impedire determinati tipi di utenti dall'accesso a computer specifici.

Given a scenario, implement secure network

architecture concepts. Per questa sezione, dovresti avere familiarità con tutte le tecnologie sottostanti, incluso quando dovrebbe essere distribuito e i dettagli di alto livello di una distribuzione, ad esempio dove si trovano le cose in una rete e quale scopo servono.

Zones/topologies Assicurati di conoscere tutte queste tecnologie e come differiscono l'una dall'altra:

DMZ. Una zona de-militarizzata (DMZ) si trova in genere ai margini di una rete, a cavallo di Internet e della LAN. È comunemente usato per server e dispositivi rivolti al pubblico, come ad esempio web server per un sito Web pubblico. È comune disporre anche di servizi di proxy inverso e gateway SMTP in una DMZ. In molti ambienti, le risorse nella DMZ sono gestite singolarmente e non con gli stessi strumenti di gestione che gestiscono le risorse LAN.

LA TECNICA DI CRIPTEOS 3001 DI AVERE 2 PC UNO COLLEGATO CON INTERNET E L'ATRO COL CORE BUSINESS CHE DIALOGANO CON MESSAGGI CRITTOGRAFATI PONE IL PRIMO PC IN ZONA DMZ

Extranet. Una extranet è come una DMZ perché viene utilizzata per consentire alle persone al di fuori della tua organizzazione per ottenere l'accesso alle risorse. La differenza principale è che una extranet è utilizzato per partner e fornitori.

UTILIZZANDO PER FORNITORI E PARTNER L'ACCESSO CON IL SOFTWARE KEY-LOCK SI PUO' INTEGRARE LA TECNICA DESCRITTA AL PARAGRAFO PRECEDENTE PONENDO IL PC IN DMZ ZONE A RICONOSCERE GLI UTENTI ABILITATI, FILTRANDO OGNI ALTRO ACCESSO

Intranet. Una intranet è una rete privata utilizzata da dipendenti o altri che lavorano per un organizzazione. Di solito è disponibile solo mentre è direttamente collegato all'organizzazione rete o tramite una VPN. Una intranet è destinata esclusivamente ad uso interno. Nota che le persone a volte si riferiscono a una rete Intranet come sito Web interno dell'azienda anziché globale rete interna.

Wireless. Una rete wireless viene comunemente implementata presso un'organizzazione per facilitare l'accesso alla rete da smartphone, dispositivi di proprietà personale e organizzazione dispositivi che non sono fisicamente collegati a una rete. Per massimizzare la sicurezza, considerarele seguenti opzioni:

Utilizzare i protocolli di sicurezza più recenti. Wi-Fi Protected Access 2 (WPA2) è ampiamente utilizzato e accettabile. Utilizza la crittografia Advanced Encryption Standard (AES). Di recente, WPA3 è diventato disponibile e alla fine sostituirà WPA2. Utilizzare EAP-TLS per proteggere l'autenticazione.
Implementare l'autenticazione a più fattori per l'accesso alla rete.
Implementare un sistema di rilevamento delle intrusioni wireless (WIDS) e un sistema di prevenzione delle intrusioni wireless (WIPS).
Separare l'utilizzo wireless tra dipendenti e visitatori / ospiti.

DATO CHE I SOFTWARE ROBIONICA SONO SCRITTI IN JAVA E NON E' PER ORA POSSIBILE IMPLEMENTARLI SU SMARTPHONE A ALTRI DISPOSITIVI MOBILI, BASTA ACQUISTARE UN TABLET CON SISTEMA OPERATIVO WINDOWS O LINUX PER AVERNE LE POTENTI POSSIBILITA',

POI BASTA ABITUARSI AL NUOVO OGGETTO, MA LA SICUREZZA E' GARANTITA

Guest. Una rete ospite è una rete separata utilizzata per visitatori, ospiti o altre persone non direttamente associato alla tua organizzazione. Riduce il rischio che i computer della tua organizzazione siano esposti a malware perché i dispositivi non gestiti non sono sullo stessa rete come ospiti.

ANCHE IN QUESTO CASO VEDI PARAGRAFO DMZ PRECEDENTE

Honeypots and honeynets. Un honeypot è un singolo sistema informatico distribuito e configurato per attirare gli aggressori e tenerli lì in modo da poter ottenere informazioni su chi sono, dove sono, ciò a cui stanno tentando di accedere e quali tecniche stanno usando.

Honeypot. Un honeypot è specificamente configurato per apparire attraente per un attaccante (per esempio, potrebbe sembrare che sia in esecuzione una versione vulnerabile di una popolare applicazione Web). Un honeynet può essere considerato una raccolta di honeypot ma può contenere solo un singolo honeypot. Un honeynet consente a un'organizzazione di ottenere più dati di un honeypot perché viene considerato tutto il traffico di rete sull'honeynet (in entrata o in uscita) illegittimo e può essere catturato per analisi. Un vantaggio di honeynet e honeypot è che gli aggressori si impegnano con loro, distogliendo la loro attenzione dalle reti e dalle risorse reali.

CON LE SOLUZIONI ROBIONICA TUTTO QUESTO PUO' DIVENTARE INUTILE

NAT. Network Address Translation (NAT) ha due scopi principali: conservare l'IP indirizzi e per mascherare gli indirizzi IP di origine dei computer. Ad esempio, un'organizzazione può configurare NAT in modo che tutti gli utenti che accedono a Internet sembrino provenire da un singolo Indirizzo IP. Senza NAT, tutti gli utenti che accedono a Internet richiedono il proprio IP pubblico indirizzo, che non è possibile a causa della carenza di indirizzi IP pubblici.

Ad hoc. Una rete ad hoc è una rete temporanea, generalmente utilizzata per connettere temporaneamente più computer insieme. Ad esempio, è possibile collegare un vecchio computer a un nuovo computer per facilitare il trasferimento dei dati.

Segregation/segmentation/ isolation. Avere familiarità con i pro e i contro dei vari tipi di segmentazione. Se viene presentato uno scenario che delinea requisiti di sicurezza specifici, dovresti essere in grado di identificare più segmentazioni appropriate per lo scenario.

Physical. Quando si separano fisicamente le reti, si utilizza hardware di rete indipendente come router, switch e frewalls. Questa è considerata una segmentazione più sicura della segmentazione logica o virtuale. Nelle organizzazioni ad alta sicurezza, la segmentazione fisica è spesso la scelta migliore.

Logical (VLAN). La segmentazione logica, in genere utilizzando VLAN, consente di segmentare reti utilizzando la logica del software. I dispositivi sono collegati agli

stessi interruttori e utilizzano gli stessi router e frewalls. Tuttavia, il traffico di trasmissione non può passare tra VLAN e puoi isolare le VLAN per simulare l'isolamento fisico. L'implementazione di VLAN è facile e veloce. Le VLAN sono ampiamente supportate, il che le rende attraenti. Sono ampiamente usate. Sebbene le VLAN siano riconosciute accettabili per praticamente tutti i requisiti di segmentazione, per ambienti ad alta sicurezza in cui la massima sicurezza è il risultato più importante, dovresti guardare alla segmentazione fisica.

Virtualization. Con l'espansione della virtualizzazione, anche le capacità di virtualizzazione si sono espanse. Le moderne tecnologie di virtualizzazione virtualizzano praticamente tutti gli aspetti dell'ambiente, inclusa gran parte della rete. È possibile utilizzare la segmentazione logica (spesso tramite VLAN) senza l'uso di hardware di rete aggiuntivo. La virtualizzazione basata su l'isolamento offre un livello di sicurezza simile alla segmentazione logica della rete.

Air gaps. Un computer con intercapedine d'aria è un computer che non è connesso a Internet o connesso a qualsiasi altro dispositivo connesso a Internet. Computer con intercapedini d'aria o le reti offrono la massima sicurezza per i carichi di lavoro più sensibili. Per esempio, le reti governative si basano su gap aerei per i sistemi più sensibili. Ci sono aspetti negativi negli spazi vuoti d'aria: sono costosi da implementare e mantenere perché è necessario implementare hardware e software dedicati per gestirli e semplici operativi attività, come l'installazione delle ultime patch di sicurezza. diventare compiti che richiedono tempo.

E’ QUELLO CHE FACCIAMO CON CRIPTEOS 3001 , IL PC COMMESSO CON CORE BUSINESS E’ IN CONDIZIONI AIR GAPS

Tunneling/VPN . Una rete privata virtuale è un tunnel sicuro che collega due reti private, due private computer o un computer privato a una rete privata. Inventato nel 1996, le VPN sono utilizzate da praticamente tutte le organizzazioni con una rete privata per consentire ai lavoratori di lavorare in remoto o connettere due volte insieme. Come parte di un'implementazione VPN, dovresti usare il più forte metodo di autenticazione possibile, come EAP-TLS. Inoltre, è necessario utilizzare una soluzione VPN che supporta il metodo di crittografia più efficace disponibile, come IPsec o SSL VPN.

Security device/ technology placamento. Evitare l'uso del protocollo di tunneling point-to-point (PPTP) perché non è più considerato sicuro.
Molti dispositivi di rete hanno più componenti, che comunicano con i dispositivi per fornire funzionalità e migliorare le prestazioni.

ANCHE IN QUESTO CASO CRITTOGRAFIA CRIPTEOS 3001 RISOLVE IL PROBLEMA

Site-to-site. Una VPN da sito a sito è quella che collega due siti (sedi) insieme. Per esempio tu potresti connettere una filiale con la sede centrale aziendale utilizzando una VPN da sito a sito.

Remote access. Una VPN di accesso remoto è quella che consente ai lavoratori remoti di connettersi alla rete di un'organizzazione da qualsiasi luogo su Internet. Le VPN di accesso remoto sono utili per consentire ai lavoratori di lavorare da casa, in un negozio o in qualsiasi altro luogo con una connessione internet.

Sensors. Pensa ai sensori come agenti di raccolta dati. Spesso sono basati su software ma alcuni sono basati su hardware. I sensori funzionano con i dati grezzi, spesso inviandoli ai collezionisti o alla soluzione stessa (come un SIEM).

Collectors. I collezionisti sono agenti che raccolgono dati da sensori o altri input. Essi spesso parla con sensori o altri meccanismi di input. In genere, non comunicano direttamente ai dispositivi; invece, si basano su sensori o altri meccanismi per comunicare con i dispositivi.

Correlation engines. Quando si raccolgono grandi quantità di dati da molti fonti differenti, può essere difficile capire come i dati si collegano ad altri dati. Correlazione i motori sono applicazioni che cercano di stabilire relazioni tra dati diversi, spesso tramite usando l'intelligenza artificiale e l'apprendimento automatico.

Filters. Un filtro è un meccanismo che riduce la quantità totale di dati raccolti o visualizzati. Un filtro è un componente importante perché può ridurre la quantità complessiva di dati ingerire o visualizzare, che può migliorare le prestazioni o accelerare il tempo necessario per la ricerca quello che ti serve. Ad esempio, se hai catturato 10 minuti di traffico di rete utilizzando un protocollo analizzatore, è possibile applicare un display flter per visualizzare solo il protocollo desiderato, come SNMP.

Proxy. Un proxy tradizionale viene distribuito sulla LAN. Attende le richieste Web dai client e quindi inoltra le richieste per conto dei clienti su Internet. I proxy possono memorizzare nella cache contenuto per migliorare le prestazioni. Un proxy inverso viene spesso distribuito in una DMZ. Ascolta per richieste da Internet che vanno a un sistema interno (come un sito Web per ottenere la tua email) e inoltra la richiesta al server interno per conto del cliente.

Firewalls. Storicamente, quando le reti erano più semplici, i frewalls venivano posizionati sul perimetro o sul bordo della rete. Tuttavia, negli ambienti complessi di oggi, i frewalls sono posizionati ai margini della rete, al centro della rete (per ispezionare e bloccare alcuni comunicazioni interne) e internamente (per garantire connessioni business-to-business).

VPN concentrators. I concentratori di VPN si trovano più comunemente sul perimetro di la rete, a volte direttamente collegata a Internet. Questo ha senso, perché collegano i computer da Internet pubblico alla tua LAN.

SSL accelerators. Come un bilanciamento del carico (e spesso lo stesso dispositivo), gli acceleratori SSL sono in genere collocato nella LAN per server interni o nella DMZ per server rivolti al pubblico.

Load balancers. Come un bilanciamento del carico (e spesso lo stesso dispositivo), gli acceleratori SSL sono in genere collocato nella LAN per server interni o nella DMZ per server rivolti al pubblico.

DDoS mitigator. Un mitigatore DDoS è talvolta un dispositivo. In genere si trova ai margini della rete, spesso di fronte a tutto il resto. Ciò ti consente di mitigare gli attacchi DDoS prima che il traffico malevolo entri nella tua rete.

Aggregation switches. Gli interruttori di aggregazione sono responsabili del collegamento insieme di altri interruttori (ad esempio, interruttori di bordo). Questo a volte viene fatto per semplificare la rete e gestione dei cavi. Gli switch di aggregazione si trovano spesso nelle reti aziendali ma raramente trovato in piccole reti.

Taps and port mirror. È possibile utilizzare i tocchi o i mirror delle porte per acquisire le comunicazioni di rete sulla rete. È possibile toccare un interruttore (ad esempio, direttamente collegato a una porta specifica su un dispositivo specifico).

Dominio 3 | Architecture and Design

SDN Le reti difese da software (SDN) in genere risiedono a fianco o integrate con l'infrastruttura di virtualizzazione. Ti consente di distribuire e gestire switch virtuali, router e frewalls virtualmente, tramite software.

Given a scenario, implement secure systems design

La sezione verifica se hai le conoscenze per implementare una progettazione sicura di un sistema, come un computer o un dispositivo informatico. Potrebbe esserti presentato un elenco di requisiti per un implementazione e necessità di sapere quali componenti e tecnologie saranno necessari per soddisfare i requisiti dello scenario.

Hardware/frmware security

Per questi argomenti, l'attenzione è rivolta al livello hardware. Ad esempio, dovresti avere familiarità con l'hardware necessario per ottenere risultati specifici.

FDE/SED. La crittografia dell'intero disco (FDE) è invece l'atto di crittografare un intero disco rigido e non solo lo spazio utilizzato di un disco rigido o di singoli file e cartelle. FDE è meglio della crittografia che crittografa solo lo spazio utilizzato o parti parziali del disco rigido perché crittografa tutto.

CRIPTEOS 3001 CRITTOGRAFA MEZZO GIGA DI DATI IN 80 SECONDI

Le unità con crittografia automatica (SED) crittografano e decodificano automaticamente dati. Spesso utilizzato con i computer, SED consente di utilizzare la crittografia senza problemi, senza realmente effettuarla. Fornisci una password all'avvio e la decrittografia ti consente di usare il disco rigido. Se il disco rigido viene rubato, diventa inutile senza la password per sbloccare la crittografia.

AVERE LA PASSWORD INVECE DI UNA CHIAVE E' UNA DEBOLEZZA

TPM. Un modulo di piattaforma attendibile (TPM) è un chip hardware, spesso incorporato nella scheda madre di un computer, che è responsabile di aiutare a stabilire un processo di avvio sicuro, crittografare le unità disco, proteggere le password e occasionalmente altre funzioni (come per far applicare le licenze software). Il TPM può essere utilizzato da altri componenti del computer, come UEFI o sistemi operativi. Ad esempio, Windows ha la crittografia del disco BitLocker, che può utilizzare un TPM per migliorare la sicurezza della crittografia del disco.

ANCHE QUI SISTEMI DI CRITTOGRAFIA SUPERATI DA CRIPTEOS 3001

HSM. Un modulo di sicurezza hardware (HSM) è un dispositivo fisico utilizzato per operazioni crittografiche. Spesso, gli HSM vengono utilizzati per firmare le chiavi di crittografia. Comunemente, gli HSM sono abituati a proteggere un'infrastruttura a chiave pubblica interna (PKI). Ad esempio, potresti generare il tuo certificato CA principale dal tuo HSM.

ANCHE QUI SISTEMI DI CRITTOGRAFIA SUPERATI DA CRIPTEOS 3001

UEFI/BIOS. Un UEFI e un BIOS hanno lo stesso lavoro: essere l'intermediario tra frmware e sistema operativo all'avvio del computer. Il BIOS è una tecnologia legacy (in dismissione) perché UEFI svolge tutte le stesse attività e non ha le stesse limitazioni. Per esempio, quando si utilizza un BIOS, non è possibile avere

un'interfaccia utente grafica nel pre-avvio ambiente. (QUESTA INTERFACCIA UTENTE E' IL CAVALLO DI TROIA DELLLO START DEI COMPUTER)

Praticamente tutti i computer moderni utilizzano UEFI oggi.

UEFI nasce per superare i limiti di BIOS, condivide col precedente sistema di boot di essere residente in una sezione non volatile di memoria ma l'architettura, nata da un'dea di oltre 15 anni fa, è strutturata in modo diverso

In particolare UEFI permette il boot da dischi rigidi superiore a 2 Tb non utilizzando più MBR a favore ella GPT (GUID Partition Table) che è parte integrante dello standard UEFI con le seguenti novità:

- architettura indipendente da CPU e driver
- ambiente pre-OS direttamente accessibile incluso il supporto della connettività di rete.
- design modulare
- eliminazione del bootloader (di fatto non più necessario se non in casi di ultiboot avanzato)

- esecuzione di moduli firmati (Secure Boot)

IL PROBLEMA DI UEFI E' CHE POSSONO PRENDERE IL CONTROLLO DEL COMPUTER DALL'ESTERNO, SICURAMENTE IL FORNITORE DEL SISTEMA OPERATIVO, MA ANCHE ALTRI. TECNICAMENTE E' POSSIBILE DALL'ESTERNO DISATTIVARE IL COMPUTER.

Secure boot and attestation. Con l'avvio sicuro, un computer ha un elenco di hardware e frmware affidabili. All'avvio, vengono controllati l'hardware e il software, insieme a firme digitali. Se sono conformi, il computer si avvia. In caso contrario, non lo è.

Supply chain. In un attacco alla catena di approvvigionamento, gli aggressori tentano di alterare segretamente l'hardware o software e organizzazioni gonfiabili che acquistano i prodotti. Questo a volte può essere più semplice che irrompere nei sistemi da remoto. Come parte della tua dovuta diligenza, è importante controllare fornitori e l'intera catena di approvvigionamento. Gli attacchi alla catena di approvvigionamento sono stati nelle notizie recentemente. Vedere

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-howchina-used-a-tiny-chip-to-infltrate-america-s-top-companies per dettagli su un recente attacco alla catena di approvvigionamento.

Hardware root of trust. Una radice di attendibilità è un componente che viene eseguito per primo all'accensione di un computer. Ad esempio, quando si avvia uno

smartphone, boot frmware è uno dei i primi componenti da impegnare. È una radice di fiducia.

EMI/EMP. Le armi con interferenze elettromagnetiche (EMI) e impulsi elettromagnetici (EMP) sono armi volte a degradare, danneggiare o eliminare i sistemi elettrici e elettronica. Lo fanno attraverso una breve scarica di energia elettromagnetica che spesso travolge l'elettronica.

Operating systems In questa sezione, i sistemi operativi si riferiscono a sistemi operativi per computer generici (come Windows e Linux) nonché sistemi operativi appositamente creati, come quelli incorporati in un'appliance o uno smartphone.

Types. Preparati a distinguere tra le diverse caratteristiche dei tipi di sistemi operativi per l'esame.

Network. Un sistema operativo di rete è sinonimo di un funzionamento basato su server sistema. Il termine è usato raramente oggi perché praticamente tutti i sistemi operativi server sono anche sistemi operativi di rete. Molto tempo fa, era un sistema operativo di rete un sistema basato su server che ha fornito servizi ai client su una LAN. Protezione di una rete il sistema operativo è come un sistema operativo server; vedi il prossimo proiettile per i dettagli.

Server. Un sistema operativo basato su server è appositamente progettato per eseguire servizi - di piccole dimensioni
applicazioni che forniscono un servizio agli utenti finali o altri software. Per esempio, un server creato come server di posta elettronica avrebbe servizi a cui inviare posta elettronica in uscita ricevi email in entrata e scansiona email per malware. Alcuni operativi basati su server i sistemi hanno un'interfaccia utente grafica ma altri no, per maggiore sicurezza e prestazioni. Un server è spesso protetto tramite un criterio centralizzato (come un criterio di gruppo oggetto in un ambiente Active Directory). Altri modi comuni per proteggere un server includere rimanere aggiornati sulle ultime patch, disabilitare i servizi non necessari, aderire secondo il principio del privilegio minimo e il monitoraggio e il controllo di tutte le attività del server.

Workstation. Un sistema operativo per workstation è un sistema operativo basato su client per le persone da utilizzare quotidianamente al lavoro oa casa. Una workstation operativa il sistema generalmente ha una GUI ed è progettato per essere facile da usare e altamente compatibile hardware di consumo. È possibile proteggere le workstation utilizzando i criteri (in particolare quelli applicati da un punto di gestione centrale), disabilitando software e funzionalità non necessari, eseguendo software anti-malware e installando regolarmente aggiornamenti del sistema operativo.

Appliance. Un'appliance è un dispositivo hardware specializzato, che esegue spesso un sistema operativo specializzato creato appositamente per l'appliance. Tali sistemi operativi sono più piccolo di un tipico sistema operativo basato su server, esegue meno servizi e offre meno caratteristiche. A causa della ridotta funzionalità, gli apparecchi possono talvolta essere più sicuri rispetto ai sistemi operativi server (anche se a volte è vero il contrario).
La protezione di un'appliance richiede informazioni da parte del fornitore oltre a quelle interne test e sperimentazione.

Kiosk. Un chiosco è un computer appositamente costruito spesso utilizzato in uno spazio pubblico per i clienti, ospiti o lavoratori. Ad esempio, molti aeroporti offrono chioschi per consentire il check-in dei file per voli. Molti dei principali sistemi operativi offrono versioni kiosk. Chiosco operativo i sistemi sono molto più piccoli di un tipico sistema operativo del computer perché i chioschi offrono funzionalità minime, come il check-in per il tuo volo in aeroporto o prelevare denaro presso un bancomat. I sistemi operativi Kiosk sono talvolta integrati nell'hardware e possono essere difficili da aggiornare e mantenere. A causa di ciò, i chioschi possono essere vulnerabili agli attacchi. È buona norma tenere i computer dei chioschi, soprattutto quelli messi a disposizione del pubblico, sulla propria rete segmentata con la propria connessione Internet dedicata.

COME DICEVAMO CON LA TECNICA CRIPTEOS 3001 DEL PONTE LEVATOIO SI PUO' COSTRUIRE UN KIOSK SICURO

Mobile OS. Un sistema operativo mobile è progettato per gli smartphone; Android e iOS sono i due principali sistemi operativi mobili oggi. Come gli smartphone hanno ottenuto di più anche potenti sistemi operativi mobili. In molti modi, sistemi operativi mobili sono come i sistemi operativi delle workstation. In quanto tali, sono suscettibili agli attacchi, come postazioni di lavoro. È buona norma eseguire l'ultima versione del sistema operativo mobile, eseguire software anti-malware e disinstallare tutto il software e i servizi non necessari.

Patch management. Mentre abbiamo avviato la gestione delle patch nel sistema operativo sezione, si applica anche su tutta la linea a tutti i dispositivi informatici - smartphone, router, switch, punti di accesso wireless, telecamere intelligenti, ecc. Molti esperti di sicurezza concordano che il singolo passo più importante che le organizzazioni possono adottare è quello di fare in modo coerente di installare gli aggiornamenti di sicurezza non appena vengono rilasciati. Come parte della gestione delle patch strategia, assicurati di testare tutti gli aggiornamenti in ambienti non di produzione per assicurare la funzione e non introdurre problemi.

Disabling unnecessary ports and services. Quando parliamo di porte non necessarie e servizi, stiamo parlando di funzionalità integrate in un sistema operativo o dispositivo ma che non si sta utilizzando e non si intende utilizzare. Ad esempio, spesso viene fornito un server, un servizio di trasferimento fi le come un server FTP (porta 20 e 21). Se non ti serve, puoi farlo disabilitare o rimuoverlo. Le workstation spesso dispongono di un servizio di condivisione desktop remoto
(ad esempio Connessione desktop remoto che utilizza la porta 3389) che è possibile disabilitare se non prevedi di usarlo.

