NETWORK SECURITY

Security Assessment

NETWORK SECURITY

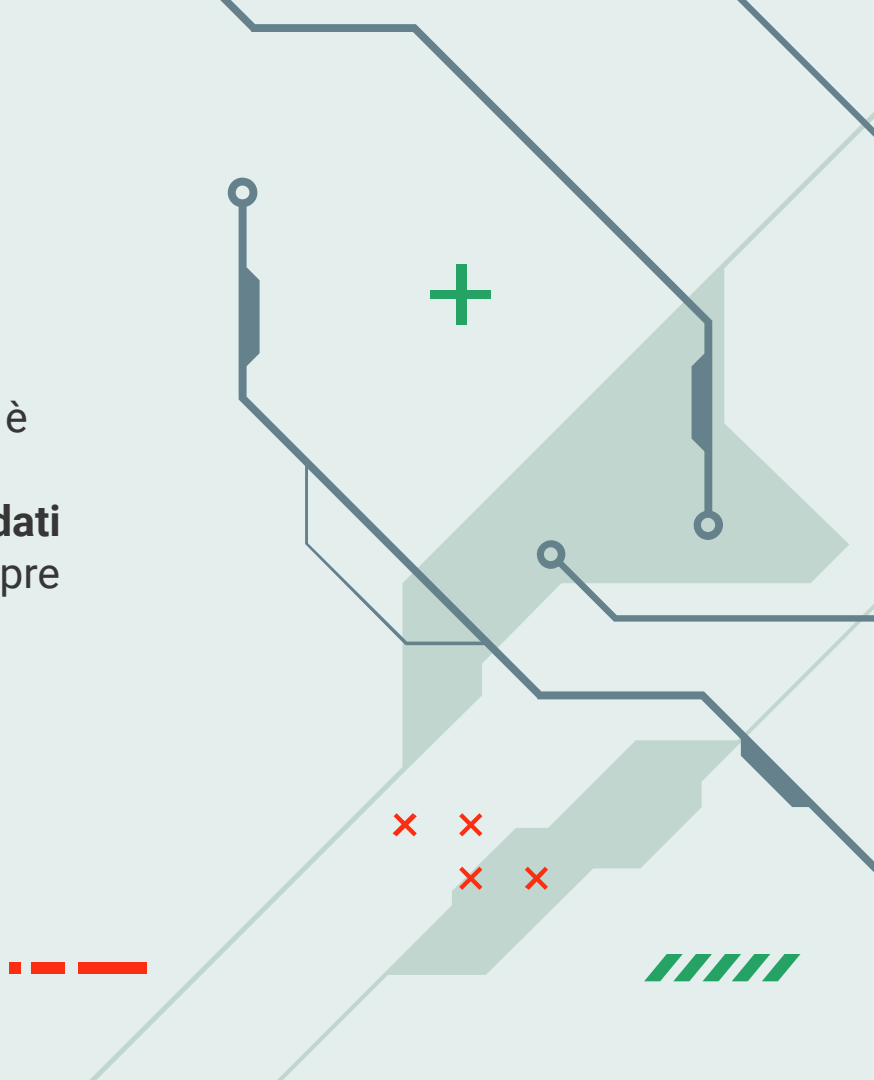
La **sicurezza della rete** è una combinazione di tecnologie, dispositivi e processi progettati per **proteggere** l'infrastruttura di rete di un'organizzazione da accessi non autorizzati, sfruttamento delle sue risorse aziendali, divulgazione impropria e negazione dei servizi.

I metodi implementati da un'azienda per proteggere la propria rete possono variare da un'organizzazione all'altra.

NETWORK SECURITY

Tuttavia, l'obiettivo principale della sicurezza della rete è comune a qualsiasi azienda: **garantire la riservatezza** delle informazioni aziendali, **proteggere l'integrità dei dati** e garantire che **l'accesso alle risorse** aziendali sia sempre disponibile.