La disabilitazione di porte e servizi non necessari riduce la totale impronta del tuo computer o dispositivo, che migliora la sicurezza.

Least functionality. Un sistema con funzionalità minima è progettato per fornire il minimo funzionalità richiesta per lo scenario. In precedenza, abbiamo menzionato chioschi negli aeroporti - questo è una minima implementazione di funzionalità. Con computer di uso generale come workstation, è difficile ottenere la minima funzionalità. Tuttavia, puntare a questo è un buon modo per iniziare.

Secure confgurations. Le configurazioni sicure sono configurazioni che sono state ritenute sicure, dalla tua organizzazione dopo i test, dai fornitori o da consulenti di terze parti fidati. Le organizzazioni spesso standardizzano l'installazione del sistema operativo in base a una configurazione sicura nota.

Trusted operating system. Un sistema operativo affidabile è in grado di offrire sicurezza e audit sufficienti per soddisfare i requisiti governativi comuni. I criteri comuni sono uno standard internazionale utilizzato per classificare i sistemi operativi come sistemi operativi affidabili.
La maggior parte dei principali sistemi operativi oggi, come Windows Server 2019 e MacOS 10.14, sono considerati sistemi operativi affidabili.

I SISTEMI OPERATIVI CHE VENGONO MESSI SUL MERCATO CON TEST FINALI ESEGUITI DAI CLIENTI NON SONO AFFIDABILI. GLI ERRORI DIVENTANO VULNERABILITA' . IL CROWD TESTING E' UNA TECNICA BUONA SOLO PER GLI AFFARI DEL PRODUTTORE; MA APRE VORAGINI DI SICUREZZA INFORMATICA

Application whitelisting/blacklisting. Molti sistemi operativi offrono altre applicazioni whitelisting (consentendo l'esecuzione delle app) e blacklist (disabilitando l'esecuzione delle app). È una buona pratica per sfruttare queste funzionalità. Hai un paio di opzioni: Disabilita tutte le app tranne quelle che sono autorizzate (la più sicura ma difficile da implementare correttamente) o abilitano

l'esecuzione di tutte le app tranne quelle che sono nella lista nera (un'implementazione comune che consente di bloccare le app specifiche).

Disable default accounts/passwords.Vengono costruiti molti dispositivi e dispositivi informatici con account e password predefiniti. Ciò consente agli acquirenti di configurare rapidamente i dispositivi e utilizzarli. Tuttavia, molte persone non cambiano mai le password predefinite o quelle predefinite, le configurazioni e alcuni dispositivi possono essere controllati da remoto con le credenziali predefinite.

Un passaggio fondamentale per proteggere i dispositivi è modificare tutte le password predefinite durante l'installazione (in particolare prima di connettere i dispositivi a Internet) e utilizzare account speciali da amministrare i dispositivi. Ad esempio, creare un utente di nome Chris per eseguire funzioni di amministrazione e disabilitare l'account integrato, se possibile.

NON BASTA. MEGLIO LE SOLUZIONI ROBIONICA

Peripherals Un'area di sicurezza spesso dimenticata sono le periferiche. In questa sezione, ne esamineremo alcuni delle considerazioni sulle periferiche più popolari.

Wireless keyboards. Le tastiere wireless a volte sono sensibili alla frequenza radio Dirottamento del segnale (RF). Gli aggressori usano un semplice strumento per intercettare le comunicazioni con l'intento di acquisire password o iniettare i propri tasti, e infine subentrare a computer con malware. Mentre la comunicazione tramite tastiera wireless è talvolta crittografata, dovresti essere consapevole del potenziale di attacco. Tastiere Bluetooth, che sono più popolari rispetto alle tastiere wireless oggi, non sono attualmente vulnerabili. Si noti che nella tastiera wireless i segnali possono spostarsi di alcune centinaia di metri.

Per evitare questo attacco, usa una tastiera cablata.

Wireless mice. I mouse wireless sono anche sensibili al dirottamento del segnale RF. Gli aggressori possono utilizzare l'automazione per rilevare un computer con un mouse wireless vulnerabile.

Per evitare questo attacco, usare un mouse cablato.

Displays. Gli amministratori non pensano spesso ai display quando si tratta di sicurezza. Ma shoulder surfing (l'atto di osservare qualcuno in segreto mentre svolgono i loro compiti informatici) è un problema serio che può comportare il furto di credenziali o altri problemi. Per ridurre al minimo il rischio di shoulder surfing, usa schermate private. Schermate sulla privacy allegate al display e

limitare severamente il campo visivo; le persone in piedi di lato o dietro di te non devono vedere chiaramente il display.

CON KEY_LOCK ANCHE SE VEDONO IN CHIARO LA PASSWORD DELLA BANCA SUL MONITOR, SUL SITO DELLA BANCA LA PASSWORD E' STATA CAMBIATA CON UNA GENERATA ALGORITMICAMENTE DI LUNGHEZZA DOPPIA.

LO SHOULDER WATCHER E' BENEFICO QUANDO SCOPRE COLLEGHI IMPEGNATI IN VIDEOGIOCHI!

WiFi-enabled MicroSD cards. Le fotocamere digitali degli ultimi modelli sono spesso dotate o sfruttano le schede MicroSD con WiFi integrato. Ciò consente a un fotografo di scattare immagini e li trasferiscono automaticamente su un altro dispositivo o su un cloud posizione di archiviazione. Questo è conveniente perché il fotografo non deve toglierlo la scheda MicroSD, inserirla in un altro dispositivo e copiare manualmente le immagini. Tuttavia, alcune di queste carte sono suscettibili agli attacchi. Gli attacchi noti possono intercettare la comunicazione e ottenere l'accesso ai dati.

In ambienti ad alta sicurezza, come fotografare una scena del crimine, evitare l'uso di schede MicroSD abilitate WiFi.

EVITARE SEMPRE. OGNI IMMAGINE PUO' ESERE FONTE DI RICATTO

Printers/MFDs. Stampanti e dispositivi multifunzione (DMF, che in genere offrono una stampa, scansione e invio di fax) a volte sono oggetto di attacchi. Gli attaccanti tentano di ottenere una copia di tutti i documenti stampati, scansionati o inviati via fax. Perché questi dispositivi si collegano spesso a rete aziendale, e talvolta una directory aziendale, sono spesso accessibili da ovunque su una rete aziendale, e talvolta anche su Internet. Inoltre, questi dispositivi spesso offrono un'interfaccia web, un server FTP o altri metodi di connettività.
Per massimizzare la sicurezza, assicurati di mantenere aggiornato il software e di disabilitare funzionalità non necessarie.

External storage devices. I dispositivi di archiviazione esterni vengono spesso utilizzati per dati temporanei trasferimento o per backup. A volte, questi dispositivi di archiviazione esterni sono accessibili in remoto tramite un'interfaccia Web o un protocollo di trasferimento file come FTP. Per massimizzare la sicurezza, utilizzare la crittografia completa del disco e disabilitare tutta la connettività remota ai dispositivi. Affidati alla connettività locale, ad esempio tramite USB.

Digital cameras. Le fotocamere digitali si collegano a dispositivi informatici tramite USB o simili con metodi cablati. A volte, possono anche connettersi ai dispositivi utilizzando WiFI o un altro metodo senza cavo. Come i dispositivi di archiviazione, fai affidamento sui metodi cablati per massimizzare la sicurezza. Mantenere anche la tua fotocamera aggiornata.

Explain the importance of secure staging deployment concepts

La rete di produzione di un'azienda deve essere disponibile 24/7/365 per massimizzare le prestazioni complessive, ridurre i costi e ridurre i rischi. Per allinearsi ai requisiti di disponibilità di una rete di produzione, è necessario utilizzare reti non di produzione per testare le modifiche di configurazione, gli aggiornamenti del software e altre modifiche all'ambiente. Dopo aver convalidato una modifica in un ambiente non di produzione (o, meglio ancora, in più ambienti non di produzione), puoi procedere con il cambiamento nel tuo ambiente di produzione.

QUI SI PARLA DI AZIENDE CON UNA STRUTTURA IMPORTANTE. PER PICCOLE AZIENDE E MICROAZIENDE LA PROBLEMATICA E' DIVERSA.

VEDIAMO LA STRUTTURA STANDARD DELLO SVILUPPO SOFTWARE

Sandboxing . Pensa a una sandbox come fanno i bambini: un posto dove giocare. Quando i bambini giocano in una sandbox, pensano a esplorare, sperimentare e divertirsi. In un ambiente IT, un sandbox è considerato l'ambiente in cui inizialmente si testano le cose. Ad esempio, se stai pensando di distribuire un importante aggiornamento dell'applicazione a un'app chiave, potresti provarlo in un sandbox prima. Se hai uno strumento di rete nuovo di zecca che stai valutando, potresti provare in una sandbox. I sandbox sono belli da avere, ma quando le organizzazioni non hanno un sandbox, di solito usano un ambiente di sviluppo per sandboxing e sviluppo.

Environment .Acquisire familiarità con i diversi ambienti descritti qui. Dovresti essere in grado di scegliere l'ambiente appropriato in base a un determinato scenario. Ad esempio, se si desidera eseguire un test in un ambiente che assomigliava di più alla produzione, quale ambiente useresti? Continua a leggere per vedere la risposta.

Development. Un ambiente di sviluppo è il primo ambiente utilizzato per lo sviluppo o il test del codice, dopo un sandbox. Mentre un sandbox è un ambiente facoltativo, un ambiente di sviluppo è spesso un ambiente obbligatorio per le organizzazioni che utilizzano a ciclo di vita sicuro dello sviluppo software (SDLC).

Test. Un ambiente di test viene utilizzato dopo un ambiente di sviluppo. Assomiglia più da vicino a un ambiente di produzione che a un ambiente di sviluppo, ma non così vicino un ambiente di stadiazione.

Staging. Un ambiente di gestione temporanea è l'ultimo ambiente per i test prima di un ambiente di produzione. Un ambiente di gestione temporanea viene talvolta definito test di accettazione (AT) o ambiente di collaudo universale (UAT). Questo ambiente ricorda molto da vicino la produzione.

Production. L'ambiente di produzione è l'ambiente live. Alla quale le aziende fanno affidamento per mantenere il business in esecuzione, mantenere i clienti felici e fare soldi. L'ambiente non deve mai essere utilizzato per i test o essere modificato prima che le modifiche vengano testate in ambienti di non produzione.

Secure baseline . Una base sicura è un modello, una configurazione, un codice o un'immagine che la società considera sicuro. Ad esempio, un'azienda potrebbe avere una base sicura per i propri dispositivi Windows 10. La linea di base viene utilizzata ogni volta che l'azienda distribuisce un nuovo dispositivo Windows 10. I benefici di una base sicura include avere una configurazione coerente (tutti i dispositivi iniziano allo stesso modo),ridurre l'errore umano (perché una linea di base sicura viene riutilizzata ripetutamente) e risparmiare tempo (no dover eseguire le attività di configurazione iniziale ogni volta che viene distribuito un dispositivo).

Puoi applicare concetti simili alle configurazioni delle app e ad altre aree del tuo ambiente. Dopo che un dispositivo è stato distribuito, tende a deviare dalla configurazione iniziale (la linea di base sicura). Più a lungo è attivo un dispositivo, più tende a spostarsi.

Integrity measurement. Per garantire la conformità con la base sicura, le organizzazioni si rivolgono a soluzioni di gestione della configurazione. Le soluzioni di gestione della configurazione possono applicare le impostazioni di base sicure. Per esempio, ogni ora, il software di gestione della configurazione può verificare la configurazione corrente sulla base sicura e regola le impostazioni che non si allineano.

Le organizzazioni spesso combinano i criteri (basati su server o centralizzati in Active Directory o un servizio di directory simile) con la gestione della configurazione. Con le politiche, è possibile impedire le modifiche a impostazioni di sistema critiche.

Explain the security implications of embedded systems. I sistemi integrati sono in genere ambienti operativi incorporati nell'hardware di a dispositivo specializzato. In questi casi, hai accesso limitato o inesistente all'hardware o ai componenti. In molti casi, l'hardware non è riparabile dall'utente. Le opzioni tendono ad essere più limitate, quindi la scelta il fornitore e la soluzione giusti sono importanti.

SCADA/ICS Il controllo di supervisione e l'acquisizione dei dati (SCADA) si riferiscono a sistemi di controllo geograficamente dispersi, come quelli che controllano la distribuzione di energia o acqua. Industrial Control Systems (ICS) è un termine più ampio che si riferisce a sistemi di controllo industriale automatizzato. ICS è tutto ciò che riguarda i sistemi di controllo industriale mentre SCADA si riferisce geograficamente sistemi di controllo dispersi prevalenti nelle utility. Perché SCADA e ICS sono legati componenti infrastrutturali di grandi dimensioni e critici, la sicurezza è della massima importanza. Gli aggressori possono abbattere le reti elettriche, interrompere le forniture di acqua o gas o interrompere in altro modo le principali utilità.

Smart devices/IoT
SoC -RTOS. I dispositivi intelligenti e i dispositivi IoT sono dispositivi connessi a Internet o a una rete che usano la tecnologia per migliorare la loro funzionalità. Ad esempio, un orologio intelligente può rilevare se sei stato seduto tutto il giorno e ti chiede di alzarti e muoverti. Un frigorifero intelligente può inviare un avviso quando si è a corto di latte o è necessario sostituire il filtro dell'acqua.

HVAC. Come altri dispositivi, i sistemi HVAC hanno iniziato a connettersi alle reti wireless e a Internet. Ciò consente di accendere, spegnere o controllare in altro modo il sistema HVAC da qualsiasi luogo. È conveniente, ma aumenta il rischio che un utente malintenzionato possa maliziosamente accedere al tuo sistema HVAC. Mentre rendere la tua casa o il tuo business troppo freddo o troppo caldo non è un enorme preoccupazione per la sicurezza, un utente malintenzionato potrebbe riscaldare la sala server o il data center per causare a denial of service quando i server si spengono a causa del surriscaldamento.

SoC . Per questa sezione, SoC si riferisce al sistema su un chip, non al centro operativo di sicurezza. Dispositivi SoC sono sostanzialmente piccoli computer su un chip, come un Raspberry Pi (che ha un SoC più altri componenti hardware). Perché questi sono come i computer, a volte sono sensibili agli attaccanti. Le implicazioni variano a seconda dell'uso del dispositivo. Le preoccupazioni comuni, sono accesso remoto non autorizzato e protezione dell'accesso fisico.

BISOGNA DIFENDERE IL PERIMETRO DEL CORE BUSINESS DA ATTACCHI DELL'INTERNET OF THINGS CON CRIPTEOS 3001 NELLA VERSIONE PONTE LEVATOIO

RTOS.Un sistema operativo in tempo reale (RTOS) è un sistema che elabora le richieste in una quantità specifica di tempo. Un sistema operativo standard, come Windows 10, elabora le richieste in ordine e il tempo di consegna varia; non ci sono garanzie sulla quantità di tempo di elaborazione ci vorrà per eseguireun compito. I sistemi RTOS sono in genere integrati e i tempi di risposta sono importanti funzionalità dell'implementazione. Come qualsiasi sistema operativo, ci sono implicazioni per la sicurezza - vale a dire accesso non autorizzato, DoS ed escalation di privilegi.

Wearable technology. La tecnologia indossabile comprende camicie, giacche, zaini, orologi, occhiali e altri dispositivi indossabili. Spesso questi dispositivi si connettono ad altri dispositivi, ad esempio come smartphone (ad esempio via Bluetooth). Come minimo, le implicazioni di sicurezza includono la perdita di informazioni di identificazione personale e informazioni sulla salute (gli smartwatch possono monitorare la frequenza cardiaca, il livello di attività, i modelli di sonno e altri tipi di organi vitali).

Home automation. Il mondo dell'automazione domestica è ampio e continua a crescere. Ci sono telecamere, sistemi di sicurezza, sistema di illuminazione, sistemi audio, interruttori, persiane e sistemi ingresso. Praticamente tutti i dispositivi di automazione domestica si connettono tra loro, connettersi a hub o sistemi di controllo centrale o connettersi a Internet. In alcuni casi, si connettono a tutte quelle cose! Le implicazioni per la sicurezza sono varie. Una preoccupazione comune è l'accesso non autorizzato alla struttura (casa o ufficio).

Ad esempio, immagina di connettere un Alexa, dispositivo abilitato a una porta del garage o catenaccio intelligente. Dici "Alexa, apri il garage" per aprire la porta del garage. Chiunque può dirlo, anche da fuori casa. I venditori stanno iniziando ad aumentare la sicurezza per gestire questo tipo di attività. Ad esempio, i dispositivi possono chiedere un PIN prima di eseguire un'attività. Poiché molti di questi dispositivi controllano l'accesso o le telecamere di sicurezza, esistono altri rischi per la sicurezza, come furto con scasso o copertura di accesso non autorizzata cancellando i filmati di sicurezza. Gli aggressori possono assumere un dispositivo di automazione domestica e provare a usarlo per assumere il controllo dei tuoi dispositivi informatici se condividono la stessa rete.

FORSE E' MEGLIO RIPENSARE LA VALIDITA' DI QUESTE INNOVAZIONI?

Printers/MFDs .Le implicazioni di sicurezza di stampanti e dispositivi multifunzione sono legate alla perdita di dati. Immagina che tutto ciò che tutti hanno stampato nella tua azienda è stato segretamente inviato a un hacker, e poi pubblicato il materiale sul web oscuro (dark web). Oppure immagina che tutto sia stato digitalizzato dai tuoi dipendenti è stato inviato di nascosto al tuo concorrente. Queste sono alcune delle implicazioni per questi dispositivi.

Camera systems. Con i sistemi di telecamere collegati a reti o Internet, è necessario pensare allefoto e i video dalle telecamere. Chi può accedervi? Cosa accadrebbe se tutte le immagini e video sono diventati pubblici? Altre implicazioni di sicurezza sono la disabilitazione dei sistemi di telecamere o riconfigurazione dei sistemi di telecamere (ad esempio, per indicare un muro o interrompere la registrazione). NEGLI EVENTI DI SICUREZZA INFORMATICA DANNO COME GADGET UNA COPERTURA PER LA WEBCAM DEL TELEVISORE NELLA TUA CAMERA DA LETTO!

Special purpose . I dispositivi per scopi speciali sono quelli che hanno una distribuzione limitata per uso specializzato. Tipicamente, non trovi questi tipi di dispositivi in una casa o in un'azienda.

Medical devices. Tutti i dispositivi che vedi infermieri e dottori utilizzano in un ospedale o ufficio medico si qualificano come dispositivi medici. Per l'esame, ci concentriamo su dispositivi collegati (cablati o wireless). Questi dispositivi memorizzano o trasmettono informazioni sensibili sulla salute e informazioni per il paziente. Le implicazioni per la sicurezza sono di ampia portata, incluso il mancato rispetto di regolamenti come l'HIPAA, che diventano oggetto di un'azione legale di classe, in corso di valutazione sanzioni e perdita di affari.

IL REGOLAMENTO EUROPEO DELLA PRIVACY, GDPR, STABILISCE IMPORTANTI LIMITAZIONI SUI DATI SENSIBILI CHE CONTENGONO INFORMAZIONI SULLA SALUTE.

PECCATO CHE IN ITALIA HANNO UNIFICATO LA TESSERA SANITARIA CON LA TESSERA CONTENENTE IL CODICE FISCALE, QUINDI PER ESIBIRE IL CODICE FISCALE DOBBIAMO DARE LA TESSERA SANITARIA, SE L'INTERLOCUTORE E' MALINTENZIONATO CI SONO PROBLEMI

Vehicles. Negli ultimi anni, molte auto sono ora connesse a Internet. Alcun auto hanno intelligenza artificiale e possono guidare se stesse. Molti hanno sistemi di

frenata di emergenza automatizzati. Gli attaccanti hanno mostrato attacchi a prova di concetto in cui disabilitano a distanza un'auto o un altro veicolo o compromettono il loro regolare funzionamento. Le implicazioni di sicurezza sono legate alla sicurezza dei passeggeri e di coloro che li circondano.

Se un attaccante può controllare da remoto un'auto o disabilitare un'auto su un'autostrada o su un sistema stradale ad alta velocità, è estremamente pericoloso.

Aircraft/UAV. Limitare gravemente il controllo remoto è un passo importante per proteggere un aereo. Tuttavia, ci sono implicazioni di sicurezza dall'interno dell'aeromobile, come interferenze con l'elettronica del velivolo, che potrebbe causare un malfunzionamento o provocare un incidente. Con veicoli aerei senza equipaggio (UAV), il controllo remoto è una caratteristica fondamentale, quindi è importante proteggere le comunicazioni. Per i sistemi basati sui consumatori, includono le implicazioni di sicurezza degli UAV invasione della privacy (ad esempio un UAV che scatta segretamente foto di te nel tuo cortile) e perdita di dati (ad esempio, copia o eliminazione di tutti i dati registrati dall'UAV).

Summarize secure application development and deployment concepts. Abbiamo parlato dell'importanza di una sicurezza a più livelli. Un tale approccio inizia con lo sviluppo di applicazioni. All'inizio dello sviluppo del software, la sicurezza non era una considerazione. Man mano che Internet cresceva in popolarità, divenne chiaro che la sicurezza è un concetto chiave. Microsoft ha introdotto Trustworthy Computing nel 2002 per abbracciare la sicurezza in tutto il mondo ciclo di vita dello sviluppo, al di fuori dello sviluppo.
Mentre la popolarità di DevOps e la consegna rapida aumentavano, le organizzazioni avevano bisogno di un modo per farlo incorporare i loro team di sicurezza nei progetti in precedenza. Invece di avere una revisione della sicurezza presso fine di un progetto, le organizzazioni trovano valore nell'includere i membri del team di sicurezza dall'inizio di un progetto. Perché i team di sicurezza si fondano perfettamente con i team DevOps, devono usare automazione. Con l'automazione, i team di sicurezza possono muoversi rapidamente, come un team DevOps.
Combinando la sicurezza con DevOps ti offre Secure DevOps, a volte indicato come DevSecOps.

Development lifecycle models
Secure DevOps

QUI SI CITANO DIVERSI MODELLI DI SVILUPPO SOFTWARE, MA ROBIONICA PROPONE I SOFTWARE RIAN, GO-DRY E TESTATOR CHE PERMETTONO DI RIDURRE GLI ERRORI QUASI A ZERO,

INDIPENDENTEMENTE DAL MODELLO DI SVILUPPO. PER PROGETTI MOLTO GRANDI BISOGNA SPEZZETTARE IL PROGETTO IN PARTI PICCOLE TESTABILI SEPARATAMENTE, COME DEFINITO DALLA METODICA UML (UNIFIED MODELING LANGUAGE)

Waterfall vs agile. Il metodo a cascata nell'approccio tradizionale allo sviluppo del software: raccogle i requisiti, crea un progetto, sviluppa il codice, fai il giro dei giri di test, risolve qualsiasi problema e quindi consegna un prodotto finale. Il metodo agile è un approccio iterativo organizzato in fasi chiamate "sprint". Per ogni sprint, viene definito un set di risultati.
Uno sprint dura un periodo prestabilito, ad esempio 2 settimane, quindi i progressi vengono erogati regolarmente. I risultati sono difesi dal valore che apportano al cliente e quelli di alto valore vengono consegnati in precedenza in un progetto. I clienti devono essere maggiormente coinvolti nel progetto rispetto all'approccio a cascata.

Security automation. Tradizionalmente, la sicurezza era un insieme manuale di processi. Con DevOps, soprattutto DevSecOps, l'automazione è diventata molto importante. Parte dell'abilitazione dell'automazione è abbracciare un concetto noto come "infrastruttura come codice" o "sicurezza come codice". quando
i team di sicurezza possono utilizzare il codice per distribuire e applicare la sicurezza, accelera i tempi di implementazione, migliora la coerenza e consente di integrare la sicurezza nel progetto dall'inizio.

Continuous integration. Tradizionalmente, la sicurezza era un insieme manuale di processi. Con DevOps, soprattutto DevSecOps, l'automazione è diventata molto importante. Parte dell'abilitazione dell'automazione è abbracciare un concetto noto come "infrastruttura come codice" o "sicurezza come codice". Quando i team di sicurezza possono utilizzare il codice per distribuire e applicare la sicurezza, accelera i tempi di implementazione, migliora la coerenza e consente di integrare la sicurezza nel progetto dall'inizio.