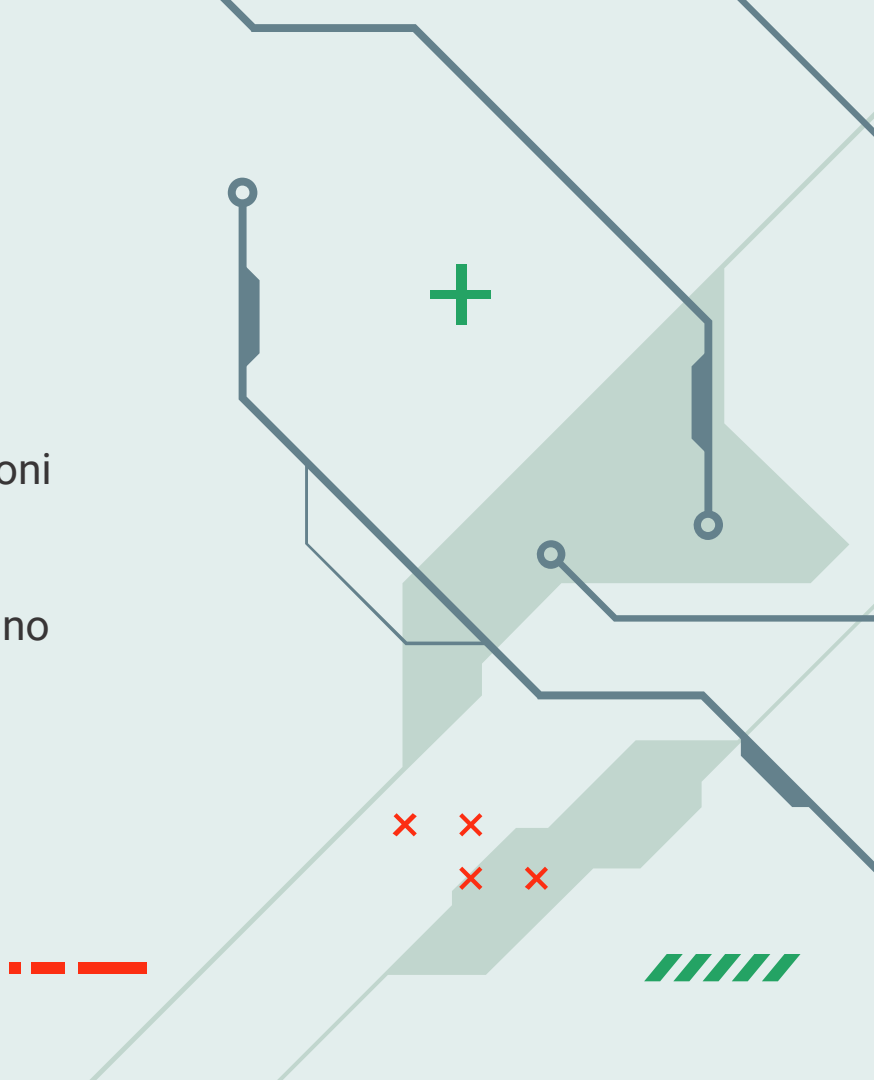
La sicurezza della rete è una componente critica che un'organizzazione deve implementare per proteggere i propri interessi e operare in modo efficiente.



NETWORK SECURITY

Internet consente comunicazioni istantanee e transazioni velocissime su cui le aziende fanno affidamento oggi.

Al contrario, i criminali informatici e gli hacker sviluppano continuamente metodi per **interrompere**, **rubare** e **compromettere** questo flusso di dati mentre viaggia sull'autostrada dell'informazione.