Baselining. Baselining è un metodo per confrontare ciò che hai con un set di metodo precedentemente stabilito. È possibile basare i requisiti del progetto, la configurazione del sistema operativo e codice pari. Le linee di base sono utili per gli audit e la risoluzione dei problemi

Immutable systems. In un ambiente server tradizionale, i server sono distribuiti e quindi gli amministratori li aggiornano, li aggiornano e cambiano le loro configurazioni. Con sistemi immutabili, se sono necessarie modifiche dopo la distribuzione dei server, nuovi server hanno implementato tali modifiche. Se è

necessario un aggiornamento, nuovi server con l'aggiornamento
sono distribuiti. Con i sistemi immutabili, tutti i server o altri componenti sono uguali. L'infrastruttura immutabile fornisce coerenza e prevedibilità alla tua infrastruttura.

Infrastructure as code. Infrastruttura come codice (IaC) è un metodo per gestire la tua infrastruttura (virtualizzazione, server, tecnologie di rete) utilizzando il codice e l'automazione. Iac aiuta a prevenire la bozza di configurazione, garantisce coerenza nell'infrastruttura e riduce errore umano.

Version control and change management. Il controllo della versione è un processo mediante il quale si assegna un numero di versione all'applicazione o codice. Ad esempio, la versione iniziale dell'applicazione potrebbe essere la versione 1.0. Dopo aver fissato il primo set di bug, potresti rilasciare la versione 1.01. Piccoli aggiornamenti al codice sono piccoli incrementi per la tua versione mentre i principali aggiornamenti al codice (come la prossima versione di un'app) hanno grandi incrementi alla tua versione (ad esempio da 1.9 a 2.0).

Il controllo della versione consente di tenere traccia delle modifiche al tuo codice, insieme a quando sono state introdotte tali modifiche. La gestione del cambiamento è il processo di gestione dei cambiamenti in un ambiente. Le modifiche in un ambiente potrebbero essere correlate a una versione dell'applicazione, a un aggiornamento del server oa una modifica della configurazione di rete. Le organizzazioni utilizzano la gestione delle modifiche per garantire che vi sia una documentazione adeguata per le modifiche pianificate, che ci sia un adeguato test delle modifiche in anticipo e che le modifiche abbiano luogo durante finestre di manutenzione note.

Provisioning and deprovisioning .Il provisioning è il processo di distribuzione. Il deprovisioning è il processo di disattivazione. Ad esempio, se si sta preparando la distribuzione di una nuova applicazione nell'ambiente di produzione, potrebbe essere necessario eseguire il provisioning di 16 server Web, 4 server di database e 4 server di app.

Secure coding techniques. Per massimizzare la sicurezza della tua applicazione, è necessario includere la seguente protezione tecniche di codifica:

Proper error handling. Uno degli scopi principali della gestione degli errori è assicurarsi che il la tua applicazione si arresta in modo sicuro senza restituire informazioni sensibili, come ad esempio informazioni che potrebbe portare l'attaccante a conoscere meglio la tua rete, le versioni del software o i dettagli della tua configurazione. È buona norma mantenere i messaggi di errore generici per

gli utenti finali. Ad esempio, potresti ricevere un messaggio di errore che dice "Qualcosa è andato storto. Vi preghiamo di provare di nuovo più tardi."

Proper input validation. Le applicazioni spesso richiedono input dagli utenti. Ad esempio, un'applicazione webbased potrebbe chiederti di fornire il tuo indirizzo email o di scegliere un'opzione in un menu a discesa. Per massimizzare la sicurezza, tutti gli input devono essere convalidati per essere sicuri. La convalida deve verificare la lunghezza corretta (ad esempio, se si richiedono le ultime 4 cifre di un numero di telefono, l'input deve essere lungo 4 cifre) e il tipo di carattere corretto (ad esempio, se stai chiedendo il cognome di qualcuno in inglese, allora l'input dovrebbe consistere solo di lettere dell'alfabeto inglese). Senza una corretta convalida dell'input, si esegue il rischio di comportamento imprevisto dell'applicazione che potrebbe causare un incidente di sicurezza.

Normalization. Ci sono un paio di modi per pensare alla normalizzazione. Un modo è prendere input o dati memorizzati e standardizzazione del modo in cui sono memorizzati. Ad esempio, se hai un database di informazioni di contatto del cliente, è possibile convertire "California", "California", "Cali", "S.
CA "e" N. CA "a" CA ". Allo stesso modo, potresti convertire i numeri di telefono "213.555.1212" e da "213 / 555-1212" a "213-555-1212". Un altro modo di pensare alla normalizzazione è da una prospettiva di database. Implica un obiettivo simile: standardizzare il modo in cui i dati vengono archiviati. Con database, è inoltre possibile ridurre la ridondanza dei dati.

Stored procedures. Le procedure memorizzate sono istruzioni SQL (si pensi allo "script di database") utilizzate per una varietà di scopi. Ad esempio, puoi trovare informazioni dettagliate sul tuo database, inserire dati nel database o persino eseguire il backup del database.

Code signing. È possibile utilizzare un certificato per firmare il codice. Quando si firma il codice con una firma digitale, viene identificato l'autore del codice. Inoltre, c'è un hash del codice che consente ad altri di vedere se il codice è cambiato da quando è stato firmato. La firma del codice è a buona prassi per garantire che il codice possa essere convalidato come legittimo.

Encryption. Esistono molti modi per utilizzare la crittografia con il codice. Puoi crittografare il tuo codice a riposo, ed è possibile utilizzare il codice per crittografare l'input o l'output. Per massimizzare la sicurezza, puoi utilizzare la crittografia per archiviare tutte le informazioni riservate, come nomi utente, password, chiavi, percorsi file e nomi dei server interni. Invece di mantenere le informazioni sensibili

in chiaro del testo all'interno del codice, è possibile utilizzare la crittografia per memorizzare informazioni al di fuori del codice e chiamarlo all'interno del codice.

Obfuscation/camouflage. Offuscamento del codice, a volte indicato come camuffamento del codice, è l'atto di rendere il codice difficile da leggere o comprendere, ad esempio è possibile rimuovere tutti i commenti e utilizzare caratteri casuali per i nomi delle stringhe. A volte è stato utlizzato per scoraggiare le persone dal rubare o riutilizzare il codice. Tuttavia, questa è una forma di "sicurezza attraverso l'oscurità ", il che significa che non c'è molto valore in questo metodo perché non rende il codice più sicuro, ma invece richiede solo un po 'più di tempo a interpretalo. Peggio ancora, quando altri sviluppatori della tua organizzazione vogliono basarsi sul tuo codice, rende il loro lavoro più difficile.

Code reuse/dead code. Il riutilizzo del codice è una pratica comune. Il riutilizzo del codice implica il riutilizzo del codice già scritto o così com'è o come punto di partenza in una nuova applicazione. Supponiamo che tu abbia scritto un'applicazione per inserire nuove informazioni in un proprietà database e ora stai scrivendo un'applicazione per aggiungere informazioni a un rivenditore online banca dati; potresti riutilizzare il codice invece di ricominciare da zero. Il riutilizzo del codice può aiutare a ridurre errori e bug e ridurre le ore totali richieste per lo sviluppo.

Codice morto è il codice che non viene utilizzato. Ad esempio, supponiamo di avere un'applicazione da caricare, scaricare e modificare le immagini, ma in seguito si sceglie di rimuovere l'opzione da modificare. Il codice di modifica esiste ancora ma ora è considerato morto.

Server-side vs. client-side execution and validation. All'inizio di questa sezione, abbiamo parlato un po 'di convalida dell'input. È possibile eseguire la convalida sul client (ad esempio, in un browser) o sul server (ad esempio, codice back-end per eseguire la convalida). Convalida presso il sitoil lato client ha alcuni vantaggi: ad esempio, non si invia alcun input non valido al server. Tuttavia, uno degli aspetti negativi è che la convalida del client potrebbe essere ignorata; ad esempio, un utente malintenzionato può utilizzare un front-end personalizzato per comunicare con l'applicazione. La convalida sul lato server ha anche alcuni vantaggi: il codice di convalida si trova su un livello di server e ha potenza aggiuntiva e infrastruttura aggiuntiva, in particolare rispetto alla convalida basata su browser. Inoltre, la convalida sul lato server è difficile da bypassare. È un bene esercitarsi a utilizzare entrambi i tipi di validazione per massimizzare la sicurezza.

Memory management. La gestione della memoria è il processo di ottimizzazione dell'utilizzo di memoria, allocazione della memoria ad applicazioni e servizi e

deallocazione di memoria. Senza la gestione della memoria di proprietà e la convalida dell'input, la tua app potrebbe essere suscettibile di generare attacchi di flusso o altre vulnerabilità.

Use of third-party libraries and SDKs. È possibile utilizzare librerie e SDK di terze parti per salvare tempo e benefici dall'uso di codice che è già stato testato e rivisto. L'aspetto negativo è che il codice dipenderà dalla libreria o dall'SDK, il che potrebbe portare alla mancanza di supporto, problemi di sicurezza o aggiornamenti significativi quando cambiano le librerie o gli SDK.

Data exposure. L'esposizione ai dati si verifica quando informazioni sensibili sono esposte al di fuori dellla tua app o anche all'interno della tua app. Per ridurre l'esposizione dei dati, è necessario utilizzare la crittografia per tutte le informazioni sensibili, indipendentemente dal fatto che siano inattive (memorizzate su disco) o in transito (ad esempio la trasmissione dalla tua app a un database).

Static code analyzers. Un analizzatore di codice statico è uno strumento per verificare la presenza di vari problemi nel codice, come le vulnerabilità. Si esegue un'analisi del codice statico prima di rilasciare l'applicazione.

Dynamic analysis (e.g., fuzzing). L'analisi dinamica del codice controlla il codice mentre viene eseguito. È possibile verificare la presenza di problemi comportamentali (come ciò che accade se semi-casuale le informazioni vengono passate all'app) e i problemi di prestazioni.

Stress testing. Dopo aver sviluppato il codice ma prima di implementarlo nella produzione, tu dovrebbe utilizzare prove di stress per garantire che il codice rimanga valido sotto carichi pesanti e con improvvisi aumenti nell'uso o nell'attività.

Sandboxing. Molti sviluppatori sono abituati a lavorare in ambienti DEV, QA e di produzione. I sandbox sono ambienti isolati di non produzione che vengono spesso utilizzati per eseguire isolati test, in particolare test che potrebbero avere un impatto o avere impatti sconosciuti. Una sandbox è utile perché non puoi influenzare nessun altro lavoro di sviluppo in corso o l'ambiente di produzione.

Model verifcation. Dopo aver sviluppato un'applicazione, è necessario utilizzare la verifica del modello per provare che l'app fa ciò che il modello dell'app afferma di poter fare. Ad esempio, se l'app automatizza la configurazione di un server Web, è necessario eseguire l'app per assicurarsi che configuri un server Web.
Come parte del ciclo di vita dello sviluppo del software, testate e convalidate il

codice. Questo ha un diretto impatto sulla qualità complessiva del codice. Conoscere le tecnologie di qualità del codice riportate di seguito.

Code quality and testing

Compiled vs. runtime code .Il codice compilato viene eseguito attraverso un compilatore per diventare codice nativo. Molte lingue sono linguaggi compilati, come C ++, C # e Go. Il codice compilato è in genere più veloce dell'interpretazione codice. Il codice di runtime è il codice che viene compilato in fase di runtime ("just in time").

Summarize cloud and virtualization concepts. Per l'esame, devi essere in grado di distinguere tra concetti e tecnologie chiave del cloud e componenti di virtualizzazione di base. In particolare, essere in grado di richiamare il tipo di distribuzione, hypervisor o posizione di una distribuzione in base a una serie di requisiti.
L'hypervisor è un server o un'appliance che esegue macchine virtuali (VM). L'hypervisor fornisce le basi hardware e software per la tua infrastruttura virtuale.
Le VM sono facili da implementare, soprattutto con l'automazione. La facilità di implementazione combinata con la velocità a volte può portare all'espansione delle macchine virtuali: hai più macchine virtuali di cui hai bisogno o addirittura ti rendi conto di averlo fatto e hai perso traccia di ciò che hai e di quali VM sono ancora richiesti o in uso.

Hypervisor VM sprawl avoidance

Type I. Un hypervisor di tipo I viene eseguito direttamente sull'hardware sottostante, fornendo accesso quasi diretto all'hardware delle macchine virtuali. È il tipo più performante e prevede la maggior scalabilità. VMware ESXi e Microsoft Hyper-V sono due dei leader in questo tipo di hypervisor.

Type II. n hypervisor di tipo II è una virtualizzazione basata su software che viene eseguita su un sistema operativo, come Windows o Linux. Non offre molte delle funzionalità avanzate di un hypervisor tipo I, non fornisce le stesse prestazioni e non si adatta. Tuttavia, è utile per scenari di sviluppo e test. Un hypervisor di tipo II è più adatto per l'uso individuale, come da sviluppatori o amministratori di sistema.

Application cells/containers. I contenitori sono un altro modo per virtualizzare l'applicazione. Invece di eseguire singole macchine virtuali, impacchetti app / codice e dipendenze in un unico contenitore. I contenitori sono portatili e condividono un sistema operativo di back-end.
Puoi eseguire più contenitori su un singolo server e non si conosceranno.

VM escape protection. Quando l'attaccante ottiene l'accesso a una macchina virtuale, è un grosso problema. Ma se l'attaccante può uscire dal VM e ottenere il controllo dell'hypervisor, questo è un affare molto più grande - ecco cos'è la fuga di VM. è difficile da fare, ma molti ci hanno provato. Non esiste un'unica configurazione o impostazione che impedisca Fuga dalla VM. Invece, devi fare affidamento sulla tua strategia di sicurezza a più livelli (difesa in profondità).

CON LA CRITTOGRAFIA CRIPTEOS 3001 IL PROBLEMA E? RISOLTO

Cloud storage L'archiviazione cloud è come l'archiviazione locale: un gruppo di unità disco o SSD, a volte connesse, che archiviano dati. Tuttavia, l'archiviazione cloud è nel cloud, non in locale e invece di distribuire e gestire l'archiviazione, è sufficiente consumarlo. Pensalo come un servizio di archiviazione. I vantaggi comprendono costi amministrativi ridotti e costi ridotti. I lati negativi stai perdendo il controllo dell'hardware e gran parte della configurazione; spesso non puoi scegliere come vengono archiviati i dati o come vengono crittografati. Rinunci al controllo.
Quando si distribuiscono carichi di lavoro sul cloud, è possibile scegliere tra diversi modelli. Per alcune soluzioni, sono possibili più modelli di distribuzione cloud e si sceglie in base su requisiti specifici. Altre volte, è possibile basare un solo modello di distribuzione cloud sui tuoi obiettivi. Molte organizzazioni, in particolare le grandi organizzazioni aziendali, ne usano alcune ogni modello di distribuzione. In altri casi, in particolare con le start-up, viene utilizzato solo SaaS.

Cloud deployment models
SaaS. Software-as-a-service (SaaS) è un modello di servizio cloud molto popolare. È stato da molto tempo, anche prima che le persone lo chiamassero SaaS e usassero il termine "the cloud."

PaaS. Platform-as-a-service (PaaS) è un ambiente completo per l'esecuzione delle tue app. Una tipica soluzione PaaS include server, archiviazione, reti e altre infrastrutture e software necessario per l'applicazione. Un esempio comune di PaaS sono le soluzioni di database come servizio, come il database SQL di Azure di Microsoft. Gestiscono l'infrastruttura; hai accesso a SQL.

IaaS. Infrastruttura come servizio (IaaS) fornisce i componenti sottostanti che è necessario eseguire il tuo data center nel cloud pubblico. IaaS offre altre funzionalità di virtualizzazione, reti virtuali, servizi di archiviazione e sicurezza. Se hai solo bisogno di eseguire VM nel cloud, allora hai solo bisogno di IaaS.

Private. Un cloud privato è uno che viene distribuito in locale e destinato solo alla tua organizzazione. Spesso imita un cloud pubblico con virtualizzazione e automazione

Public. Un cloud pubblico è uno che viene distribuito nell'ambiente di un provider ed è destinato essere un ambiente multi-cliente. Le risorse sono condivise tra i clienti, sebbene i clienti sono segmentati l'uno dall'altro. Virtualizzazione e automazione forniscono la chiave backend tecnologie di base in un cloud pubblico.

Hybrid. Un cloud ibrido combina uno o più cloud privati con uno o più pubblici nuvole. Ad esempio, un'organizzazione potrebbe avere il proprio cloud privato integrato nel proprio ambiente e utilizzare anche alcune macchine virtuali basate nel data center di un fornitore di servizi e SaaS soluzione nel cloud pubblico. In tali scenari, è comune utilizzare soluzioni che si integrano i clouds il più vicino possibile. Ad esempio, gli utenti potrebbero autenticarsi alle app allo stesso modo indipendentemente dal fatto che l'app sia nel cloud privato dell'azienda o nel cloud pubblico . Allo stesso modo, tutti i registri di controllo di tutte le origini potrebbero essere archiviati nella stessa posizione.

Community. Un cloud di comunità, un modello di implementazione cloud relativamente nuovo, è un cloud creato per una comunità specifica, come l'industria legale. L'ambiente è condiviso tra più clienti. Spesso, i cloud di comunità sono considerati una forma ibrida di cloud privati costruito e gestito specificatamente per un gruppo target.

On-premises vs hosted vs cloud. In locale si riferisce alla propria sala server, data center o ufficio. Ospitato si riferisce a data center di terze parti che forniscono spazio segmentato per le apparecchiature informatiche dei clienti; ad esempio, è possibile noleggiare un rack per ospitare i server. Un cloud è come un ambiente ospitato, ma invece di noleggiare un rack per mettere i tuoi server fisici, acquisti soluzioni virtualizzate, come un servizio di database o un ambiente IaaS.

VDI/VDE. L'infrastruttura desktop virtuale (VDI) si riferisce ai computer client virtualizzati su cui sono ospitati hypervisor e resi disponibili agli utenti finali. Con VDI hai una gestione centralizzata e può offrire agli utenti singole VM. L'ambiente desktop virtuale (VDE) si riferisce a un desktop virtualizzato eseguito localmente sul computer client. VDI è più scalabile e offre connettività remota alle macchine virtuali, mentre VDE è una soluzione localizzata, in genere per uno scopo molto specifico (come utilizzare come ambiente di sviluppo o test).

Broker. Un broker di sicurezza di accesso al cloud (CASB) è una soluzione di sicurezza che viene generalmente collocata tra il tuo ambiente locale e l'ambiente del tuo provider cloud. A CASB applica le politiche di sicurezza della tua organizzazione in tempo reale.
Molte organizzazioni implementano una strategia di sicurezza a più livelli per il loro

ambiente, implementando anti-malware, auditing, registrazione, monitoraggio, risposta agli incidenti di sicurezza e altri servizi. Richiede molto tempo, denaro e manodopera per distribuire e mantenere tutti questi servizi. La sicurezza come servizio tenta di affrontare la sfida di eseguire il poroprio ambiente sicurezza offrendo servizi di sicurezza su abbonamento. Un provider distribuisce, mantiene e monitora lo stack di sicurezza mentre il cliente consuma i dati e urgente comunicazioni dal fornitore.

CON LA SICUREZZA DI CRIPTEOS 3001 PUOI AVERE I VANTAGGI DEL CLOUD SENZA PROBLEMI, QUINDI, RISPETTO A TUTTE LE SOLUZIONI SOPRA DESCRITTE, PUOI SCEGLIERE IN BASE A CRITERI DI ECONOMIA E DI SALVATAGGIO DEI DATI SU PIU' DATABASE DI CLOUD SEPARATI, IN MODO CHE LA DISTRUZIONE FISICA DI UN DATABASE NON IMPLICHI LA PERDITA. CON L?ATTACCO ALLE TORRI GEMELLE DEL 2001, MOLTE AZIENDE CHE AVEVANO IL BACKUP DEI DATI NELL'ALTRA TORRE SONO FALLITE PERCHE', OLTRE CHE PERDERE TRAGICAMENTE I LAVORATORI AVEVANO PERSO TUTTO IL LORO KNOW.HOW.

Cloud access security

Explain how resiliency and automation. Quando si tratta di ridurre i rischi, ci sono due strategie chiave che è possibile utilizzare: resilienza e automazione. La resilienza implica la progettazione e la distribuzione di soluzioni senza un solo punto di errore (che si tratti di un server, un frewall o persino un centro dati). L'automazione è l'atto di automatizzare le attività che sarebbero normalmente eseguite da un amministratore o sviluppatore. L'automazione riduce notevolmente l'errore umano perché gli amministratori e gli sviluppatori non possono apportare manualmente modifiche alla configurazione.

Templates. Per automatizzare, è necessario utilizzare codice, script, applicazioni di terze parti o un mix di tutti e tre. Immagina che la tua organizzazione debba distribuire 25 server Web al mese per supportare la tua attività applicazione Web che utilizza un totale di 500 server Web. Senza un modello, potresti avere per configurare manualmente parti del server, ad esempio il servizio Web. Utilizzando un modello salva tempo e migliora la coerenza, il che spesso porta a una migliore sicurezza generale. Per esempio, se il server Web utilizza un file di configurazione per la configurazione, è possibile utilizzare un server Web modello di configurazione. Ogni volta che si distribuisce un nuovo server, si configura il servizio Web con il modello.
Master image. Un'immagine master è l'immagine di un sistema operativo che è stato configurato per soddisfare le tue politiche e standard dell'organizzazione. Ad

esempio, potresti avere un'immagine del server per il web server con gli ultimi aggiornamenti di sicurezza, la configurazione specifica richiesta e i prerequisiti installati. Un'immagine master accelera il tempo necessario per distribuire un nuovo server e migliora la coerenza.

Automation/scripting

Automated courses of action. Supponiamo di avere un server che gestisce un servizio web e i crash del servizio web; un amministratore viene informato dal sistema di monitoraggio e riavvia manualmente il servizio. Ora immaginate che lo scenario sia automatizzato. Avete un servizio si riavvia automaticamente se si ferma o si blocca, senza intervento umano. È possibile anche automatizzare una linea di azione basata su una serie graduale di compiti (come ad esempio lo spiegamento un nuovo server) o sulla base di eventi specifici che si verificano (come un crash di servizio).

Continuous monitoring. Il monitoraggio continuo è l'atto di monitorare l'ambiente 24/7/365. Mentre il monitoraggio da solo normalmente si riferisce a strumenti che ti aiutano a trovare se un server è inattivo o un'app non funziona correttamente, il monitoraggio continuo è focalizzato sulla garanzia che le tue configurazioni aderiscano alle tue linee di base o requisiti – automatizzati processi ripristinano le configurazioni se vengono rilevate errate configurazioni.

Confguration validation. La convalida della configurazione è un processo per cercare la configurazione deriva: quando un server, un servizio o un'app non corrispondono più alla configurazione iniziale o desiderata.

Templates. Immaginate che la vostra organizzazione deve distribuire 25 server web al mese per supportare un'applicazione web che utilizza un totale di 500 server web. senza un modello, potrebbe essere necessario configurare manualmente parti dei server, come il servizio web. L'utilizzo di un modello consente di risparmiare tempo e migliora la coerenza, il che spesso porta a una maggiore sicurezza generale. Ad esempio, se il server web utilizza un file di configurazione per la configurazione, è possibile utilizzare un modello di configurazione web sever. Ogni volta che si distribuisce un nuovo server, si configura il servizio web con il modello.

Master image. Un'immagine master è un'immagine di un sistema operativo che è stato configurato per soddisfare le politiche e gli standard della vostra organizzazione. Ad esempio, si potrebbe avere un'immagine del server per i server web che ha gli ultimi aggiornamenti di sicurezza, la configurazione specifica necessaria e i prerequisiti installati. Un master image velocizza il tempo per distribuire un nuovo server e migliora la coerenza.

Non-persistence. Se quando si spegne il computer, tutti i dati rimangono come sul disco rigido per avere persistenza. Se quando si spegne il computer, tutto il contenuto della memoria del computer viene cancellato, si tratta di una non persistenza. Con la crescita dell'automazione e del cloud pubblico, la non persistenza è diventata più importante. Con la non persistenza, puoi fare di più automatizza facilmente.

Elasticity.L'elasticità è il processo di approvvigionamento di nuove risorse per soddisfare la domanda aggiuntiva, ad esempio aggiunta di server Web per fornire risorse aggiuntive durante le vacanze. L'elasticità comporta anche il deprovisioning delle risorse in quanto non necessarie, ad esempio la rimozione dell'ulteriore server dopo le vacanze quando la domanda è ridotta.

Scalability La scalabilità è come l'elasticità ma si occupa solo di aumentare le risorse, non di ridurle.
Distributive allocation . Nel tuo ambiente, distribuisci risorse. Spesso questo si basa sul fornitore standard (è possibile acquistare server da un singolo fornitore e utilizzare un tipo di sistema operativo, ad esempio). Con l'allocazione distributiva, distribuisci le risorse in un modo vario al fine di ridurre la dipendenza da un singolo fornitore, un singolo sito o un solo tipo di tecnologia. L'obiettivo con l'allocazione distribuita è ridurre il rischio, ad esempio il rischio associato alla presenza di un singolo provider cloud la cui rete subisce un attacco DDoS.

Snapshots. Una snapshots è un backup temporizzato. È possibile eseguire una snapshots di un disco. È possibile creare snapshots di una macchina virtuale. Con molte piattaforme di rete dell'area di archiviazione, è anche possibile creare una snapshots di un volume. Come i backup, le snapshots possono contenere informazioni riservate. Crittografa le tue snapshots per migliorare la sicurezza.

Revert to known state. Quando si torna a uno stato noto con un computer, si reimposta la configurazione del computer a una data e ora specifiche, come la data e l'ora della snapshots o backup.

Rollback to known confguration. Quando si esegue il rollback a una configurazione nota, si esegue il rollback eseguire il backup di un'applicazione su una versione che è stata documentata per avere un set specifico di funzionalità o una configurazione.

Live boot media. Immagina di prendere un DVD e inserirlo in un computer. Si avvia fino a un sistema operativo non persistente. Svolgi compiti. Quindi, si rimuove il DVD e riavvia il computer. Questo descrive l'uso del supporto live boot media. Fornisce supporto di live boot media in un ambiente operativo temporaneo (di solito temporaneo) non persistente.

Redundancy. Redundancy prevede più componenti per ridurre l'impatto di un errore del sistema. Per garantire la Redundancy in un server, avremmo 2 processori, più memory stick, più dischi rigidi che lavorano insieme, almeno due alimentatori e almeno due schede NIC. Per ridondanza per essere più efficace, deve estendersi a tutti i componenti e sistemi dipendenti. Ad esempio, immagina che il tuo server abbia due alimentatori ma collega i cavi di alimentazione nella stessa presa multipla. La tua Redundancy di potenza ha sofferto, anche se ancora Redundancy in caso di guasto di uno degli alimentatori. Nota che puoi avere Redundancy nei tuoi componenti, ma ciò non significa che tu abbia un'alta disponibilità (che è descritto sotto). Ad esempio, potresti avere 2 alimentatori ma solo 1 è collegato.

Fault tolerance. La fault tolerance agli errori consente a un sistema di continuare a funzionare anche se si verifica un errore in un componente. Ad esempio, immagina di avere 3 dischi rigidi in un RAID 5. Un disco rigido si guasta, ma i dati continuano ad essere accessibili. Il RAID è in uno stato degradato ma funziona. Questa è la tolleranza agli errori. La tolleranza ai guasti si concentra in genere sull'hardware, non sul software.
High availability. High avalability descrive un ambiente in cui i sistemi continuano a essere disponibili indipendentemente da ciò che non funziona o da come fallisce. L'alta disponibilità è come la tolleranza agli errori ma si concentra su entrambi hardware e software. La disponibilità elevata non è sempre disponibilità istantanea ma in genere si sforza di essere il più vicino possibile.

RAID .RAID è il processo di acquisizione di più dischi rigidi e la loro combinazione fisica o virtuale insieme per migliorare le prestazioni o la disponibilità. RAID è classificato per tipi. Per esempio, RAID 1 è un mirror in cui almeno 2 dischi rigidi hanno dati identici, mentre RAID 5 è un set di strisce con un minimo di 3 dischi rigidi, con 1 disco rigido utilizzato per parità.

Fault tolerance
High availability

Explain the importance of physical security
control . Oltre all'importanza dell'hardware, del software e della sicurezza della configurazione, è necessario conoscere anche i controlli di sicurezza fisica. I controlli di sicurezza fisica riguardano la sicurezza delle tue forze, i data center, i dipendenti e le risorse fisiche.

Lighting. Immagina un ufficio building di notte. È scuro. I dipendenti sono tornati a casa. Senza un'illuminazione adeguata, un ladro potrebbe intrufolarsi nella struttura e

forse anche irrompere senza che nessuno (persone che guidano, telecamere di sicurezza o persino guardie di sicurezza) siano in grado di vedere nulla. L'illuminazione è un importante deterrente per la sicurezza: in genere i ladri non amano essere visti e l'illuminazione è il loro nemico. Come minimo, dovresti usare l'illuminazione per illuminare gli ingressi, uscite e percorsi pedonali. Per ulteriore sicurezza, prendi in considerazione l'utilizzo dell'illuminazione a movimento, che si illumina intensamente quando viene rilevato un movimento nelle vicinanze.

Signs. I segni sono utili per proteggere le tue strutture. Ad esempio, pubblicando i segni "Non violare" il perimetro della tua struttura dice alle persone che la tua struttura non è un luogo autorizzato ai visitatori. La pubblicazione dei cartelli "Le strutture sono monitorate da telecamere di sicurezza" è efficace perché avverte le persone che potrebbero essere sorvegliate e quindi più suscettibili all'arresto e alla condanna se commettono un crimine.

Fencing/gate/cage. Mentre puoi camminare per molti di questi edifici, la difesa è importante per le strutture riservate come un data center. All'interno di aree riservate come un data center o una sala server, è a buona pratica per utilizzare un'ulteriore sicurezza fisica come cancelli (per eseguire un controllo di identità prima dell'entrata di nebbia) e delle gabbie (per segmentare i sistemi IT). In un ambiente condiviso tra i clienti, le gabbie sono spesso utilizzate per segmentare le attrezzature dei clienti.

Security guards. Le guardie di sicurezza sono efficaci nel proteggere la vostra struttura. Possono vedere e sentire cose che le telecamere di sicurezza non possono sempre vedere o ascoltare (al di fuori della vista della telecamera, ad esempio). Essi possono valutare una situazione in base alla propria esperienza e agire rapidamente (ad esempio, vedi una persona in una maschera da sci e chiamare la polizia). Possono anche servire da deterrente. Se il tuo edificio ha una guardia di sicurezza ma l'edificio in fondo alla strada no, un ladro potrebbe scegliere quest'ultimo edificio.

Alarms. All'ingresso non autorizzato, un allarme può contattare automaticamente la polizia, attivare una sirena rumorosa o entrambi. Un allarme è un efficace controllo di sicurezza fisica perché vederlo spesso spaventa i ladri dal tentare persino di entrare nella tua struttura. Se decidono di intervenire, la sirena d'allarme probabilmente li spaventerebbe e potrebbe persino allertare la polizia, che può catturare il ladro.

Safe .Una cassaforte è una camera blindata chiusa e blindata, in genere abbastanza piccola da trasportare ma a volte grande abbastanza per entrare. Le cassette di sicurezza vengono utilizzate per conservare gli oggetti più preziosi o insostituibili. Per esempio, è possibile archiviare denaro o una chiave principale in una cassaforte. Le casseforti sono spesso efficaci contro incendi, inondazioni e ladri.

Protected cabling
enclosures. A volte, è necessario proteggere leggermente gli oggetti. Ad esempio, potresti voler bloccare alcuni documenti di progetto di notte. Armadi o contenitori sicuri sono utili per un fissaggio sicuro elementi. Generalmente tengono fuori osservatori casuali o vicini curiosi. Tuttavia, lo sono non molto sicuri perché possono essere aperti con strumenti comuni. Pertanto, dovrebbero essere utilizzati solo con oggetti non di importanza critica o sensibili.

Airgap. Un gap aereo è una segmentazione fisica di un computer o di una rete da Internet o da un'altra rete insicura. Ad esempio, potresti avere un server sensibile collegato a una LAN e la LAN non è connessa a nessun dispositivo o rete che abbia accesso a Internet. Quindi, il computer non può essere collegato da Internet. Un gap d'aria aumenta notevolmente la sicurezza di un computer o di una rete. Tuttavia, come visto nelle notizie di recente, i compromessi sono ancora possibili utilizzando chiavette USB o altri metodi offline.

Mantrap . I mantraps sono aggeggi fisici che minimizzano o impediscono il tailgating. Ad esempio, potresti vedere un tornello sicuro in uno stadio o altro evento; consente a una sola persona di entrare alla volta.

Faraday cage , Una gabbia di Faraday è un recinto che blocca i campi elettromagnetici. Ad esempio, lo smartphone non può essere contattato quando è archiviato in una gabbia di Faraday. Le gabbie di Faraday sono spesso utilizzate per proteggere le delicate apparecchiature elettroniche, come quelle sequestrate come prove in un caso criminale.

LOCK TYPES. Ci sono molti tipi di serrature, ognuna con punti di forza e di debolezza. Ad esempio, la maggior partepersone hanno familiarità con serrature o manopola serrature, che sono entrambi nella maggior parte delle case, spesso sula porta d'ingresso. Altri tipi di serrature sono serrature a incastro, spesso si trovano in edifici commerciali e serrature a camme, spesso trovate negli armadietti. Alcune organizzazioni scelgono di usare i cavi per bloccare fisicamente i computer alle scrivanie, il che li rende più difficili da rubare.

Biometrics. La biometria è un tipo di sistema di identificazione che si basa sulla misurazione delle caratteristiche di una persona, come retina, viso e voce. La biometria viene talvolta utilizzata per l'autenticazione primaria, come lo sblocco del computer o dello smartphone. Altre volte, la biometria viene utilizzata per un secondo fattore di autenticazione, ad esempio quando si va in una struttura riservata, potrebbe essere necessario scorrere un badge per accedere alla proprietà e quindi

utilizzare una scansione manuale per accedere ad altre aree della struttura. La biometria migliora la sicurezza, soprattutto rispetto alle password.

Secure cabinets/ Protected distribution/ Lock types

Barricades/bollards. Le barricate sono muri usati per bloccare l'accesso. A volte sono brevi, ad esempio per bloccare l'accesso alle auto. Altre volte sono alti, in modo da bloccare l'accesso alle persone. Le barricate vengono spesso utilizzate temporaneamente, ad esempio durante un disastro ambientale o una rivolta. Le bitte sono pali che sono installati nel terreno e sporgono dal terreno abbastanza da fornire una barricata. Spesso vengono installati per circondare importanti infrastrutture, come un generatore di backup. Altre volte vengono utilizzati per la sicurezza, ad esempio per tenere le auto lontane dai pedoni passerelle.

I Barricades/bollards sono lucchetti usati per proteggere singoli beni, come computer, biciclette, macchine fotografiche o altre piccole attrezzature. Queste serrature spesso impediscono i ladri casuali ma di solito non sono sicure abbastanza da scoraggiare i ladri professionisti.

Tokens/cards .I token e le carte sono spesso carte piccole (dimensioni di portafoglio o più piccole) che i dipendenti usano per guadagnare accesso a edifici, parcheggi e altre strutture. I lettori di token e di carte lo sono spesso posto in punti di ingresso (come le porte) per leggere elettronicamente le carte, convalidare le carte con a computer back-end e sbloccare le porte quando viene presentata una carta valida.
I controlli ambientali forniscono il controllo della temperatura e la protezione ambientale per le tue strutture.

Environmental controls

HVAC. Riscaldamento, ventilazione e aria condizionata (HVAC) controllano la temperatura delle tue strutture. Mentre mantenere le persone a proprio agio in un momento è importante, HVAC è fondamentale per operazioni del data center perché le apparecchiature informatiche spesso diventano instabili o impossibili per funzionare quando le temperature diventano troppo calde.

Hot and cold aisles. In un data center, è fondamentale mantenere la temperatura adeguata e assicurarsi che l'attrezzatura continui a funzionare. Una tecnica comune è quella di designare filari caldo e freddo. In tale scenario, i server e le apparecchiature devono affrontare ciascuno (ad esempio, i server in fila 1 server di fronte nella fila dritto). L'aria calda esce dal retro di ogni fila ma non entra nell'assunzione di altre apparecchiature. Sulla base di questa configurazione, ogni altra riga è a fila fredda (di aspirazione) e ogni altra fila è una fila calda (di scarico).

Fire suppression. La soppressione del fuoco si riferisce a tecnologie che riducono la diffusione di fire (come porte fire) o aiutare a mettere fuori un fire (come estintori fire). Ci sono molti tipi di soppressione dei fire, come i sistemi di irrigazione (spesso usati in ambienti spesso ma non ideale per i data center) e la soppressione libera di anidride carbonica (o altri agenti puliti soppressione fire, ideale per i data center).

Screen flters.Un filtro schermo è un monitor / schermo sovrapposto che riduce drasticamente il campo visivo del monitor o schermo. Quando metti uno schermo sul monitor di un computer, diventa difficile per le persone che camminano o guardano casualmente alle tue spalle vedere lo schermo. Una persona deve stare direttamente dietro di te nell'angolo giusto per vedere lo schermo, e questo rende difficile che qualcuno lo faccia senza preavviso. I filtri dello schermo sono spesso utilizzati dai dirigenti o altre persone che lavorano abitualmente con dati sensibili, come fogli di calcolo salariali o rapporti sul rendimento dei dipendenti.

Cameras. Quando si utilizzano le telecamere per acquisire attività nella propria struttura, si ottiene il vantaggio di essere in grado di riprodurre le attività in un secondo momento, contribuendo potenzialmente a rintracciare le persone responsabili in un incidente. Inoltre, fai attenzione a potenziali intrusi: la vista delle telecamere è spesso abbastanza dissuasiva per convincere i cattivi a trasferirsi in una struttura meno sicura. Le telecamere sono una parte importante della tua strategia di sicurezza fisica a più livelli.

Motion detection. La rilevazione del movimento è stata storicamente legata a sistemi di allarme come gli allarmi antifurto. Voi impostare l'allarme quando si lascia la struttura e viene considerato qualsiasi movimento rilevato in seguito malevolo e si attiva un allarme. Il rilevamento del movimento si è esteso anche ad altri usi, incluso l'uso in telecamere di sicurezza che iniziano a registrare quando viene rilevato un movimento, le luci che girano accese quando viene rilevato un movimento e automazione che chiude una porta o un cancello dopo 5 secondi viene rilevato l'ultimo movimento.

Logs. Con la sicurezza fisica, i registri sono collegati a tutte le soluzioni di sicurezza fisica, come il lettori badge, lettori di biometria e registri dei visitatori utilizzati per accedere manualmente a una struttura. I registri sono importanti perché possono aiutarti a indagare su un incidente. Ad esempio, puoi scoprire quale garage un impiegato ha usato, da quale porta sono entrati, il momento in cui sono entrati e tutte le porte aperte da allora in poi. È possibile correlare tali informazioni dalle informazioni dalle telecamere per formare un'immagine completa.

Infrared detection. Le telecamere del modello tardivo possono registrare nell'oscurità quasi completa utilizzando la tecnologia di rilevamento a infrarossi. Utilizzando la radiazione infrarossa, il rilevamento è possibile attraverso le firme di calore. In condizioni di scarsa illuminazione, le telecamere a infrarossi sono importanti. Altrimenti, puoi investire in un'illuminazione adeguata per ridurre al minimo la necessità di rilevamento a infrarossi.

Key management.Con la sicurezza fisica, la gestione delle chiavi è il processo di gestione delle chiavi. Spesso parliamo di chiavi fisiche, come la costruzione di chiavi o chiavi master. Ma la gestione delle chiavi si estende anche alle chiavi digitali. Per massimizzare la sicurezza, è necessario disporre di un processo formale per la gestione chiavi, in particolare chiavi sensibili come una chiave master che può aprire tutte le porte della struttura.

Come la sicurezza digitale, dovresti aderire al principio del privilegio minimo con le chiavi. Il riparatore dell'aria condizionata assegnato per riparare il sistema HVAC nell'Edificio 2 dovrebbe ottenere solo una chiave per l'Edificio 2. Le chiavi master devono essere conservate in un luogo sicuro, come una cassetta di sicurezza o una cassetta di sicurezza.

4. Identity and Access Management

4.1 Compare and contrast identity and access management concepts

Il controllo dell'accesso alle risorse è uno dei temi fondamentali della sicurezza. Scoprirai una varietà di diversi controlli di sicurezza che lavorano insieme per fornire il controllo degli accessi. Una risorsa può essere informazioni, sistemi, dispositivi, strutture o personale. Questa sezione è focalizzata sui concetti relativi alla concessione e alla revoca dei privilegi per lo scopo dell'accesso ai dati o eseguire azioni sui sistemi. Ci sono 4 sezioni in Identità e gestione degli accessi.

Identifcation, authentication, authorization and accounting (AAA)

Identifcation. L'identificazione è il processo di qualcuno che afferma di essere un'identità particolare. Il soggetto deve fornire un'identità a un sistema per iniziare i processi di autenticazione, autorizzazione e contabilità. Ad esempio, l'oggetto potrebbe digitare un nome utente, scorrere una smart card o fornire un token dispositivo. Un principio fondamentale è che tutti i soggetti devono hanno identità univoche.

Authentication. L'autenticazione verifica l'identità del soggetto confrontando uno o più fattori rispetto a un database di identità valide (ad es. account utente). Un altro nucleo il principio è che le informazioni utilizzate per verificare l'identità sono

informazioni private e dovrebbe essere protetto. Ad esempio, invece di archiviare le password in chiaro, i sistemi di autenticazione memorizzano gli hash delle password nel database di autenticazione.
L'identificazione e l'autenticazione avvengono sempre insieme come un unico processo in due passaggi: fornire un'identità è il primo passo e verificare l'identità (autenticazione) è il secondo passo.

Senza completare entrambi i passaggi, un soggetto non può accedere a una risorsa.

Authorization. L'autorizzazione indica chi si fida di eseguire operazioni specifiche - i soggetti hanno accesso agli oggetti in base a identità comprovate. Ad esempio, gli amministratori concedono a un utente l'accesso ai file in base alla comprovata identità dell'utente. Se l'azione è consentita, il soggetto è autorizzato; se non è consentito, il soggetto non è autorizzato. L'identificazione e l'autenticazione sono aspetti "tutto o niente" della gestione degli accessi;
le credenziali di un utente dimostrano un'identità rivendicata o non lo fanno. Al contrario, l'autorizzazione include una vasta gamma di varianti. Ad esempio, un utente potrebbe essere in grado di leggere un file ma non eliminare il file, oppure un utente potrebbe essere in grado di creare un nuovo documento ma non alterarne altri documenti degli utenti.

Accounting. La contabilità comprende auditing, registrazione e monitoraggio, che forniscono responsabilità assicurando che i soggetti possano essere ritenuti responsabili delle loro azioni. Ad esempio, quando il controllo è abilitato, può registrare quando un soggetto legge, modifica o elimina un file.
Mentre la contabilità si basa sull'identificazione e sull'autenticazione efficaci, non richiede effetiva autorizzazione. In altre parole, una volta identificati e autenticati i soggetti, i meccanismi contabili possono tracciare la loro attività anche quando provano ad accedere alle risorse per cui non sono autorizzati.

Multifactor authentication

Something you are. Ciò include una caratteristica fisica di un individuo con diverso tipi di biometria. Gli esempi includono impronte digitali, stampe vocali, motivi a retina, motivi a iride, forme del viso, topologia del palmo e geometria della mano.

Something you have. Ciò include i dispositivi fisici che un utente possiede. Esempi include una smart card, un token hardware, una memory card o un'unità USB.

Something you know. Potrebbe essere una password, un numero di identificazione personale (PIN) o passphrase, ad esempio.

Somewhere you are. Ciò include la posizione di una persona in base a un computer specifico, una posizione geografica (basata su un indirizzo IP) o un numero di telefono (basato sull'ID chiamante).

Something you do. Ciò include una caratteristica attuabile di un individuo. Esempi sono dinamiche di firma e battitura.
I metodi di base dell'autenticazione sono anche fattori. L'autenticazione a più fattori include due o più dei seguenti fattori:

Federation .Una federazione è composta da reti distinte di diverse organizzazioni. In una federazione, l'intenzione è che queste organizzazioni condividano risorse e / o dati mentre continuano a utilizzarli le loro credenziali esistenti. Ad esempio, immagina che Company1 voglia collaborare da vicino Azienda2 condividendo le informazioni del calendario. Azienda1 può federare con Azienda2. Utenti in Azienda1 è possibile visualizzare le informazioni del calendario degli utenti in Azienda2 utilizzando le proprie credenziali di Azienda1. Gli utenti in Azienda2 possono visualizzare le informazioni del calendario in Azienda1 usando il loro Credenziali dell'azienda2. Le federazioni facilitano la condivisione e la connessione delle organizzazioni ai servizi cloud pubblici.

Single sign-on. Single Sign-On (SSO) utilizza identità federate per offrire un'esperienza più fluida per utenti quando accedono alle risorse. Tuttavia, anziché un attributo utente, il provider ospitato corrisponderebbe all'ID di accesso interno dell'utente con un'identità federata. Ad esempio, supponiamo che i dipendenti accedono all'interno dell'organizzazione utilizzando il proprio ID di accesso aziendale. Quando un utente accede ai servizi online, il sistema di gestione delle identità federate utilizza il proprio ID di accesso per recuperare l'identità federata corrispondente.

Transitive trust. La fiducia transitiva è il concetto che se A si fida di B e B si fida di C, allora A eredita la fiducia di C.
La fiducia transitiva è una grave preoccupazione per la sicurezza perché potrebbe consentire di aggirare le restrizioni o le limitazioni tra A e C, in particolare se A e C si fidano entrambe B. Un esempio di questo sarebbe quando un utente (A) richiede dati da B e poi B richiede i dati da C, i dati che gli utenti ricevono sono essenzialmente da C - uno sfruttamento transitorio della fiducia.

4.2 Given a scenario, install and confgure identity and access services

In questa sezione, ti verrà data l'opportunità di scegliere un'identità e un accesso appropriati servizio e come dovrebbe essere configurato sulla base di un elenco di requisiti .

LDAP . In questa sezione, ti verrà data la possibilità di scegliere Molte organizzazioni utilizzano una directory centralizzata memorizzata in un database che memorizza informazioni sugli utenti e altri oggetti ed è generalmente utilizzato come sistema di controllo degli accessi. Un esempio di questo si basa sul protocollo LDAP (Lightweight Directory Access Protocol). Ad esempio, Microsoft Active Directory Dominio Services (AD DS) è basato su LDAP.
La directory LDAP è simile a una rubrica telefonica per servizi e risorse di rete. Gli utenti, i client e i processi possono cercare nel servizio di directory per trovare il sistema o la risorsa desiderati. Utenti deve autenticarsi al servizio di directory prima di eseguire query e attività di ricerca.

Kerberos. Kerberos utilizza un sistema di ticket per l'autenticazione. Offre una soluzione Single Sign-On per gli utenti e fornisce protezione per le credenziali di accesso. Kerberos offre riservatezza e integrità per il traffico di autenticazione che utilizza la sicurezza end-to-end e aiuta a proteggere dalle intercettazioni e ripetere gli attacchi. La versione attuale, Kerberos 5, si basa sulla crittografia a chiave simmetrica (anche nota come crittografia a chiave segreta) utilizzando lo standard AES (Advanced Encryption Standard) simmetrico protocollo di crittografia.
ANCHE QUI RICORDO CHE LO STANDARD AES E' MOLTO DEBOLE RISPETTO ALL?ALGORITMO DI ROBIONICA CRIPTEOS 3001
un'identità e un accesso appropriato servizio e come dovrebbe essere configurato sulla base di un elenco di requisiti.

TACACS+. Il sistema di controllo accessi (TACACS) del Terminal Access Controller è stato introdotto in alternativa a RADIUS (descritto di seguito). TACACS Plus (TACACS +) è stato successivamente creato come open, protocollo documentato pubblicamente. TACACS + offre numerosi miglioramenti rispetto a RADIUS di separare l'autenticazione, l'autorizzazione e la contabilità in processi separati. Inoltre, TACACS + crittografa tutte le informazioni di autenticazione, non solo la password come RADIUS lo fa.
Questo è uno dei protocolli di autenticazione utilizzati sui collegamenti PPP (Point-to-Point Protocol).