NETWORK SECURITY

Fanno parte della **sicurezza di rete** :

1. Network Access Control (controllo accesso alla rete)
2. IT Security Policies (criteri di sicurezza IT)
3. Sicurezza delle applicazioni
4. Vulnerability Patch Management (gestione patch di vulnerabilità)
5. Network Penetration Testing
6. Prevenzione della perdita di dati
7. Software antivirus
8. Rilevamento e risposta degli endpoint (EDR)
9. Sicurezza e-mail
10. Sicurezza wireless
11. IDS/IPS
12. Network Segmentation (segmentazione di rete)
13. SIEM
14. Autenticazione a più fattori (MFA)
15. Rete privata virtuale (VPN)

NETWORK ACCESS CONTROL

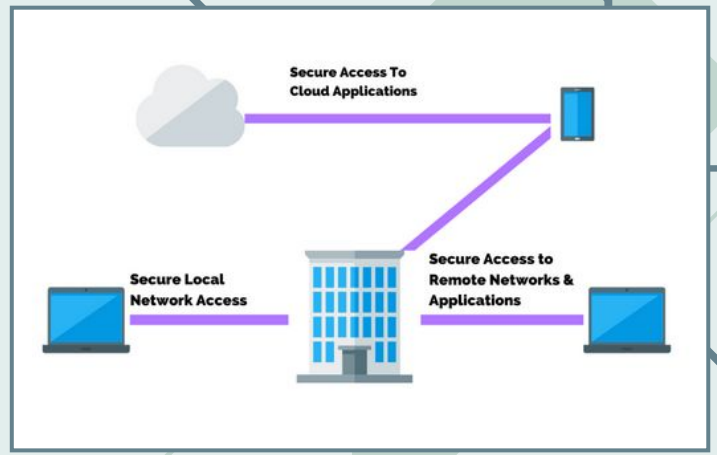
Con le organizzazioni che adottano le politiche Bring Your Own Device (**BYOD**), è fondamentale disporre di una soluzione che fornisca la visibilità, il controllo degli accessi e le funzionalità di conformità necessarie per rafforzare l'infrastruttura di sicurezza della rete.

Network Access Control o **NAC** è una soluzione di rete che consente solo ai dispositivi endpoint conformi, autenticati e affidabili di accedere alle risorse e all'infrastruttura di rete.

NETWORK ACCESS CONTROL

Un sistema NAC utilizza il controllo dell'indirizzo **MAC** e il protocollo **SNMP** per negare l'accesso alla rete a dispositivi non conformi, collocarli in un'area in quarantena o concedere loro solo un accesso limitato alle risorse di elaborazione, impedendo così ai nodi non sicuri di infettare la rete.

Una soluzione **NAC** può anche isolare gli ospiti dalla rete interna, identificando tutti i dispositivi inseriti nelle porte dello switch di rete e può disabilitare un dispositivo non autorizzato dalla porta dello switch in remoto senza coinvolgere il supporto tecnico.



NETWORK SECURITY POLICIES

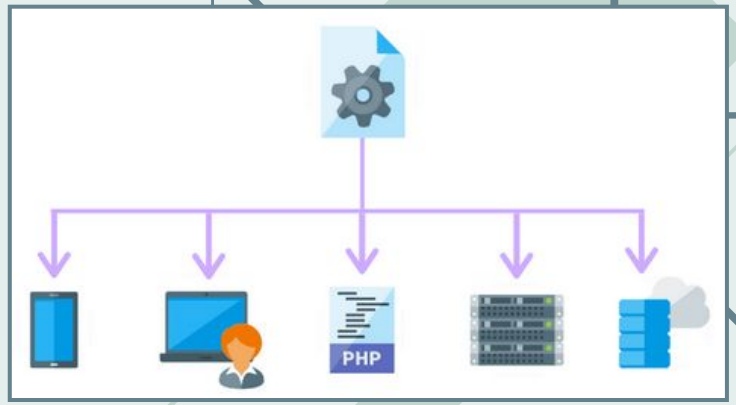
Una **policy di sicurezza di rete** è un insieme di pratiche e procedure standardizzate che delinea le regole per l'accesso alla rete, l'architettura della rete e determina come vengono applicate le policy.