CHAP. Challenge Handshake Authentication Protocol (CHAP) crittografa i nomi utente e le password ed esegue l'autenticazione utilizzando un dialogo sfida-risposta che non può essere riprodotto.
CHAP inoltre riautentica periodicamente il sistema remoto in un determinato momento sessione di comunicazione per verificare un'identità persistente del client remoto. Questa attività è trasparente per l'utente.
Questo è un altro protocollo di autenticazione standardizzato per PPP. Autenticazione

password Il protocollo (PAP) trasmette nomi utente e password in chiaro. Non offre alcuna forma di crittografia, ma fornisce semplicemente un metodo per trasportare le credenziali di accesso dal client al server di autenticazione.

MS-CHAP. MS-CHAP è la versione Microsoft del protocollo CHAP ed esiste in due versioni, MSCHAPv1 e MS-CHAPv2. Alcune delle differenze tra CHAP e MS-CHAP sono queste MS-CHAP fornisce un meccanismo di modifica della password controllato dall'autenticatore e un meccanismo di tentativo di autenticazione controllato dall'autenticatore. Inoltre, MS-CHAPv2 fornisce reciproca autenticazione tra pari mediante la creazione di una sfida tra pari sulla risposta pacchetto e una risposta dell'autenticatore sul pacchetto Success. Ci sono punti deboli noti con MS-CHAP, incluso l'uso di DES per crittografare l'hash della password NTLM, che si apre la porta per attacchi hardware personalizzati che utilizzano attacchi a forza bruta.
RADIUS . Il servizio utente dial-in di autenticazione remota (RADIUS) centralizza l'autenticazione per il telecomando connessioni. In genere viene utilizzato quando un'organizzazione ha più di un server di accesso remoto. Un utente può connettersi a qualsiasi server di accesso alla rete, che quindi passa le credenziali dell'utente al server RADIUS per autenticazione, autorizzazione e contabilità. Mentre RADIUS crittografa lo scambio della password, non crittografa l'intera sessione. È possibile utilizzare protocolli aggiuntivi per crittografare la sessione di dati.
Security Assertion Markup Language (SAML) è un linguaggio basato su XML che è comunemente utilizzato per scambiare informazioni di autenticazione e autorizzazione tra organizzazioni federate. Viene comunemente utilizzato per fornire SSO agli utenti che accedono a risorse Internet.

OpenID Connect. OpenID Connect è un livello di autenticazione che utilizza il framework OAuth 2.0. Fornisce autenticazione decentralizzata, che consente agli utenti di accedere a più siti Web non correlati con un set di credenziali gestito da un servizio di terze parti, denominato OpenID fornitore.

OAuth. OAuth (che implica un'autenticazione aperta) è uno standard aperto utilizzato per la delega dell'accesso. L'ultima versione di questo framework è OAuth 2.0; è supportato da molti servizi online fornitori.

Shibboleth. Shibboleth è un pacchetto software standard gratuito e aperto utilizzato per SSO e federazione tra e all'interno delle organizzazioni. Il software è di proprietà e gestito dal consorzio internazionale Shibboleth.

Secure token.Un token di sicurezza è un dispositivo fisico utilizzato per l'autenticazione, in aggiunta o in luogo di una password. Esempi di token sicuro

includono una keycard wireless o un dispositivo USB.
Alcuni token memorizzano chiavi crittografiche (come una firma digitale), dati biometrici (come dettagli di fingerprint) o password.

NTLM.NT LAN Manager (NTLM) è una suite di protocolli di sicurezza Microsoft che fornisce agli utenti autenticazione, integrità e riservatezza. La suite di protocolli NTLM è implementata in un Security Support Provider, che combina il protocollo di autenticazione LAN Manager, protocolli di sessione NTLMv1, NTLMv2 e NTLM2 in un unico pacchetto.

4.3 Given a scenario, implement identity and access management controls

Dopo l'autenticazione, il passaggio successivo è l'autorizzazione. Il metodo per autorizzare gli utenti ad accedere le risorse dipendono dal metodo di controllo dell'accesso.

Access control models. I modelli di controllo dell'accesso definiscono il modo in cui gli utenti ottengono l'accesso alle risorse. Esistono diversi modelli, ognuno con i propri metodi di accesso. Ecco l'accesso cinque più popolare modelli di controllo:

MAC. Il modello Mandatory Access Control (MAC) utilizza etichette applicate a entrambi utenti e oggetti. Ad esempio, un utente che ha l'etichetta "top secret" può essere concesso l'accesso a un documento che ha l'etichetta "top secret". In questo esempio, il soggetto e il l'oggetto ha etichette corrispondenti.

DAC. Il modello Discretionary Access Control (DAC) utilizza un elenco di controllo di accesso (ACL) cheviene applicato agli oggetti. L'ACL definisce il proprietario dell'oggetto e il proprietario può concedere o negare l'accesso a qualsiasi altro utente. Il New Technology File System (NTFS), utilizzato sui sistemi operativi Microsoft Windows, utilizza il modello DAC.

ABAC. Il modello ABAC (Attribute Based Access Control) utilizza regole che possono includere più attributi su utenti e oggetti. Ciò consente al modello di essere flessibile, come si applica le regole per tutti gli utenti e gli oggetti allo stesso modo. Le regole all'interno di una politica possono usare un linguaggio semplice dichiarazioni come "Consentire ai lavoratori del negozio di accedere alla WAN utilizzando un dispositivo mobile aziendale".

Role-based access control. Il modello di controllo di accesso basato sui ruoli (RBAC) utilizza ruoli o gruppi, che sono generalmente identificati dalle funzioni di lavoro. Invece di assegnare autorizzazioni direttamente agli utenti, gli account utente

vengono inseriti in ruoli e gli amministratori assegnano i privilegi i ruoli. Se un account utente ha un ruolo, l'utente ha tutti i privilegi assegnati a quel ruolo.

Rule-based access control. Il modello di controllo di accesso basato su regole applica regole globali che si applicano a tutte le materie. Ad esempio, un firewall utilizza regole che consentono o bloccano il traffico a tutti gli utenti. Le regole all'interno del modello di controllo di accesso basato su regole sono talvolta riferite a come restrizioni o filtri.

Proximity cards. Le carte di prossimità sono indossate o detenute da un portatore autorizzato. Quando essi passare un lettore di prossimità, il lettore è in grado di determinare chi è il portatore e se hanno accesso autorizzato.

Physical access control. I controlli fisici sono considerati qualcosa che hai; sono la prima linea di difesa quando forniscono adeguata sicurezza.

Smart cards. Le smart card sono identificativi, badge o tessere di sicurezza delle dimensioni di una carta di credito con un striscia magnetica incorporata, codice a barre o chip per circuito integrato. Contengono informazioni sul portatore autorizzato che può essere utilizzato per l'identificazione e / o l'autenticazione
scopi. Alcune smart card possono persino elaborare informazioni o archiviare quantità ragionevoli di dati in un chip di memoria.

Fingerprint scanner. Le impronte digitali sono i motivi visibili sulle dita e sui pollici delle persone. Sono unici per un individuo e sono stati usati per decenni in campo fisico sicurezza per l'identificazione. Gli scanner di impronte digitali sono ora comunemente utilizzati su computer portatili e unità flash USB per l'identificazione e l'autenticazione.

Retinal scanner. Gli scanner retinici si concentrano sul modello dei vasi sanguigni sul retro l'occhio della gente. Sono la forma più accurata di autenticazione biometrica e possono differenziarsi tra gemelli identici. Gli scanner retinici in genere richiedono che gli utenti siano vicini quanto tre pollici dallo scanner.

Iris scanner. Gli scanner dell'iride si concentrano sull'area colorata intorno alla pupilla e sono i secondi forma più accurata di autenticazione biometrica. Come la retina, l'iride rimane relativamente invariato per tutta la vita di una persona. Le scansioni dell'iride sono considerate più accettabili dagli utenti generici rispetto alle scansioni della retina in genere perché le scansioni possono verificarsi da più lontano - da 20 a 40 piedi (da 6 a 12 metri)

Voice recognition. Questo tipo di autenticazione biometrica si basa sulle caratteristiche di a voce parlante della persona, nota come un'impronta vocale. L'utente parla una frase specifica, che viene registrato dal sistema di autenticazione. Per autenticarsi, ripetono la stessa frase, che viene confrontato con la registrazione originale. Talvolta viene utilizzato il riconoscimento del pattern vocale come meccanismo di autenticazione aggiuntivo, ma raramente viene utilizzato da solo.

Facial recognition. Gli scanner per il riconoscimento facciale utilizzano i motivi geometrici delle persone volti per il rilevamento e il riconoscimento. Ad esempio, potrebbe essere utilizzato il sistema di autenticazione una o più foto di te combinate con il tuo nome. Anche le scansioni del viso sono abituate identificare e autenticare le persone prima che possano accedere ad spazi sicuri, ad esempio come caveau sicuro.

Biometric factors .Un'altra tecnica di autenticazione e identificazione comune è l'uso della biometria, quali sono i metodi per qualcosa che sei fattore di autenticazione.

False acceptance rate. Una falsa accettazione si verifica quando viene autenticato un utente non valido; è anche noto come falso autenticazione positiva. Ad esempio, il sistema di autenticazione si autentica correttamente un intruso che utilizza un account non valido o un'impronta digitale non registrata. Il rapporto tra falso positivi per autenticazioni valide è il tasso di falsa accettazione (FAR).

False rejection rate . Un falso rifiuto si verifica quando un utente valido non è autenticato. Ad esempio, un sistema di autenticazione potrebbe rifiutare erroneamente l'impronta digitale di un utente valido con un'impronta digitale registrata. Questa è talvolta definita un'autenticazione falsa negativa. Il rapporto tra falsi rifiuti per autenticazioni valide è il tasso di rifiuto falso (FRR).

Certifcate-based authentication

Crossover error rate. È possibile utilizzare il tasso di errore crossover (CER), noto anche come tasso di errore uguale (ERR), per confrontare la qualità generale dei dispositivi biometrici. Il punto in cui le percentuali di FRR e FAR sono uguali è il CER e il CER sono usati come valore di valutazione standard per confrontare l'accuratezza del diverso dispositivi biometrici. I dispositivi con CER più bassi sono più precisi dei dispositivi con CER più alti.

Tokens . Un token è un dispositivo che genera password che visualizza un numero per l'autenticazione. A qualsiasi punto nel tempo, il server di autenticazione e il token avranno lo stesso numero per ciascuno utente. I token sono in genere combinati con

un altro meccanismo di autenticazione. Per esempio, gli utenti possono inserire un nome utente e una password, quindi inserire il numero visualizzato sul token: questo è un esempio di autenticazione a più fattori.
Per l'autenticazione basata su certifcate, i certificati vengono rilasciati all'utente o al dispositivo e presentati quando si accede alle risorse.

Hardware. I dispositivi token hardware utilizzano password dinamiche una tantum, rendendole più sicure delle password statiche, che rimangono le stesse per un lungo periodo di tempo.
La password dinamica viene cambiata frequentemente. Una password un tempo dinamica viene utilizzata una sola volta e non è più valido dopo che è stato utilizzato.

Software. Alcune organizzazioni utilizzano un PIN visualizzato da un'applicazione software in esecuzione sul dispositivo dell'utente. Ad esempio, un server di autenticazione potrebbe inviare periodicamente un nuovo PIN a sei cifre per un'app mobile.

HOTP/TOTP. Una tendenza che molte organizzazioni online stanno utilizzando è l'autenticazione in due passaggi.
Ad esempio, quando si accede a un sito Web di una banca, il sistema di autenticazione invia un codice tramite un messaggio di testo sul tuo cellulare. Si autentica correttamente dopo aver inserito il codice sul sito web della banca. Questo processo utilizza in genere uno dei seguenti standard e molte organizzazioni online usano una combinazione di entrambi:

CAC/PIV. Le carte Common Access Card (CAC) o Personal Identity Verifcation (PIV) sono smart card che includono immagini e altre informazioni identificative sul portatore. Gli utenti spesso li indossano come badge per la sicurezza fisica e li inseriscono nella smart card lettori per accedere alle risorse digitali.

HOTP. Il codice di autenticazione del messaggio hash (HMAC) include una funzione hash utilizzata da lo standard One-Time Password (HOTP) basato su HMAC per creare password monouso. In genere crea numeri da sei a otto cifre. Il valore HOTP rimane valido fino all'utilizzo.

TOTP. Lo standard One-Time Password basato sul tempo è simile a HOTP ma utilizza un timestamp e rimane valido solo per un periodo di tempo specifico. La password TOTP scade se l'utente non utilizza il codice entro il termine.

Smart card. Le smart card contengono informazioni su un utente ai fini dell'identificazione e / o autenticazione. Tuttavia, non sono metodi di identificazione

efficaci da soli perché possono essere facilmente persi o rubati. Molte organizzazioni richiedono agli utenti di autenticarsi utilizzando un altro metodo, ad esempio un PIN o un nome utente e una password. Smart più attuale le carte includono un microprocessore e uno o più certificati. I certificati possono essere utilizzatiper crittografia asimmetrica, come la crittografia dei dati o la posta elettronica con firma digitale.

IEEE 802.1x. IEEE 802.1x fornisce un framework per l'autenticazione e la gestione delle chiavi nelle reti cablate e wireless. In questo scenario, il software sul client comunica con il server di autenticazione. Dopo aver eseguito correttamente l'autenticazione, lo switch di rete o il punto di accesso wireless consente al client di accedere alla rete.

File system security. I metodi per proteggere i dati sui sistemi di archiviazione dei dati dipendono dal sistema file e il tipo di media. Utilizzando il principio del privilegio minimo, gli amministratori possono limitare l'accesso ai dati nei sistemi fle supportati per ridurre al minimo la perdita accidentale e intenzionale di dati o corruzione. Ad esempio, i sistemi operativi Windows utilizzano il sistema fle NTFS per limitare l'accesso degli utenti ai dati utilizzando autorizzazioni come lettura, modifica, ecc., mentre i sistemi operativi Linux utilizzano altri sistemi fle che forniscono funzionalità simili. Per proteggere i dati in memoria dispositivi che non dispongono di un sistema fle che supporta la limitazione dell'accesso, gli amministratori possono implementare crittografia. Ad esempio, i sistemi operativi Windows possono utilizzare BitLocker per andare a proteggere dati da accesso non autorizzato.

Database security .La sicurezza del database può utilizzare una vasta gamma di controlli di sicurezza per proteggere i database compromessi di riservatezza, integrità e disponibilità. Questi controlli possono essere utilizzati per proteggere i dati, le applicazioni del database o le funzioni memorizzate, i sistemi di database, i server di database e i collegamenti di rete associati. I controlli possono includere tecnici, controlli amministrativi e fisici. Ad esempio, i controlli tecnici potrebbero essere un database firewall, crittografia del database e controllo o monitoraggio delle autorizzazioni del database.

4.4 Given a scenario, di erentiate common account management practices

Sebbene esistano vari metodi per la gestione degli account, è fondamentale per un'organizzazione comprendere e implementare l'account utente appropriato e le pratiche di gestione della sicurezza dell'account.

Shared and generic accounts/credentials. Un account condiviso o generico è un account che è in genere condiviso da più di un individuo ai fini dell'accesso alle risorse. Mentre l'account ha un accesso limitato alle risorse, è difficile per le organizzazioni sapere chi ha utilizzato l'account in una determinata occasione.

Guest account. Un account ospite è simile a un account condiviso ma in genere è abilitato su richiesta per uso occasionale o singolo. Spesso, gli account degli ospiti hanno password vuote e forniscono agli utenti un accesso anonimo. Dal momento che questo può essere un rischio per la sicurezza, è un best practice per lasciare gli account ospiti disabilitati fino a quando non sono richiesti.

Service account. Un account di servizio è un account utilizzato in modo specifico da un servizio anziché un individuo (ad es. software che necessita dell'accesso alle risorse). Dal servizio gli account in genere hanno un livello di privilegi più elevato rispetto agli account utente, spesso lo sono configurato con password complesse e complesse. Tuttavia, è comune configurare il servizio account per non richiedere la scadenza della password.

Privileged account. Un account privilegiato è un account con un livello di privilegi più elevato rispetto agli account utente per le risorse. È necessario concedere i privilegi di amministratore a un utente approvazione da parte del personale competente all'interno dell'organizzazione.

Least privilege. Il principio del privilegio minimo garantisce che agli utenti venga concesso solo il privilegi di cui hanno bisogno per svolgere il loro ruolo all'interno dell'organizzazione.

Onboarding. L'onboarding è il processo di aggiunta di nuovi utenti alla gestione delle identità sistema di un'organizzazione. Il processo di onboarding viene utilizzato anche quando il ruolo lavorativo di un utente o la posizione cambia o quando all'individuo vengono concessi ulteriori livelli di privilegio o accesso.

O□boarding. L'imbarco è la rimozione dell'identità di un utente dal sistema di gestione delle identità una volta che la persona ha lasciato l'organizzazione. Ciò può includere la disabilitazione e / o eliminazione dell'account utente, revoca dei certificati e chiusura di altri specifici privilegi concessi. Può anche includere l'informazione del personale di gestione dell'accesso fisico per non consentire all'individuo di entrare nell'edificio in futuro.

Permissions auditing and review. Il controllo e la revisione delle autorizzazioni è il processo per garantire che solo gli utenti idonei abbiano accesso alle risorse

all'interno di un'organizzazione. Nell'ambito di il processo, l'organizzazione determinerà se i privilegi di ciascun utente per l'allineamento delle risorse con il ruolo dell'utente all'interno dell'organizzazione. Durante l'audit, l'organizzazione valuterà il l'efficacia dei suoi controlli di accesso e garantire che i conti siano gestiti in modo adeguato.

User account. Un account utente, noto anche come account denominato, è un account associato a un individuo ai fini dell'accesso alle risorse. Spesso, l'account avrà un accesso limitato alle risorse (ad esempio, l'utente può leggere solo determinati file ed eliminane solo alcuni).

Usage auditing and review. Il controllo e la revisione dell'utilizzo è il processo di registrazione delle azioni gli utenti eseguono le risorse all'interno di un'organizzazione. Come parte del processo, l'organizzazione determinerà se le azioni di ciascun utente si allineano ai privilegi e ai ruoli dell'utente all'interno dell'organizzazione.

Time-of-day restrictions. Le organizzazioni potrebbero scegliere di limitare l'accesso di un utente alle risorse per specificare orari in un giorno e giorni della settimana. Ad esempio, per ridurre al minimo vulnerabilità di sicurezza, un'organizzazione potrebbe implementare una politica che limita quella di un accesso dell'utente alle risorse solo per l'orario di lavoro. Di conseguenza, l'utente non avrà accesso a risorse durante le ore non lavorative.

Recertifcation. La ricertificazione è il processo di rinnovo di una certificazione e accreditamento dopo aver apportato modifiche al processo di certificazione originale o dopo un periodo di tempo specifico. La politica di sicurezza di un'organizzazione dovrebbe specificare le condizioni che richiedono la ricertificazione.

Standard naming convention. Una convenzione di denominazione standard è una convenzione concordata per le risorse di denominazione. La convenzione potrebbe essere basata sulla posizione, lo scopo o relazione e dovrebbe garantire che il nome sia univoco all'interno di un'organizzazione.

Account maintenance. Una convenzione di denominazione standard è una convenzione concordata per le risorse di denominazione. La convenzione potrebbe essere basata sulla posizione, lo scopo o relazione e dovrebbe garantire che il nome sia univoco all'interno di un'organizzazione.

Group-based access control. Le organizzazioni potrebbero scegliere di concedere l'accesso alle risorse in base all'appartenenza dell'utente a un gruppo. Questo metodo

semplifica le spese amministrative ma può indebolire la sicurezza se le autorizzazioni degli utenti non vengono controllate e riviste periodicamente.

Location-based policies. Le organizzazioni potrebbero scegliere di concedere l'accesso alle risorse in base all'appartenenza dell'utente a un gruppo. Questo metodo semplifica le spese amministrative ma può indebolire la sicurezza se le autorizzazioni degli utenti non vengono controllate e riviste periodicamente.

Account policy enforcement

Credential management. Nei sistemi che utilizzano un algoritmo di hashing come Secure Hash Algoritmo 3 (SHA-3), le password sono generalmente memorizzate come hash; sono raramente memorizzati come testo semplice. In effetti, questi sistemi non memorizzano la password: quando un utente esegue l'autenticazione, il sistema esegue l'hashing della password fornita, la confronta con l'hash della password memorizzata e autenticare l'utente solo se gli hash corrispondono.

Group policy. Le organizzazioni potrebbero implementare più criteri password per gli utenti. Le politiche potrebbero applicarsi a diversi gruppi di utenti o applicare politiche sovrapposte a vari gruppi di utenti all'interno dell'organizzazione.

Password complexity. La complessità di una password si riferisce a quanti caratteri e tipi sono inclusi nella password. Un'organizzazione può persino implementare una password criterio che richiede un numero minimo di ciascun tipo di carattere (caratteri maiuscoli, caratteri minuscoli, numeri e caratteri speciali o simboli).

CONTRO GLI HACKER NON C'E' PASSWORD CHE TENGA

Expiration. La scadenza della password è il tempo massimo di validità della password di un utente. Un'organizzazione può implementare una politica di password per la scadenza della password per definizione l'età massima della password. Ad esempio, un'organizzazione potrebbe richiedere agli utenti di cambiare la loro password dopo 90 giorni. Di conseguenza, ogni utente dovrà reimpostare la propria password prima di poter accedere alle risorse il 91 ° giorno.

Recovery. Le organizzazioni potrebbero fornire un processo attraverso il quale gli utenti possono riottenere l'accesso un account a cui non hanno più accesso. Ad esempio, una password self-service il processo di ripristino consente agli utenti di recuperare l'accesso al proprio account rispondendo a uno o più domande di sicurezza. Solo l'utente autorizzato può sapere con le risposte corrette, quali hanno fornito quando è stato effettuato il provisioning dell'account.

Disablement. Le organizzazioni potrebbero fornire un processo attraverso il quale gli utenti possono riottenere l'accesso un account a cui non hanno più accesso. Ad esempio, una password self-service il processo di ripristino consente agli utenti di recuperare l'accesso al proprio account rispondendo a uno o più domande di sicurezza. Solo l'utente autorizzato può sapere con le risposte corrette, quali hanno fornito quando è stato effettuato il provisioning dell'account.

Lockout. Un'organizzazione può implementare un criterio password per bloccare un account dopo viene inserita una password errata un numero predefinito di volte. In genere, questo numero è impostato abbastanza alto da consentire alcuni errori dell'utente.

Password history. La cronologia delle password è l'elenco delle password precedenti di un utente. In genere, i sistemi di autenticazione memorizzano molte delle password utilizzate da ciascun utente.

Password reuse. Un'organizzazione può implementare una politica di password che impedisce agli utenti dal riutilizzo delle password nell'elenco cronologico delle password. Per impedire agli utenti di ottenere attorno al criterio modificando ripetutamente la password fino a quando una password precedentemente utilizzata non viene esclusa dalla cronologia delle password e quindi può essere utilizzata di nuovo, un'organizzazione può combinare una restrizione di riutilizzo della password con un'impostazione minima dell'età della password. Per ad esempio, un'organizzazione potrebbe scegliere di impostare l'età minima della password su un giorno che gli utenti possono reimpostare le password solo una volta al giorno.

Password length. La lunghezza della password è il numero di caratteri nella password di un utente. Le password più lunghe sono più difficili da decifrare rispetto alle password più brevi. Molte organizzazioni richiedono che le password degli account privilegiati siano più lunghe di quelle degli account utente.

5. Risk Management

5.1 Explain the importance of policies, plans and procedures related to organizational security

Questo argomento è un argomento di design / architettura di alto livello. Dovresti essere a tuo agio a spiegare il concetto e sapere come possa aiutare la sicurezza di un'organizzazione.

La gestione del rischio è il modo in cui un'organizzazione gestisce la probabilità di un evento e l'impatto dell'evento sull'organizzazione. Perché ogni organizzazione assumerà un certo livello o rischio, ciò comporta in genere organizzazioni che sviluppano e implementano processi, politiche e procedure.

Standard operating procedure. Una procedura operativa standard (SOP) è l'azione specifica richiesta per implementare a meccanismo di sicurezza, controllo o soluzione specifici all'interno di un'organizzazione. Le SOP dovrebbero essere documentato in dettaglio. Nella maggior parte degli scenari, le procedure sono specifiche del sistema e del software,
quindi devono essere aggiornati con l'evolversi dell'hardware e del software. Le procedure aiutano a garantire standardizzazione della sicurezza su tutti i sistemi; se vengono seguite correttamente, tutte le attività dovrebbero essere conformi a politiche, standard e linee guida.

Agreement types. Un accordo è un accordo tra due parti. Ad esempio, un accordo costituisce un accordo tra due organizzazioni o tra IT e altri dipartimenti.

BPA. Una procedura operativa standard (SOP) è l'azione specifica richiesta per implementare a meccanismo di sicurezza, controllo o soluzione specifici all'interno di un'organizzazione. Le SOP dovrebbero essere documentato in dettaglio. Nella maggior parte degli scenari, le procedure sono specifiche del sistema e del software, quindi devono essere aggiornati con l'evolversi dell'hardware e del software. Le procedure aiutano a garantire standardizzazione della sicurezza su tutti i sistemi; se vengono seguite correttamente, tutte le attività dovrebbero essere conformi a politiche, standard e linee guida.
Un accordo di partnership commerciale (BPA) è un documento utilizzato dalle partnership commerciali per definire tutti i termini e le condizioni della relazione d'affari. In genere questo l'accordo include gli obiettivi e la durata della partnership, gli importi del contributo, obblighi contabili, distribuzione di profitti, processo per l'aggiunta o la rimozione di partner, e i termini e le condizioni di cessazione della società.

SLA. Un contratto di servizio (SLA) è un documento dettagliato che descrive la descrizione di controlli di fornitori, consulenti e appaltatori utilizzati per definire i livelli previsti di prestazione, compensazione e conseguenze. Alcuni dei componenti comuni negli SLA includono tempi di attività del sistema, tempi di fermo massimi, carico di picco, carico medio, responsabilità per i tempi di diagnostica e failover, nonché i rimedi finanziari e altri rimedi contrattuali se l'accordo viene violato.

MOU. Un protocollo d'intesa (MOU) o protocollo d'intesa (MOA), è un documento generale che definisce l'intenzione di due entità di collaborare lavorare insieme verso un obiettivo comune. Un MOU è il primo passo della comprensione reciproca tra due parti e includerà punti generali, mentre un MOA è il passo successivo quando due parti definiscono ulteriori dettagli per l'avvio di un accordo.

ISA. Un accordo di sicurezza di interconnessione (ISA) è simile a un MOU / MOA tranne che lo è più formale e include sanzioni pecuniarie se una delle parti non soddisfa i propri obblighi. Ad esempio, se due parti prevedono di trasmettere dati sensibili, possono utilizzare un ISA per specificare i requisiti tecnici della connessione, ad esempio come le due parti stabilire, mantenere e disconnettere la connessione. Potrebbe anche specificare il minimo metodi di crittografia utilizzati per proteggere i dati.

Personnel management

L'atto di gestire dipendenti e appaltatori viene definito "gestione del personale". La gestione del personale si occupa spesso del processo di assunzione di nuove persone, di licenziamento di lavoratori esistenti e di mantenimento di buoni rapporti con i dipendenti attuali.

Vacanze obbligatorie. Alcune organizzazioni hanno una politica che richiede dipendenti in posizioni sensibili per fare vacanze obbligatorie per cinque o dieci giorni consecutivi. Comune nel settore finanziario, queste politiche aiutano a scoraggiare le frodi a causa del conoscenza del fatto che un'altra persona svolgerà le mansioni e l'esame di un dipendente col loro lavoro. Inoltre, alcuni complessi sistemi di appropriazione indebita e frode richiedono il dipendente di prendere misure quotidianamente per coprire i crimini. È comune per le organizzazioni pianificare inoltre gli audit in modo che coincidano con le vacanze obbligatorie per aumentare la probabilità di scoprire frodi e altri crimini.

Job rotation. La rotazione dei posti di lavoro è una politica che obbliga i dipendenti a trasformarsi in diversi lavori, o almeno ruotare alcune delle loro funzioni. Questa pratica può scoraggiare le frodi (come il sabotaggio) e prevenire anche l'abuso di informazioni. Come le vacanze obbligatorie, la rotazione del lavoro lo rende più difficile per un dipendente coprire le proprie tracce, poiché qualcun altro svolgerà i propri compiti. Inoltre, la rotazione del lavoro può anche scoprire errori innocenti come un altro transizione dei dipendenti nel ruolo.

Separation of duties. La separazione dei compiti separa i compiti e i privilegi associati per specifici processi di sicurezza tra più persone all'interno dell'azienda. Questo processo è comunemente usato nei sistemi di contabilità finanziaria, per cui vi sono ruoli separati per ricevere assegni, depositare contanti e riconciliare estratti conto bancari e approvare scrittura o ff s. Gli stessi vantaggi esistono nella sicurezza delle informazioni, per cui ci sono ruoli separati per l'accesso di gestione a firewalls, server, account, ecc. È indispensabile che un'organizzazione implementa una politica

di sicurezza in modo che nessun singolo agente possa compromettere i controlli di sicurezza.

Clean desk. Alcune organizzazioni richiedono che una scrivania sia priva di documenti o altro materiale che potrebbe contenere informazioni sensibili o interne. Una politica di scrivania pulita assicura che i dipendenti siano a conoscenza degli oggetti lasciati fuori dalla propria scrivania. Questo impedisce maliziosi individui che camminano intorno all'uffico e si imbattono in informazioni sensibili.

Background checks. I controlli in background vengono utilizzati per identificare il precedente di una persona attività. La maggior parte dei controlli di base viene effettuata prima dell'impiego e può includere i precedenti penali, finanziari o di guida di un individuo. Mentre ci sono eccezioni alla regola, il comportamento passato è un indicatore abbastanza affidabile di come le persone potrebbero esibirsi oggi.

Exit interviews. Le interviste di uscita sono condotte quando un dipendente si ritira, si dimette è licenziato dalla compagnia. Non solo questa intervista consente alla società di recuperare attività, consente al management di conoscere eventuali problemi, problemi o lamentele che potrebbe influenzare la perdita futura. È anche vantaggioso per il management ricordare ai dipendenti che se ne vanno la società circa i dettagli di eventuali accordi di non divulgazione che sono stati firmati quando l'impiegato è stato assunto.

Role-based awareness training. La formazione è un modo chiave per garantire che i dipendenti comprendano importanti politiche e procedure aziendali. La formazione sulla consapevolezza basata sul ruolo è formazione personalizzata per ruoli. Ad esempio, la formazione che dai a qualcuno che lavora come un amministratore di rete è diverso dalla formazione impartita a un venditore. Mentre alcuni la formazione è applicabile a tutti i ruoli, in gran parte no.

Data owner. Il proprietario dei dati ha la responsabilità di garantire che l'organizzazione sia adeguata controlli di sicurezza basati sulle classificazioni dei dati definite nella politica di sicurezza. I dati il proprietario potrebbe essere ritenuto responsabile per negligenza se non riesce a stabilire e applicare le politiche di sicurezza per proteggere i dati sensibili. Ad esempio, il proprietario dei dati potrebbe essere il principale operatore operativo (COO), il presidente o un capo dipartimento.

Systems administrator. L'amministratore di sistema è responsabile della concessione dell'accesso adeguato agli utenti. Potrebbero o meno avere diritti di amministratore completi, ma lui avrà la possibilità di assegnare autorizzazioni. Gli amministratori in genere assegnano le autorizzazioni basato sul principio del privilegio minimo, in base

al quale concedono agli utenti l'accesso solo ai dati necessario per svolgere i loro compiti.

System owner. Il proprietario del sistema è la persona che possiede una risorsa o un sistema processata, inclusi dati sensibili. Il proprietario del sistema sviluppa e mantiene il piano di sicurezza del sistema e garantisce che il sistema sia distribuito in base alla sicurezza requisiti. Mentre il proprietario del sistema è in genere la stessa persona del proprietario dei dati, può avere un ruolo diverso in un'organizzazione (ad es. capo dipartimento).

User. Un utente è un individuo che accede ai dati utilizzando un sistema informatico per realizzare compiti di lavoro. In genere, gli utenti hanno accesso solo ai dati di cui hanno bisogno per svolgere il proprio lavoro compiti.

Privileged user. Un utente privilegiato è un individuo che richiede un livello superiore di privilegi alle risorse rispetto ad altri account utente. Concedere privilegi amministrativi richiede l'approvazione da parte del personale appropriato all'interno dell'organizzazione.

Executive user. Un utente esecutivo è un individuo che si trova al vertice o quasi della direzione di un'organizzazione. Mentre un utente esecutivo potrebbe non essere un utente privilegiato, l'account potrebbe richiedere controlli speciali. Ad esempio, potrebbero essere solo alcuni utenti privilegiati in grado di gestire l'account di un utente esecutivo.

NDA. Un accordo di non divulgazione (NDA) è un contratto legale tra due o più parti che dettaglia le informazioni riservate che le parti condivideranno tra loro e dovrebbe limitare l'accesso alle informazioni da terze parti. Gli NDA possono richiedere che entrambe le parti sono limitati nell'uso delle informazioni o possono limitare l'uso delle informazioni da parte di una sola festa. Ad esempio, alcuni contratti di lavoro includeranno una clausola che limita l'uso e la diffusione da parte dei dipendenti di informazioni riservate di proprietà dell'azienda.

Onboarding. L'onboarding si verifica quando un dipendente viene assunto da un'organizzazione. Alla persona vengono fornite informazioni sull'occupazione e al proprio account utente viene fornito il accesso adeguato alle risorse di sistema. Molte organizzazioni automatizzeranno questo processo assicurare coerenza e aderire alle pratiche di sicurezza.

Continuing education. Poiché le minacce alla sicurezza informatica sono in costante evoluzione, è importante affinché un'organizzazione fornisca al personale addetto alla

sicurezza gli strumenti e le conoscenze per comprendere le potenziali minacce e come evitarle. Come minimo, la formazione sulla sicurezza informatica dovrebbe includere i metodi di attacco più comuni, gli strumenti e le tecniche utilizzate per la protezione dagli attacchi e la metodologia appropriata per rispondere agli incidenti della sicurezza informatica.

PER QUESTO ABBIAMO TRADOTTO E SEMPLIFICATO QUESTO TESTO CHE DOVREBBE ESSERE LETTO DA TUTTI E CAPITO ALMENO AL 50 %.

Acceptable use policy/rules of behavior. Una politica di utilizzo accettabile (AUP) è un insieme di regole difeso dall'organizzazione che dettaglia il tipo di comportamento consentito durante l'utilizzo beni aziendali. Un AUP dovrebbe contenere un linguaggio esplicito che contenga i requisiti procedurali e le responsabilità degli utenti. Lo scopo di AUP è di aiutare a limitare i rischi poste a un'organizzazione salvaguardando l'azienda e le sue proprietà, sia fisiche che intellettiali.
Adverse actions. Mentre è difficile identificare tutti i comportamenti inappropriati, un'organizzazione dovrebbe informare i dipendenti che le azioni avverse che l'effetto operazioni aziendali potrebbero causare una sospensione dei servizi. Questo dovrebbe essere descritto nell'AUP o nella politica di sicurezza.

General security
policy. Le politiche di sicurezza generali dovrebbero identificare le regole e le procedure per tutte le persone che accedono ai beni e alle risorse di un'organizzazione. Le politiche di sicurezza dovrebbero anche definire come a la società prevede di proteggere le risorse e le risorse fisiche e informatiche.

Social media networks/applications. Un'organizzazione dovrebbe sviluppare una politica di sicurezza dei social media che regola l'uso dei social media da parte dei dipendenti. Durante l'utilizzo dei social media per motivi di lavoro può essere vantaggioso per l'organizzazione, avere regole chiaramente definite e le procedure per l'utilizzo dei social media dalle risorse dell'azienda possono ridurre significativamente il rischio.

Personal email. La politica di sicurezza dovrebbe chiaramente definire l'uso di e-mail aziendali e personali. Ad esempio, la politica potrebbe indicare che l'uso personale della posta elettronica aziendale è rigorosamente vietato o la politica potrebbe includere linee guida sull'uso personale dell'email aziendale.
Alcune organizzazioni consentono ai dipendenti di accedere alla posta elettronica personale da risorse aziendali (ad es.computer, dispositivi mobili, ecc.). Perché l'accesso a questi indirizzi e-mail non controllati presenta un rischio per

l'organizzazione, la politica di sicurezza dovrebbe definire come e quando i dipendenti possono accedere alla loro e-mail personale.

5.2 Summarize business impact analysis concepts . Questa sezione è focalizzata sui concetti di analisi dell'impatto sul business ma rimane ad un livello elevato, simile a cosa ci si potrebbe aspettare da un manager o direttore.

RPO. Un obiettivo del punto di ripristino (RPO) è un momento specifico nel quale una risorsa può essere ripristinata. In genere i proprietari delle risorse o delle applicazioni decidono l'RPO e la direzione lo approva. IT sta configura la frequenza richiesta di replica e / o backup per soddisfare l'RPO. Per esempio, è necessario eseguire il backup delle risorse critiche più frequentemente rispetto alle risorse meno critiche.

RTO. Un obiettivo di tempo di recupero (RTO) definisce per quanto tempo l'organizzazione può operare senza risorsa o applicazione. Ancora una volta, i proprietari delle risorse o delle applicazioni decidono su RTO e la direzione lo approva. Il personale IT configura i sistemi e / o l'ambiente da soddisfare la RTO. Ad esempio, i tempi di recupero per le app critiche sono spesso molto brevi.

Functions Identifcation of critical systems

MTTF/MTTR. Per la gestione del ciclo di vita dell'hardware all'interno di un'organizzazione, è necessario pianificare l'hardware per sostituzione e / o riparazione. Il programma dovrebbe essere basato sul tempo medio di fallimento (MTTF) e tempo medio di riparazione (MTTR) stabiliti per ciascun asset. Tipicamente, MTTF è la durata funzionale prevista dell'asset in base a un ambiente operativo specifico. MTTR è il tempo medio necessario per eseguire una riparazione sul dispositivo.

MTBF. Il tempo medio tra guasti (MTBF) è il tempo medio tra un guasto e un successivo fallimento. I produttori spesso elencano solo MTTF se i valori MTTF e MTBF sono uguali.

Mission-essential. Le funzioni essenziali della missione sono un insieme defunto di funzioni in un'organizzazione che deve essere continuato o ripreso rapidamente dopo un'interruzione delle normali operazioni. Alcune organizzazioni implementeranno livelli di funzioni essenziali per la missione.

Dopo aver difeso le funzioni essenziali della missione in un'organizzazione, è importante identificare i sistemi critici che supportano queste funzioni. Un sistema critico è definito come un sistema che deve essere altamente disponibile e / o affidabile. I sistemi più critici sono legati alla sicurezza, missione, affari o sicurezza.

Single point of failure. Un singolo punto di errore fa parte di un sistema che causerà un errore dell'intero del sistema, se presente non riesce. Un singolo punto di errore non è auspicabile per le organizzazioni con un obiettivo di elevata disponibilità.

Impact L'impatto è una stima delle potenziali perdite per un'organizzazione associata a uno specifico rischio. Durante l'analisi del rischio, le organizzazioni svilupperanno una stima della probabilità e dell'impatto. I tipi comuni di impatto includono:

Life. Le organizzazioni potrebbero stimare le valutazioni dei rischi in base all'impatto sulla vita o sulla qualità della vita, fattori. Ad esempio, un'organizzazione potrebbe considerare l'impatto della salute il club beneficia i dipendenti.

Property. Le organizzazioni potrebbero stimare le valutazioni del rischio in base all'impatto sulla proprietà. Ad esempio, un'organizzazione potrebbe considerare l'impatto delle apparecchiature di leasing al contrario ad acquistarlo.

Safety. Le organizzazioni potrebbero stimare le valutazioni dei rischi in base ai rischi per la sicurezza o la salute.
Questi potrebbero essere correlati a un luogo, stile di vita, occupazione o attività. Ad esempio, un'organizzazione potrebbe considerare il rischio di acquistare un edificio in cui tornado o terremoti sono ricorrenze comuni.

Financial. Le organizzazioni potrebbero stimare valutazioni del rischio basate su tali impatti finanziari come entrate, costi e spese persi.

Reputation. Le organizzazioni potrebbero stimare le valutazioni dei rischi in base all'impatto sociale fattori come la reputazione. Ad esempio, un'organizzazione potrebbe valutare il rischio di difendere partiti politici per paura di alienare parte della base di clienti.

assessment

Privacy impact . Una valutazione dell'impatto sulla privacy è un processo che aiuta le organizzazioni a identificare e minimizzare i rischi per la privacy di nuovi progetti o politiche. L'organizzazione controlla la propria elabora e identifica il modo in cui questi processi potrebbero influire o compromettere la privacy di le persone i cui dati sono raccolti, raccolti o elaborati.

Privacy threshold assessment. Una valutazione della soglia di privacy aiuta un'organizzazione a determinare se un sistema contiene informazioni private. È uno strumento efficace che aiuta le organizzazioni ad analizzare e registrare i requisiti di

documentazione sulla privacy delle attività aziendali e determinare se una privacy è richiesta una valutazione d'impatto.

5.3 Explain risk management processes and concepts

Come con la sezione precedente, devi essere a tuo agio con i concetti qui, specialmente come un manager potrebbe avere familiarità con loro. C'è meno attenzione ai tecnicismi e più attenzione agli aspetti commerciali.

Threat assessment Una valutazione della minaccia viene utilizzata da un'organizzazione per determinare la credibilità e la gravità di una potenziale minaccia, nonché la probabilità che la minaccia diventi realtà. In genere, una valutazione della minaccia include identificazione, valutazione iniziale, gestione dei casi e valutazione di follow-up. Queste informazioni ottenute da una valutazione della minaccia sono utilizzate in una valutazione di rischio. I tipi di minacce includono:

Environmental. Le minacce ambientali o "Madre natura" sono tornadi, terremoti, inondazioni, siccità, ecc.

Manmade. Le minacce artificiali possono essere intenzionali o accidentali e possono includere la perdita di dati, hacking, ecc.

Internal vs. external. Tutte le minacce che le organizzazioni prendono in considerazione durante una valutazione delle minacce rientrerà in una delle due categorie: interna o esterna. Le minacce interne sono minacce che un'organizzazione può controllare. Ad esempio, un'organizzazione potrebbe valutare il rischio di implementazione un sistema di prevenzione della perdita di dati per garantire che i dati aziendali non siano esposti a personale non autorizzato. D'altra parte, le minacce esterne sono minacce che un'organizzazione non è in grado di controllare. Ad esempio, un'organizzazione non può controllare meteo, manifestanti o hacker esterni.

SLE. L'aspettativa a perdita singola (SLE) è il valore monetario atteso di un'attività a causa del insorgenza di un rischio.

ALE. L'aspettativa di perdita annualizzata (ALE) è la perdita monetaria attesa di un'attività dovuta al verificarsi di un rischio per un periodo di un anno.

ARO. Il tasso annualizzato di occorrenza (ARO) è la frequenza alla quale si prevede che un rischio si verificano su un periodo di un anno. Il valore ARO può variare da zero, indicando che il rischio è si prevede che non si verifichi mai, per un numero molto elevato, indicando che il rischio si verifica frequentemente.

Asset value. Come parte di una valutazione del rischio, un'organizzazione valuterà il valore delle attività.
Il valore assegnato a un'attività è specifico e comprende costi tangibili (ad es. Acquisto costo) nonché i costi immateriali (ad es. valore per il concorrente).

Risk register. Un registro dei rischi, chiamato anche registro dei rischi, è un documento principale gestito da un'organizzazione durante una valutazione del rischio per tenere traccia dei problemi e affrontare i problemi non appena si presentano.

Likelihood of occurrence. La probabilità che si verifichi è la probabilità che uno specifico si verificherà il rischio. Il valore può essere espresso in una frazione compresa tra 0 e 1 o in percentuale.

Supply chain assessment. Come parte di una valutazione del rischio, un'organizzazione potrebbe eseguire una valutazione della catena di approvvigionamento al fine di ridurre la vulnerabilità e garantire continuità in affari. Utilizzando gli strumenti del processo di gestione dei rischi, le organizzazioni valutano i rischi e incertezze causate da attività logistiche o risorse da parte dei partner nella fornitura catena.

Impact. L'impatto di un rischio è le conseguenze se si verifica (ovvero, il costo di un rischio). Valutazione del rischio Durante la gestione del rischio, un'organizzazione determina la probabilità di un evento e il impatto dell'evento sull'organizzazione. Il processo può essere molto dettagliato, complesso e lungo e prevede più passaggi. Ecco i termini chiave da comprendere:

Quantitative. Una delle due metodologie di valutazione del rischio, la valutazione quantitativa del rischio assegna i costi effettivi alla perdita di un'attività. Entrambi i metodi sono importanti per una valutazione completa del rischio, poiché la maggior parte delle organizzazioni utilizza un ibrido di entrambe le metodologie in ordine per ottenere una visione equilibrata.

Qualitative. Una delle due metodologie di valutazione del rischio, la valutazione qualitativa del rischio assegna costi soggettivi e immateriali alla perdita di un'attività. Entrambi i metodi sono importanti per una valutazione completa del rischio, poiché la maggior parte delle organizzazioni utilizza un ibrido di entrambe le metodologie per ottenere una visione equilibrata.

Testing. Un'organizzazione potrebbe scegliere di utilizzare test basati sul rischio per valutare il sistema qualità e riduzione della probabilità di difetti del sistema. Quando

le organizzazioni mancano di sufficiente tempo per testare tutte le funzionalità del sistema, i test basati sul rischio potrebbero includere la convalida del sistema funzionalità che ha il massimo impatto e probabilità di fallimento.

Penetration testing authorization. Prima che un team di sicurezza informatica possa eseguire simulazioni di attacchi della rete e dei sistemi di un'organizzazione, devono ottenere l'autorizzazione dall'organizzazione. L'autorizzazione potrebbe includere l'ambito del test, la responsabilità e / o l'accesso fisico.

PER IL GDPR CI VOGLIONO CONTRATTI TRA AZIENDA CLIENTE E TEAM DI PENETRATION TESTING, CON AVVOCATI, ASSICURAZIONI CHE TUTTI NON POSSONO SOSTENERE ECONOMICAMENTE. IL PRODOTTO VULNER DI ROBIONICA RISOLVE IL PROBLEMS E RIENTRA NEL PARAGRAFO SUCCESSIVO

Vulnerability testing authorization. Prima che un team di sicurezza informatica possa eseguire la scansione dei sistemi e la rete di un'organizzazione per identificare le vulnerabilità di sicurezza, devono ottenere l'autorizzazione dall'organizzazione.

VULNER SCANDISCE I SITI PER TROVARE VULNERABILITA' E NON SCANDISCE LE RETI, CI SONO ALTRI CHE LO FANNO

Risk response techniques. Dopo che un'organizzazione ha completato una valutazione del rischio, loro deve affrontare ogni rischio specifico utilizzando una delle seguenti opzioni: Accettare. Un'organizzazione potrebbe accettare il rischio (in base alla propria tolleranza al rischio) dopo l'analisi costi / benefici determina che il costo delle contromisure sarebbe superiore al costo della perdita di attività a causa di un rischio. In genere, accettare il rischio richiede una dichiarazione scritta ciò indica perché non è stata implementata una protezione e chi è responsabile, nonché le conseguenze se il rischio è realizzato.

Transfer. Un'organizzazione potrebbe trasferire o assegnare il rischio collocando il costo della perdita su un'altra entità interna o esterna all'organizzazione. Ad esempio, un'organizzazione potrebbe acquistare un'assicurazione o esternalizzare alcune responsabilità.

Avoid. Un'organizzazione potrebbe evitare il rischio selezionando opzioni alternative che hanno meno rischio associato rispetto all'opzione predefinita. Ad esempio, un'organizzazione potrebbe richiedere i dipendenti devono volare verso le destinazioni piuttosto che consentire loro di guidare.

Mitigate. Un'organizzazione potrebbe ridurre il rischio (chiamato anche mitigazione del rischio) implementando misure di sicurezza o contromisure per eliminare le vulnerabilità o bloccare le minacce. Sulla nota a margine, la selezione delle contromisure è un'attività di valutazione post-rischio.

Change management La gestione delle modifiche viene utilizzata dalle organizzazioni per garantire che nessuna modifica comporti una riduzione o sicurezza compromessa. Mentre la gestione del cambiamento aiuta le organizzazioni a prevenire indesiderate riduzioni della sicurezza, l'obiettivo principale della gestione delle modifiche è garantire che tutte le modifiche nell'organizzazione include documentazione dettagliata , controllo, può essere rivisto e esaminato.

5.4 Given a scenario, follow incident response procedures

In questa sezione, l'ordine è importante. Assicurati di capire l'ordine che prende una risposta e le persone coinvolte nei vari compiti.

Incident response plan. Un piano di risposta agli incidenti è un documento che aiuta l'IT a rispondere a un incidente. Include dettagli su come rilevare, come rispondere e come recuperare.

Documented incident types/category defnitions. Per creare il piano di risposta agli incidenti, un'organizzazione definirà gli eventi comuni che classificano come incidenti di sicurezza, ad esempio come tentativo di intrusione di rete, tentativo di attacco denial-of-service, rilevamento di software dannoso, accesso non autorizzato ai dati o violazione delle politiche di sicurezza.

Computer incident response team. Un team di risposta agli incidenti informatici o cyber-incidente team di risposta (CIRT), è un gruppo accuratamente selezionato di persone ben addestrate il cui scopo è rispondere a un incidente informatico o di sicurezza informatica. Questa squadra gestirà l'incidente in modo che possa essere rapidamente contenuto e studiato, e l'organizzazione può recuperare. Il
il team è generalmente composto da dipendenti che possono abbandonare le loro attuali responsabilità e avere l'autorità per prendere decisioni critiche.

Deter. Un'organizzazione potrebbe scoraggiare i rischi implementando deterrenti per i trasgressori sicurezza e politica. Ad esempio, un'organizzazione potrebbe implementare audit, sicurezza telecamere o autenticazione avanzata.

Ignore. Un'organizzazione potrebbe ignorare o rifiutare il rischio, negando l'esistenza di un rischio. In questo scenario, l'organizzazione spera che il rischio non sarà mai

realizzato. Questo dovrebbe essere considerato una tecnica di risposta al rischio inaccettabile.

Information Security. Il ruolo della sicurezza delle informazioni include la valutazione dell'entità del danno, contenimento, analisi forensi di base e recupero. I membri delle informazioni, Il team di sicurezza sono addestratoinella gestione degli incidenti elettronici.
IT/MIS. Il ruolo IT/MIS è quello di facilitare gli effetti agli utenti e di assistere le informazioni Squadra di sicurezza con le questioni tecniche come richiesto. In caso di un incidente, l'IT team dovrà sapere dove è possibile accedere ai dati e quali aree della rete vi sono limiti o no.

IT Auditor. Il ruolo del revisore IT è quello di osservare e apprendere come è iniziato un incidente, garantire che vengano seguite le procedure e collaborano con IT e sicurezza per evitare problemi in futuro.
I revisori IT potrebbero essere presenti durante un incidente (ad esempio se lavorano per l'organizzazione), ma in quel momento non intraprenderanno molte azioni.

Security. Il ruolo di sicurezza può includere la valutazione di eventuali danni fisici, l'indagine di prove fisiche e la protezione delle prove durante un'indagine forense a mantenere una catena di prove. Se un incidente comporta il contatto diretto con un bene, il team di sicurezza dovrebbe avere l'addestramento appropriato per assistere

Attorney. Il ruolo del procuratore è quello di garantire l'usabilità di qualsiasi prova raccolta durante un'indagine nel caso in cui la società scelga di intraprendere un'azione legale. L'avvocato può anche fornire consulenza in merito a problemi di responsabilità in caso di incidente attira clienti, distributori o il pubblico in generale.

Human Resources. Il ruolo delle risorse umane è quello di fornire consigli su come gestire situazioni che coinvolgono i dipendenti. Le risorse umane in genere non verranno utilizzate fino a dopo un'indagine è iniziato e solo se è coinvolto un dipendente.

Public Relations. Il ruolo delle pubbliche relazioni è quello di comunicare con i team leader per garantire una comprensione accurata del problema e dello stato dell'azienda e comunicare con la stampa o informare gli azionisti della situazione attuale. L'immagine dell'azienda è un bene che ha un valore considerevole, specialmente se lo è quotata in Borsa.

Financial Auditor. Il revisore finanziario tenterà di assegnare un numero monetario al danno che si è verificato a seguito di un incidente. Questo valore monetario è frequentemente richiesto per le compagnie di assicurazione e richiesto se l'organizzazione intraprende azioni legali.
Tuttavia, è considerato uno degli aspetti più difficili della valutazione di un incidente.

Management. Il ruolo della direzione durante un incidente, oltre a dare alla squadra l'autorità per operare, è prendere le grandi decisioni sulla base del contributo degli altri membri della squadra.

Roles and responsibilities. Chi è incluso in un CIRT e i loro ruoli dipenderanno in gran parte dai bisogni e le risorse dell'organizzazione. Mentre il team può includere personale esterno (ad es. forze dell'ordine, venditori o specialisti tecnici), ecco un elenco dei ruoli comuni:

Reporting requirements/escalation. Le procedure di segnalazione e escalation degli eventi dovrebbero essere documentati nel piano di risposta agli incidenti. Questo processo garantirà la sicurezza delle informazioni degli eventi e punti deboli associati ai sistemi che vengono comunicati in modo tempestivo, può essere intrapresa l'azione correttiva appropriata.

Cyber-incident response teams. Un team di risposta agli incidenti informatici è responsabile dell'elaborazione del piano di risposta agli incidenti informatici. Il team è un team tecnico e inizia a rispondere immediatamente dopo aver appreso di un incidente. L'obiettivo finale è quello di sradicare i componenti dell'incidente (come malware) e far funzionare di nuovo normalmente l'organizzazione.

Exercise. Un team di risposta agli incidenti informatici è responsabile dell'elaborazione del piano di risposta agli incidenti informatici. Il team è un team tecnico e inizia a rispondere immediatamente dopo aver appreso di un incidente. L'obiettivo finale è quello di sradicare i componenti dell'incidente (come malware) e far funzionare di nuovo normalmente l'organizzazione.

Incident response process. Un processo di risposta agli incidenti efficace viene gestito in più fasi o fasi.

Preparation. Durante la fase di preparazione, un'organizzazione stabilirà una capacità di risposta agli incidenti in modo che l'organizzazione sia pronta a rispondere agli incidenti. Inoltre, l'organizzazione pianificherà di prevenire incidenti garantendo che sistemi, reti e applicazioni siano sicuri.

Identifcation. Una delle parti più difficili del processo di risposta agli incidenti è determinare con precisione se si è verificato un incidente e, in tal caso, l'entità e l'entità del problema. Durante questa fase, un'organizzazione determinerà se un incidente si è verificato in passato, si sta verificando ora o potrebbe verificarsi in futuro.

Containment. La maggior parte degli incidenti richiede contenimento, quindi è importante per un'organizzazione sviluppare una strategia di riparazione personalizzata. Come parte della fase di contenimento, un'organizzazione documenta le azioni e le procedure per ciascun tipo di incidente (ad es. spegnimento di un sistema, scollegarlo da una rete, ecc.).

Eradication. Dopo che un incidente è stato contenuto, un'organizzazione potrebbe aver bisogno di sradicare o eliminare i componenti dell'incidente. Ad esempio, durante questa fase, un'organizzazione potrebbe dover eliminare malware o disabilitare gli account utente violati, nonché mitigarli vulnerabilità che sono state sfruttate. Durante la fase di eradicazione, è importante identificare tutti gli host within etti all'interno dell'organizzazione in modo che possano essere corretti.

Recovery. Durante la fase di ripristino, un'organizzazione ripristinerà tutti i sistemi interessati funzionamento normale e verificare che i sistemi funzionino normalmente. Inoltre, l'organizzazione potrebbe dover riparare le vulnerabilità identificate per prevenire incidenti simili.
Ad esempio, durante questa fase un'organizzazione potrebbe ripristinare i sistemi da backup, ricostruire sistemi, installare patch / aggiornamenti, cambiare password o configurare frewalls.

5.5 Summarize basic concepts of forensics

Lessons learned. Dopo il recupero, è importante che un'organizzazione organizzi una riunione con tutte le parti interessate e identificare eventuali miglioramenti che possono essere apportati al processo. Lo svolgimento di una riunione di "lezioni apprese" può essere estremamente utile per migliorare la misura di sicurezza e il processo di gestione degli incidenti. Questo incontro consente all'organizzazione di ottenere la chiusura di un incidente esaminando ciò che è accaduto e l'efficacia di passaggi di risposta agli incidenti. Idealmente, questa riunione dovrebbe svolgersi entro alcuni giorni dall'incidente per garantire una maggiore precisione nel ricordare eventi e azioni.

Order of volatility . L'ordine di volatilità è l'ordine in cui un'organizzazione dovrebbe raccogliere prove forensi. Poiché i dati altamente volatili possono essere facilmente persi, i dati più volatili dovrebbero essere raccolti prima e i dati meno volatili

dovrebbero essere raccolti per ultimi. Ad esempio, un'organizzazione potrebbe scegliere il seguente ordine: memoria fisica, memoria virtuale, unità disco, backup e stampe.

Chain of custody. In scenari in cui le prove potrebbero essere utilizzate in controversie civili o penali, è importante per un'organizzazione per stabilire una catena di custodia, nota anche come catena di prove, che documenta l'ubicazione delle prove dal momento in cui sono raccolte al momento in cui sono raccolte appare in tribunale. Questo può includere la polizia che lo raccoglie, i tecnici delle prove che elaborarlo e gli avvocati che lo utilizzano in tribunale.

Legal hold. Una sospensione legale è un processo che un'organizzazione potrebbe utilizzare per conservare tutte le informazioni pertinenti quando è previsto un contenzioso. Il processo di conservazione legale è in genere avviato da una comunicazione di un avvocato a un'organizzazione per sospendere la normale disposizione di documenti, ad esempio come il riciclaggio dei backup su nastro o l'archiviazione o la cancellazione dei dati. In base al tipo di supporto, esistono vari metodi che un'organizzazione può utilizzare per recuperare dati ai fini dell'analisi forense.

Data acquisition

Capture system image. Quando si acquisisce un'immagine di sistema, un'organizzazione creerà un duplicato esatto a livello di settore dei media. In genere, il duplicato viene creato utilizzando un duplicatore del disco rigido o uno strumento di imaging del software che rispecchia i dati a livello di blocco.

Network trafc and logs. Come parte della rete forense, un'organizzazione potrebbe monitorare e analizzare il traffico di computer ai fini del rilevamento e delle informazioni sulle intrusioni raccolta o come parte delle prove in contenzioso. Un'organizzazione potrebbe anche utilizzare la rete sniffing, registrazione, acquisizione e analisi del traffico di rete e dei registri eventi in ordine per indagare su un incidente di sicurezza della rete.

Capture video. Durante l'acquisizione di video e / o audio ai fini dell'analisi forense, è importante per un'organizzazione comprendere come il sistema registra i dati (ad es. digitale o analogico) e le opzioni disponibili per recuperare i dati (ad es. scrittura di CD / DVD, USB, ecc.).

Record time offset. Durante la riproduzione di un'immagine di sistema, media o dati, è importante affinché un'organizzazione comprenda il tempo stabilito per la registrazione delle informazioni (ad es. fuso orario). Il tempo impostato viene in

genere registrato durante l'acquisizione dei dati per garantire ciò, gli investigatori spiegano la differenza quando rivedono le informazioni in un secondo momento.

Take hashes. Dopo che un'immagine è stata acquisita, viene generalmente verificata in punti critici durante l'analisi per garantire che l'evidenza sia ancora nel suo stato originale. Questa verifica include in genere l'utilizzo delle funzioni hash SHA-1 o MD5. Il processo di verifica del file l'immagine con una funzione hash è chiamata hash.

Screenshots. In alcuni scenari, può essere necessario acquisire informazioni per analisi forensi usando schermate. In genere, si tratta ancora di catturare immagini di informazioni sullo schermo del computer. Questo è comunemente usato nell'analisi forense meno critica o negli scenari quando l'acquisizione di un'immagine di sistema, supporto o dati non è disponibile.

Witness interviews. Molte volte durante l'analisi forense, è importante intervistare, o deporre, individui che potrebbero avere conoscenze dirette relative all'incidente. Questo può includere le persone responsabili dei sistemi o dei dispositivi di rete che erano compromesso o individui che potrebbero avere informazioni sull'attacco.

Preservation Recovery. Dopo che i dati sono stati acquisiti, devono essere conservati come prova. Mentre ci sono varie leggi che coprono il sequestro e la conservazione dei dati, in casi penali ciò verrà spesso eseguito da parte delle forze dell'ordine, come richiesto da un mandato. Tuttavia, nel contenzioso civile lo farà in genere unuffico all'interno dell'organizzazione. Il presupposto è che un'azienda è in grado di fare investigare le proprie attrezzature senza un mandato.

Gathering. Molte volte durante un'analisi forense, può essere necessario recuperare le informazioni che sono state eliminate intenzionalmente o per errore. È responsabilità di un ricercatore recuperare quante più prove possibile usando vari strumenti o metodologie. Il tipo di dati recuperati varia a seconda dell'indagine, ma esempi includono log di chat, email, documenti, immagini o cronologia di Internet. Questi dati potrebbero essere recuperati dallo spazio accessibile del disco, spazio eliminato (o non allocato) o file cache del sistema operativo.

Strategic intelligence. L'intelligenza strategica è la raccolta, l'elaborazione, l'analisi e la diffusione dell'intelligenza di informazioni per la formulazione di piani politici e militari nell'ambito della politica internazionale e nazionale livelli. Nel mondo commerciale, queste informazioni vengono utilizzate per costruire qualità che consentano ai leader essere strateghi e ective caci. Le informazioni di intelligence

raccolte nel controspionaggio sono per proteggere il programma di intelligence di un'organizzazione da un aggressore o dall'opposizione servizio di intelligence. Le informazioni raccolte possono essere utilizzate per analisi forensi, contatore spionaggio o sabotaggio.

Counterintelligence .Nel calcolare i valori di costo in una valutazione quantitativa del rischio, è importante che un'organizzazione tenga traccia delle ore-uomo e delle spese sostenute dal team di risposta agli incidenti. Questo è perché le valutazioni utilizzano importi monetari specifici, come i costi e i valori delle attività.

Active logging. Durante la raccolta del controspionaggio, potrebbe essere necessario che un'organizzazione mantenga registri attivi dell'attività dell'opposizione o dell'attaccante.

Hot site. Un sito di backup attivo è un duplicato dell'attuale data center dell'organizzazione. Tutti i sistemi sono configurati con backup quasi completi dei dati dell'utente. In genere, in tempo reale la sincronizzazione viene utilizzata tra i siti per garantire che i dati siano aggiornati. Mentre un sito caldo è il opzione più costosa, consente all'organizzazione di ripristinare le normali operazioni in il tempo più breve con perdite minime dopo un disastro.

5.6 Explain disaster recovery and continuity of operations concepts

Questa sezione è incentrata sulla continuità aziendale e il ripristino di emergenza. Molti professionisti IT hanno esposizione a vari aspetti di questi argomenti nel loro lavoro quotidiano, quindi potresti già essere a tuo agio con molte delle informazioni qui.

Recovery sites In base ai requisiti aziendali, potrebbe essere necessario disporre di una posizione in cui un'organizzazione può trasferirsi a seguito di un ripristino di emergenza. Questa posizione è nota come ripristino o backup, sito.

Warm site. Un sito caldo contiene tutto l'hardware e la connettività necessari per il ripristino Servizi; è un duplicato ragionevole dell'attuale data center dell'organizzazione. Tuttavia, i dati devono essere ripristinati dopo un disastro. Ad esempio, gli ultimi backup dal sito Web la struttura di deposito deve essere consegnata e il restauro in metallo nudo deve essere completato.

Cold site. Un sito freddo è semplicemente uno spazio operativo vuoto con servizi di base. Qualunque cosa necessaria per ripristinare il servizio deve essere procurato e consegnato al sito prima del recupero può iniziare. Mentre un sito freddo è il meno costoso, il ritardo nel diventare completamente operativo può essere sostanziale.

Full. Un backup completo è una copia completa dei dati. Un backup completo fornisce il più semplice metodo di recupero, poiché è possibile ripristinare facilmente tutti i dati utilizzando un singolo ripristino impostato. Tuttavia, molte organizzazioni li usano su base periodica solo perché richiedono molto tempo e richiedono una grande quantità di spazio di backup.

Incremental. Un backup incrementale copia solo i dati che sono stati modificati dal backup precedente, indipendentemente dal fatto che il backup fosse completo o incrementale. Un backup incrementale fornisce il tempo di backup più rapido e richiede la quantità minima di archiviazione di backup. Tuttavia, un backup incrementale ha un tempo di recupero più lento, dal momento che tutti i backup incrementali devono essere ripristinati.

Differential. Un backup differenziale copia solo i dati che sono stati modificati rispetto al backup completo precedente; è considerato un backup incrementale cumulativo. Un backup diverso fornisce un tempo di ripristino più rapido e richiede meno spazio di archiviazione rispetto a un backup incrementale di backup. Tuttavia, un backup differenziale richiede più tempo per la creazione di un backup incrementale di backup.

Snapshots. Un'istantanea è una copia di un'applicazione, disco o sistema. In genere, un'organizzazione utilizzerà un'istantanea per ripristinare un sistema o un disco a un'ora specifica. Tuttavia, un'istantanea non viene comunemente utilizzato come strategia di backup periodica a causa della quantità di backup tempo e memoria di backup richiesti.

Backup concepts

Order of restoration .Poiché lo stato e le risorse sono limitate durante il ripristino, quando si pianifica il ripristino di emergenza, è importante che un'organizzazione determini l'ordine in cui i sistemi dovrebbero essere portati online - dai sistemi critici che dovrebbero essere ripristinati dal minimo al minimo sistemi critici che dovrebbero essere ripristinati per ultimi. L'organizzazione dovrebbe rivedere periodicamente l'ordine dell'elenco dei restauri mentre i nuovi sistemi vengono portati online e i sistemi legacy vengono dismessi.
Quando si pianifica un ripristino dei dati dopo un disastro, un'organizzazione dovrebbe scegliere il tipo di backup appropriato che soddisfi i requisiti aziendali.

Off-site backups. L'implementazione dei backup garantisce la redundancy dei dati, l'hosting i backup in una posizione esterna garantiscono che i dati ridondanti non ne abbiano uno singolo punto geografico di fallimento.

Distance. Un'organizzazione dovrebbe includere una distanza sufficiente tra un sito primario e secondario per ridurre al minimo il potenziale di un disastro che attacca entrambi i siti contemporaneamente (ad es. interruzione di corrente, fre, tornado, uragano, ecc.). Mentre ci sono opinioni diverse sulla distanza minima tra un sito primario e secondario, la distanza più appropriata dipende dai requisiti aziendali.

Location selection. Quando si sceglie la posizione di un sito primario o secondario, è importante valutare i rischi ambientali, ad esempio se la posizione è suscettibile di catastrofi naturali specifiche (ad es. pianura alluvionale, linea di faglia, frequenza di tornado o uragani, eccetera.). Inoltre, l'organizzazione dovrebbe considerare la disponibilità di risorse tecniche in ogni posizione. Ciò può includere requisiti di stabilità, accesso a parti di ricambio, accesso a fonti di energia alternative, ecc.

Legal implications. In base al settore di un'organizzazione, potrebbero esserci delle leggi che incidono sulla pianificazione della continuità aziendale. Ad esempio, le imprese del settore sanitario è necessario disporre di un piano di ripristino di emergenza con linee guida stabilite per l'elettronica registri e firme. Esistono diverse leggi che regolano l'assistenza sanitaria, industrie governative, finanziarie e dei servizi pubblici.

Data sovereignty. Quando si pianifica la diversità geografica, un'organizzazione potrebbe aver bisogno di considerare le leggi sulla sovranità che regolano i dati. Ad esempio, potrebbero esserci stati o leggi locali che richiedono l'hosting dei dati in posizioni specifiche.

Tabletop exercises. Lo scopo degli esercizi da tavolo per la pianificazione della continuità operativa è dimostrare la capacità di uno o più processi aziendali critici di continuare la funzionalità dopo un'interruzione, di solito entro un periodo di tempo specifico. Alcuni di questi esercizi potrebbero essere correlati a un attacco informatico, corruzione o perdita di dati, disastri naturali o multipli interruzioni.

After-action report. Il rapporto post-azione è un documento dettagliato che riassume i risultati degli esercizi da tavolo. Può includere lo scopo e la portata, gli obiettivi, il tipo di esercizio e la metodologia, lo scenario, i partecipanti e i risultati (ad es. Successi, fallimenti, soluzioni alternative, ecc.).

Geographic considerations .È indispensabile che un'organizzazione includa la diversità geografica quando pianifica la continuità aziendale e il ripristino di emergenza.

Continuity of operations planning. La continuità della pianificazione delle operazioni aiuta a garantire operazioni senza problemi attraverso un'interruzione imprevista.

Failover. Dopo un'interruzione delle operazioni aziendali, un'organizzazione potrebbe dover considerare il failover di tutti i sistemi di informazione su un sito alternativo. Allo stesso modo, le operazioni commerciali la pianificazione deve tenere conto dei servizi disponibili durante l'interruzione e come accoglieranno l'accesso dei dipendenti a tali servizi.

Alternate processing site. Il sito alternativo di elaborazione è un sito che consente di ripristinare tutte le funzioni mission-critical o business-essenziali in caso del sito di trattamento primario. Il sito di trattamento alternativo dovrebbe mantenere la continuità attraverso il ripristino dei servizi al sito di trattamento primario.

Alternate business practices. Potrebbe essere necessario per un'organizzazione implementare un alternanza di pratiche commerciali dopo un'interruzione. Ad esempio, potrebbe essere richiesto al personale non mission-critical di lavorare da casa e i dipendenti potrebbero dover ricorrere a supplenti (o manuali) processi per lo svolgimento delle attività quotidiane fino al ripristino dei servizi.

5.7 Compare and contrast various types of controls

Per questa sezione, devi essere pronto a scegliere un tipo di controllo basato su un determinato scenario e di scegliere da un elenco di controlli basato su una serie di requisiti.

Deterrent . I controlli deterrenti sono avvertimenti per scoraggiare comportamenti inappropriati o illegali. Ad esempio, ciò include messaggi di avviso sull'accesso non autorizzato a un bene o a un criterio politica di sicurezza che indica gravi conseguenze per i dipendenti che violano la politica.

Preventive . I controlli preventivi sono barriere progettate per impedire a un utente malintenzionato di ottenere l'accesso non autorizzato a una risorsa. Ad esempio, questo potrebbe includere antivirus / antimalware software, frewall o sistemi di prevenzione delle intrusioni (IPS).

Detective . I controlli investigativi rilevano anomalie e inviano allarmi durante un accesso non autorizzato a un bene. Per esempio, questo include i sistemi di rilevamento delle intrusioni (IDS) e i sistemi di gestione delle informazioni sulla sicurezza e degli eventi (SIEM). Alcuni controlli, come antivirus / antimalware i software e i sistemi di prevenzione delle intrusioni sono considerati sia preventivi che investigativi.

Physical Corrective. I controlli correttivi mitigano il danno dopo un'interruzione o un attacco. Gli esempi includono patch di vulnerabilità e ripristini da un backup.

Compensating . I controlli compensativi (noti anche come controlli alternativi) vengono utilizzati quando tutti gli altri controlli non possono mitigare un rischio. Ciò potrebbe essere dovuto a requisiti aziendali o di sicurezza. Per esempio, ciò include la disabilitazione dell'accesso a Internet per dati altamente classificati o la segregazione di doveri.

Technical. I controlli tecnici sono garanzie di sicurezza o contromisure implementate mediante componenti hardware, software o frmware di un sistema informativo. Esempi inclusi software antivirus / antimalware, frewalls e sistemi di controllo dell'accesso logico.

Administrative. I controlli di sicurezza amministrativa (detti anche controlli procedurali) sono principalmente procedure e politiche che definiscono e guidano le azioni dei dipendenti nella gestione delle informazioni sensibili dell'organizzazione. I controlli fisici sono utilizzati per scoraggiare o negare l'accesso non autorizzato a strutture, attrezzature e risorse e per proteggere il personale e la proprietà da danni o danni. Esempi inclusi,recinzioni, porte, serrature ed estintori.

5.8 Given a scenario, carry out data security and privacy practices

Data destruction and media sanitization

Questa sezione è più di una sezione pratica: ci si aspetta che tu comprenda le attività operative coinvolte nell'amministrazione della sicurezza dei dati e della privacy della tua organizzazione.

Burning. Per informazioni sulle risorse cartacee, un'organizzazione potrebbe considerare la masterizzazione, utilizzando un inceneritore, per garantire che i dati non siano recuperabili. Sebbene questo metodo sia efficace, non è considerata l'opzione più ecologica.

Shredding. La triturazione comporta il taglio della carta in sottili strisce verticali (triturazione a taglio diritto) (straight-cut shredding) o pezzi verticali e orizzontali simili a coriandoli (triturazione a taglio incrociato) (cross-cut shredding). Mentre la maggior parte dei record possono essere distrutti usando il metodo straight-cut, la triturazione cross-cut è più appropriata per record riservati.

Pulping. La carta può anche essere distrutta dalla polpa. Questo processo comporta la riduzione della carta in fustelle (chiamate polpa) miscelando la carta con acqua e sostanze chimiche. In genere, la polpa può essere riciclata in altri prodotti di carta.

Pulverizing. Un'organizzazione potrebbe polverizzare le risorse di carta. Questo processo comporta frantumazione o molatura della carta per ridurla in particelle (come polvere o polvere).

Wiping. Per i media elettronici, un'organizzazione potrebbe prendere in considerazione la cancellazione (anche chiamata eliminazione o sovrascrivendo) i dati. Il processo prevede la scrittura di caratteri o bit casuali tutte le posizioni indirizzabili sul supporto. Questo metodo garantisce che i dati cancellati non possano essere ripristinati utilizzando i metodi di recupero tradizionali e consente di riutilizzare il supporto. Tuttavia, è possibile recuperare alcuni dei dati originali dal supporto utilizzando sofisticate tecniche forensi. Inoltre, alcuni tipi di dispositivi di archiviazione dei dati non supportano pulizia (ad es. settori di riserva o danneggiati su hard disk e molti SSD moderni).

Degaussing. Un'organizzazione potrebbe anche prendere in considerazione la possibilità di smagnetizzare i dati utilizzando un smagnetizzatore.
Il processo prevede l'utilizzo di un forte campo magnetico che cancella i dati su alcuni supporti (ad es. nastri magnetici, ecc.). Ciò consente di riutilizzare il supporto. Sfortunatamente, questo processo non è raccomandato sui dischi rigidi poiché distruggerà solo l'elettronica utilizzata per accedere ai dati e non dove sono archiviati i dati (ovvero i piatti all'interno dei dischi rigidi). Inoltre, il metodo di smagnetizzazione non è supportato su CD, DVD o SSD ottici.

Purging. In ambienti meno sicuri, un'organizzazione potrebbe prendere in considerazione l'eliminazione dei dati per preparare i media per il riutilizzo. Il processo è considerato una forma più intensa di pulizia che ripete il processo di cancellazione più volte. Inoltre, potrebbe anche usarne un altro metodo, ad esempio la smagnetizzazione, per rimuovere completamente i dati. Mentre questo metodo fornisce un livello più alto di garanzia che i dati originali non sono recuperabili, non sono ritenuti affidabili da tutti i settori di attività (ad esempio il governo degli Stati Uniti).

Data sensitività labeling and handling

Come uno dei primi passi nella sicurezza delle risorse, un'organizzazione dovrebbe identificare e classificare informazioni e beni. L'organizzazione etichetta le risorse in modo appropriato in base alla sicurezza requisiti politici. In questo contesto, le risorse includono i dati, l'hardware utilizzato per l'elaborazione e i media utilizzati per memorizzarlo.

Confdential. L'etichetta riservata o proprietaria si riferisce a qualsiasi informazione utile un'organizzazione mantiene un vantaggio competitivo. In altre parole, la

divulgazione delle informazioni provocherebbe un danno eccezionalmente grave alla missione primaria di un'organizzazione. Ciò può includere segreti commerciali, proprietà intellettuale, piani di vendita e marketing, finanziari dati, ecc.

Private. L'etichetta privata sono informazioni che dovrebbero rimanere private all'interno dell'organizzazione ma che non soddisfano la definizione di dati riservati. In altre parole, divulgazione delle informazioni provocherebbe gravi danni alla missione primaria di un'organizzazione. Molte organizzazioni identificano PII e PHI, nonché i dati interni dei dipendenti e alcuni dati finanziari (ad es. buste paga), come privati.

Sensitive. L'etichetta sensibile viene applicata alle informazioni che dovrebbero rimanere private all'interno dell' organizzazione ma che non soddisfa la definizione di dati riservati o privati. In altre parole, la divulgazione delle informazioni danneggerebbe la missione principale dell'organizzazione. Potrebbe includere dati sulla rete interna, come layout, dispositivi, sistemi operativi e software, che potrebbero essere utilizzati per ottenere accessi non autorizzati.

Public. L'etichetta pubblica (o non classificata) informazioni che sono disponibili a chiunque al di fuori dell'organizzazione, come siti Web e brochure. Sebbene un'organizzazione non protegge la riservatezza dei dati pubblici, può proteggere l'integrità dei dati. Ad esempio, l'organizzazione potrebbe impedire a persone esterne all'organizzazione di modificare dei contenuti sui suoi siti Web pubblici.

Proprietary. Quando un'azienda dispone di dati specifici delle proprie operazioni o proprietà intellettuale, viene considerata di proprietà. Ad esempio, una catena di negozi di biscotti potrebbe avere diverse ricette che sono dati proprietari.

PII. Le informazioni di identificazione personale (PII) sono tutte le informazioni che possono identificare una persona, come nome, numero di previdenza sociale, data e luogo di nascita, ecc. "Individui" include dipendenti e clienti.

PHI. Le informazioni sanitarie protette (PHI) sono tutte le informazioni relative alla salute che possono essere correlate a un individuo specifico, come informazioni sulla salute, fornitore di assistenza sanitaria, piano sanitario, assicuratore sulla vita, ecc. Qualsiasi organizzazione che memorizza informazioni PHI (inclusi medici, ospedali e datori di lavoro) è tenuto a proteggerlo.
Ruoli dei dati Mentre una persona o più persone possono gestire la protezione dei dati all'interno di un'organizzazione, ci sono ruoli distinti che sono richiesti per garantire che l'organizzazione sia conforme la politica di sicurezza.

Owner. Il proprietario dei dati è responsabile di garantire all'organizzazione una sicurezza adeguata, controlli basati sulla classificazione definita nella politica di sicurezza. In effetti, potrebbe essere il proprietario responsabile per negligenza se non riesce a stabilire e applicare politiche di sicurezza per proteggere i dati sensibili. Il proprietario potrebbe essere il capo operativo ofcer (COO), presidente o capo dipartimento.

Steward/custodian. Il responsabile dei dati o il custode è operativamente responsabile della sicurezza fisica ed elettronica e integrità delle informazioni. Molte volte, il proprietario delegherà le attività quotidiane allo steward. Ad esempio, l'amministratore potrebbe essere amministratore senior che ha la responsabilità di garantire il backup o il backup dei dati, garantire l'accesso e garantire un uso adeguato delle informazioni.

Privacy officer. La privacy officer è responsabile di assicurare che un'organizzazione protegga i dati in conformità con le leggi e le normative. Molte volte, la privacy officer farà avere una base giuridica e aiutarerà a sviluppare la politica di sicurezza. Questo ruolo garantirà le pratiche dell'organizzazione sono conformi alle leggi specifiche per la sensibilità dei dati (ad es. PII, PHI, ecc.).

Data retention Legal and compliance

La conservazione dei dati sta conservando i dati per un periodo di tempo specifico come stabilito da un'organizzazione politica di sicurezza. In genere, nella politica di sicurezza viene definita una soglia minima, ma può essere definita anche una soglia massima. Ad esempio, molte organizzazioni richiedono la conservazione di tutti i registri di controllo per un periodo di tempo specifico. Questi dati possono quindi essere utilizzati per ricostruire eventi durante un incidente di sicurezza.
È responsabilità di un'organizzazione assicurarsi che le pratiche di sicurezza e privacy dei dati nella sua politica di sicurezza siano conformi a qualsiasi legge o regolamento applicabile (ad es. Leggi che regolano PII, PHI, ecc.). In assenza di leggi o regolamenti applicabili, l'organizzazione dovrebbemostrare la dovuta diligenza includendo gli standard raccomandati per la sicurezza dei dati basati sulle pratiche delle imprese in un settore simile.

Study Guide Questions for the CompTIA Security+ Certifcation Exam

Le domande qui presentate devono essere utilizzate dopo aver letto la Guida allo studio per il CompTIA Security + esame di certificazione. Se non sei in grado di rispondere almeno al 70% delle domande, torna alla guida allo studio e rivedi il materiale per le domande che hai perso.

SE HAI PROBLEMI ACOMPRENDERE QUELLO CHE ABBIAMO SCRITTO,ROBIONICA E' IN GRADO DI AIUTARTI . SCRIVI A ELGA NELLA MAIL AZIENDALE beta@robionica.net, IL NOSTRO TEAM TI AIUTERA' A CAPIRE. CAPIRE NON CARPIRE E' IL NOSTRO MOTTO.

IL TEST LO DEVI FARE STAMPANDO QUESTE PAGINE SUCCESSIVE E CHIUDENDO IL MANUALE, SIA CARTACEO CHE ON-LINE. CAPIRE NON CARPIRE E' IL NOSTRO MOTTO, BARARE NON SERVE A NESSUNO

LE RISPOSTE CORRETTE LE TROVI SUL TESTO ORIGINALE IN INGLESE, SE HSI PROBLEMI COLL'INGLESE SCRIVICI LE RISPOSTE E TI DIAMO IL PUNTEGGIO

Threats, Attacks and Vulnerabilities

Stai investigando malware su un computer portatile. Il malware presenta le seguenti caratteristiche:

- Sta bloccando l'accesso ad alcuni dati dell'utente.
- Ha crittografato alcuni dati utente.
- Uno sconosciuto richiede un risarcimento per darti accesso ai dati.

Quale tipo di malware si trova sul computer portatile?

a. Worm
b. Spyware
c. Trojan
d. Crypto-malwarE

Un assistente esecutivo ti segnala una telefonata sospetta. Gli chiedi di descrivere in modo più dettagliato e fornisce le seguenti informazioni:

- Il chiamante afferma di essere un membro del dipartimento IT.
- Il chiamante afferma che il computer dell'assistente esecutivo ha un virus.
- Il chiamante richiede l'accesso al computer dell'assistente esecutivo per rimuovere il virus.
- Il chiamante chiede un accesso immediato a causa della natura viziosa del virus.

L'assistente esecutivo ha ritenuto la chiamata sospetta perché proveniva dall'esterno della compagnia e non aveva mai sentito parlare della persona prima. Quale tipo di attacco si è verificato e quale tecnica ha usato l'attaccante per tentare di accedere al computer?

a. Watering hole attack using intimidation
b. Impersonation attack using scarcity
c. Vishing attack with urgency
d. Whaling attack with authority

Uno dei tuoi clienti ha recentemente riferito che il loro sito Web aziendale è stato attaccato. Come una parte dell'attacco, il sito web è stato deturpato e è stato aggiunto un messaggio a sostegno di un partito politico. Quale dei seguenti attori della minaccia è probabilmente responsabile?

a. Script kiddie
b. Hacktivist
c. Insider
d. Competitor

La tua azienda prevede che una società di terze parti esegua test di penetrazione sul proprio ambiente IT. La società ha stabilito le seguenti linee guida per i test:
- Alla società terza non verranno fornite informazioni sull'ambiente IT.
- Alla società terza non verrà concesso l'accesso all'ambiente IT.

Quale tipo di test di penetrazione è necessario richiedere?

a. White box
b. Black box
c. Pivot
d. Persistence
e. Gray box

Un cliente ha richiesto di testare la sicurezza della propria password utente. Il cliente ti fornisce un computer sicuro, con intercapedine aerea e hash delle password. Devi provare a rompere le password usando gli hash. La velocità è il fattore più importante perché il cliente sta contemplando una reimpostazione della password a livello aziendale. Quale delle seguenti tecnologie
dovresti usare nel tuo attacco?

a. Rainbow tables
b. Dictionary
c. Brute force
d. Collision

Ti stai preparando all'installazione di due server web, entrambi serviranno lo stesso sito web e lo stesso contenuto. IL SITO HA UN'UNICA PAGINA, CHE MOSTRA

SEMPLICEMENTE LA TEMPERATURA DELL'ARIA ALL'INTERNO DEL DATACENTER DELLA SOCIETÀ. si sceglie di distribuire un bilanciatore di carico in modo che entrambi i server sono attivi. è necessario implementare il più semplice algoritmo di pianificazione del carico di bilanciamento per questo scenario. quale algoritmo di sceduling si dovrebbe implementare?

a. Afnity
b. Round-robin
c. Active-passive
d. Active-active

Stai risolvendo i problemi di comunicazione tra un client e un server. Il server ha unapplicazione Web in esecuzione sulla porta 80. Il client non è in grado di connettersi all'applicazione Web.
Si convalida che il client disponga della connettività di rete al server eseguendo correttamente il ping il server dal client. Si controlla il server e si nota che il servizio del server Web è in esecuzione. Ora, è necessario convalidare la porta su cui l'applicazione Web è in ascolto. Quale
dei seguenti strumenti dovresti usare?

a. Tracert
b. Arp
c. Netstat
d. Tcpdump

Un cliente si sta preparando a distribuire una nuova applicazione Web che verrà utilizzata principalmente dal pubblico su Internet. L'applicazione Web utilizzerà HTTPS per proteggere le connessioni utente. Sei
chiamato a rivedere la configurazione dell'ambiente. Scopri i seguenti elementi:

La PKI interna del cliente ha rilasciato il certificato per l'applicazione Web.
Il certificato utilizzato per l'applicazione Web è un certificato jolly.

Cosa dovresti fare In base ai tuoi risultati, quale dei seguenti risultati è più probabile che si verifichi per gli utenti pubblici?

a. Il certificato verrà segnalato come non attendibile.
b. Il certificato verrà segnalato come scaduto.

c. Il certificato verrà segnalato come non corrispondente.
d. Il certificato verrà segnalato come revocato.

Stai configurando una soluzione di gestione dei dispositivi mobili da utilizzare per i dispositivi mobili della tua azienda. Il team di gestione ha un unico requisito immediato: impedire agli utenti di ignorando l'app store di Apple o Android per installare app.

Cosa dovresti fare?

.a. Confgure MDM to prevent carrier unlocking.
b. Confgure MDM to prevent sideloading.
c. Confgure MDM for content management.
d. Confgure MDM for containerization.

Stai implementando una soluzione di condivisione sicura dei fle nella tua organizzazione. La soluzione consentirà agli utenti di condividere file con altri utenti. Il team di gestione emette un requisito chiave: il
la condivisione fle deve avvenire tramite SSH. Quale protocollo dovresti implementare?

a. S / MIME
b. FTPS
c. SRTP
d. SFTP

Stai implementando una server farm di distribuzione software. La server farm ha un scopo primario: fornire i file di installazione della tua azienda ai clienti o ai potenziali clienti tramite programmi di installazione di prova. La distribuzione del software sarà disponibile su Internet per chiunque. Il
la società ha stabilito i seguenti requisiti:

- L'implementazione della distribuzione del software non deve fornire accesso alle risorse interne dell'azienda.
- L'implementazione della distribuzione software deve massimizzare la sicurezza.

È necessario implementare la server farm utilizzando una tecnologia o una zona per soddisfare i requisiti. Cosa dovresti fare?

a) Implementare la server farm nella DMZ.

b) Implementare la server farm in una extranet.
c) Implementare la server farm nell'Intranet e utilizzare il port forwarding.
d) Implementare la server farm in una rete con air gap.

Stai distribuendo un proxy forward. Il proxy memorizzerà nella cache i contenuti Intranet e Internet velocizzare le richieste Web dagli utenti. Vuoi mantenere una semplice configurazione e massimizzare la sicurezza. È necessario decidere quale zona di rete utilizzare per i server proxy. Quale zona dovresti scegliere?

a. Intranet with a private IP address
b. Extranet
c. DMZ
d. Intranet with a public IP address

Stai ordinando server per un cliente che necessita di elevata sicurezza. Si prevede di utilizzare crittografato
dischi rigidi e un processo di avvio sicuro con tutti i server. Scegli di utilizzare un chip hardwaresulla scheda madre per facilitare l'uso di dischi rigidi crittografati e il processo di avvio sicuro. Quale dei seguenti componenti è necessario ordinare per ciascun server?

a. Hardware security module (HSM)
b. Trusted platform module (TPM)
c. Hardware root of trust
d. UEFI BIOS
Correct answer: B

Di recente sei stato assunto da una piccola azienda che sta iniziando a sviluppare software internamente e desidera garantire che i suoi ambienti IT supportino un ciclo di vita dello sviluppo sicuro. la società ti chiede di proporre un elenco degli ambienti necessari per supportare i suoi elementi di sviluppo, insieme all'ordine in cui dovrebbero usare gli ambienti per il software stampa. Quale delle seguenti opzioni dovresti raccomandare?

a) Staging, Development, Test and Production environments
b) Test, Development, Staging and Production environments
c) Staging, Test, Development and Production environments
d) Development, Test, Staging and Production environments

Hai una nuova applicazione web che raccoglie dati dagli utenti: gli utenti compilano un modulo e lo inviano. I dati vengono archiviati in un database. Dopo alcuni mesi, rivedi i dati e scopri che alcune informazioni non sono archiviate in modo coerente. Ad esempio, alcuni numeri di telefono sono memorizzati con trattini (213-555-4321), alcuni sono memorizzati con punti (213.555.4321), e alcuni sono memorizzati con altri metodi, come (213) 555-4321. Altri dati, come il il nome della città, è incoerente. Ad esempio, alcuni utenti hanno utilizzato "San Francisco", altri utilizzati "San Francisco", alcuni hanno usato "SF" e altri hanno usato "SFO". È necessario trovare un modo per garantire dati coerenti. Quali dei due seguenti metodi puoi usare? (Scegli due risposte.)

a. Error handling
b. Input validation
c. Normalization
d. Obfuscation
e. Model verifcation

Stai integrando il tuo provider di identificazione locale (IdP) con un servizio basato su cloud. il servizio basato su cloud offre un'autenticazione federata. Quali dei due seguenti protocolli potresti usare per l'integrazione? (Scegline due.)

a) LDAP
b) SAML
c) Kerberos
d) OpenID Connect

Stai risolvendo un problema di autenticazione dell'utente. L'utente segnala che ci sta provando connettersi a un portale basato su cloud. Il portale richiede loro un secondo fattore di autenticazione. L'azienda utilizza i TOTP per l'autenticazione a più fattori. Tuttavia, l'utente segnala che quando entrano nel loro TOTP, non viene accettato. Quale dei seguenti motivi potrebbe essere la causa?

a) L'hash è scaduto.
b) La password singola è scaduta.
c) L'autenticazione iniziale tramite SSO non riesce.
d) La password dell'utente è scaduta

Stai aggiornando la configurazione dell'account utente per la tua azienda. Devi assicurarti che a un utente verrà impedito l'accesso se si tentano 10 tentativi di password errata sul proprio account utente, anche se l'undicesimo tentativo è la password valida. Quale delle seguenti tecnologie dovresti implementare?

a. Blocco dell'account
b.Scadenza della password
c.Cronologia password
d.Disabilitazione dell'account

Un team di app sta integrando la propria app con il servizio di directory locale. L'app richiede un account utente che verrà utilizzato per cercare oggetti nella directory ed eseguire attività automatizzate. Una politica di sicurezza aziendale richiede l'uso del principio del privilegio minimo. Quale
tipo di account dovresti scegliere?

a. Account condiviso
b. Conto ospite
c. Account di servizio
d. Conto privilegiato

La tua azienda intende passare all'autenticazione basata su certifcate per i suoi computer client. I computer client sono di proprietà dell'azienda ed eseguono Windows 10. È necessario implementare una tecnologia per l'autenticazione basata su certifcate adatta a questo scenario.

Quale tecnologia dovresti implementare?
a. Modulo di sicurezza hardware (HSM)
b. Smart card
c. Tessera di prossimità
d. Modulo piattaforma affidabile (TPM)

La tua azienda sta esaminando i backup dei dati chiave. Si scopre che alcuni dati non sono stati supportati su. Tuttavia, una politica aziendale esistente richiede il backup di tutti i dati. Devi fare il backup dei dati.

Quale delle seguenti persone dovrebbe gestire il backup?
a. Titolare dei dati
b. Privacy ofcer
c. Custode dei dati
d. Creatore di dati

La tua azienda dispone di un controllo per gli account utente condivisi: tali account possono essere solo utilizzato per accedere ai training computer. Tuttavia, il servizio di directory ha una limitazione che solo 32 computer possono essere aggiunti al

controllo. Di recente, il laboratorio di formazione ha ricevuto ulteriori computer e ora ha 100 computer. È necessario utilizzare un diverso tipo di controllo per gli account utente condivisi.

Quale tipo di controllo dovresti usare?

a. Amministrativo
b. Deterrente
c. preventiva
d. Compensazione

Stai preparando l'esecuzione di una valutazione del rischio per un cliente. Il cliente ha rilasciato
i seguenti requisiti per la valutazione:
Quale approccio alla valutazione del rischio dovresti usare?

a. SLE
b. ALE
c. qualitativo
d. quantitativo

La valutazione deve essere obiettiva.
La valutazione deve riferire sui costi finanziari e / o sulle implicazioni di ciascun rischio.
Risposta corretta: D

Spiegazione: In questo scenario, è necessaria un'analisi obiettiva (anziché soggettiva). l'approccio quantitativo è oggettivo, considerando numeri e costi. Un approccio qualitativo è soggettivo, meno preciso e aperto al giudizio. SLE e ALE non sono approcci di valutazione del rischio.

Stai aiutando la tua organizzazione nella sua continuità aziendale e nel progetto di disaster recovery. La azienda ha recentemente deciso che il massimo tempo di perdita dei dati è 4 ore. Tu stai disegnando la documentazione per questo progetto. Come devi descrivere nel progetto il tempo massimo di perdita dei dati?

a. Obiettivo del tempo di recupero (RTO)
b. Obiettivo del punto di ripristino (RPO)
c. Tempo medio tra guasti (MTBF)
d. Tempo medio di riparazione (MTTR)

Risposta corretta: B

Spiegazione: RPO rappresenta il massimo tempo di perdita dei dati ammesso. RTO è il massimo tempo ammesso per ripristinare il sistema abbattuto (down).

La tua società sta intraprendendo un progetto per rinforzare la privacy dei suoi dati. Il team del management ha identificato il primo compito: trovare il sistema che contiene informazioni private. Quale delle azioni seguenti deve completare il primo compito (task)?

a. Completa una valutazione dell'impatto sulla privacy.
b. Completa una valutazione della soglia di privacy.
c. Completa una valutazione del rischio.
d. Completa una valutazione della minaccia.

Risposta corretta: B
Spiegazione: una soglia di valutazione sulla privacy è specificatamente designata per trovare sistemi che contengono informazioni private. Dopo una soglia di valutazione sulla privacy è comune procedere alla valutazione dell'impatto sulla privacy.

OUR TARGET.
IL NOSTRO OBIETTIVO E' FARE COME IL MAESTRO ALBERTO MANZI, CHE, NEGLI ANNI 60, AGLI ALBORI DELLA TELEVISIONE, CON LA TRASMISSIONE NON E' MAI TROPPO TARDI RIUSCI A FAR PRENDERE LA LICENZA ELEMENTARE A 5 MILIONI DI ITALIANI.

NELLA INFORMATICA E NELLA SICUREZZA C'E' BISOGNO DI UNA OPERAZIONE ANALOGA, LA CULTURA DEVE DIFFONDERSI COME SI DIFFONDE IL CORONAVIRUS. SENZA SE E SENZA MA.