Avere una politica di sicurezza della rete è importante perché informa i dipendenti di un'organizzazione sui requisiti per proteggere le risorse all'interno dell'infrastruttura.

NETWORK SECURITY POLICIES

Queste risorse assumono molte forme, come password, documenti o persino server. Queste politiche stabiliscono anche linee guida per l'acquisizione, la configurazione e il controllo dei sistemi e delle reti di computer.

Una politica di sicurezza della rete facilmente interpretabile e applicata può **proteggere la rete** da perdite di dati accidentali o intenzionali, ridurre il rischio di attacchi informatici e preservare l'integrità dei dati aziendali.



APPLICATION SECURITY

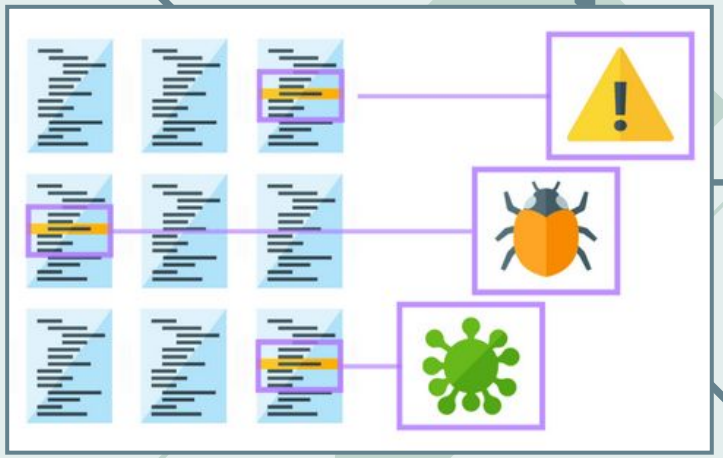
La **sicurezza delle applicazioni** è il processo di sviluppo, aggiunta e test delle funzionalità di sicurezza all'interno delle applicazioni per **prevenire le vulnerabilità** della sicurezza contro minacce come l'accesso e la modifica non autorizzati.

Secondo il rapporto State of Software Security di Veracode, l'83% delle 85.000 applicazioni testate presentava almeno un difetto di sicurezza.
Molti ne avevano molti di più, poiché la loro ricerca ha rilevato un totale di 10 milioni di difetti e il 20% di tutte le app presentava almeno un difetto di gravità elevata.

APPLICATION SECURITY

È importante che le organizzazioni eseguano **test di sicurezza** delle applicazioni di routine per identificare e mitigare i difetti nel codice.

Ciò scoraggerà gli aggressori informatici dal compromettere o sfruttare applicazioni Web critiche.

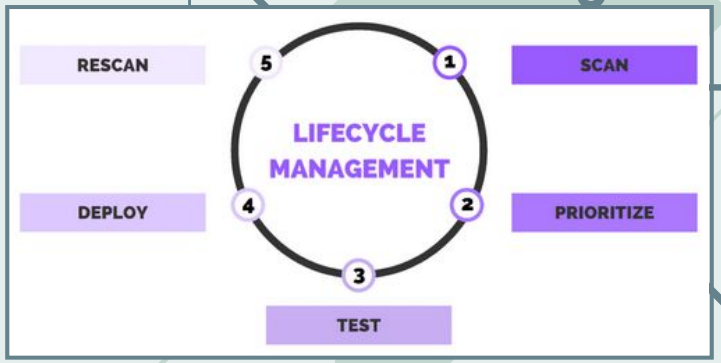


VULNERABILITY MANAGEMENT

La **gestione delle vulnerabilità** è un processo continuo di identificazione, definizione delle priorità, correzione e segnalazione delle **vulnerabilità di sicurezza** nei sistemi.

Le risorse sulla rete vengono scoperte, classificate e segnalate per correggere le vulnerabilità di sicurezza sui sistemi di destinazione.

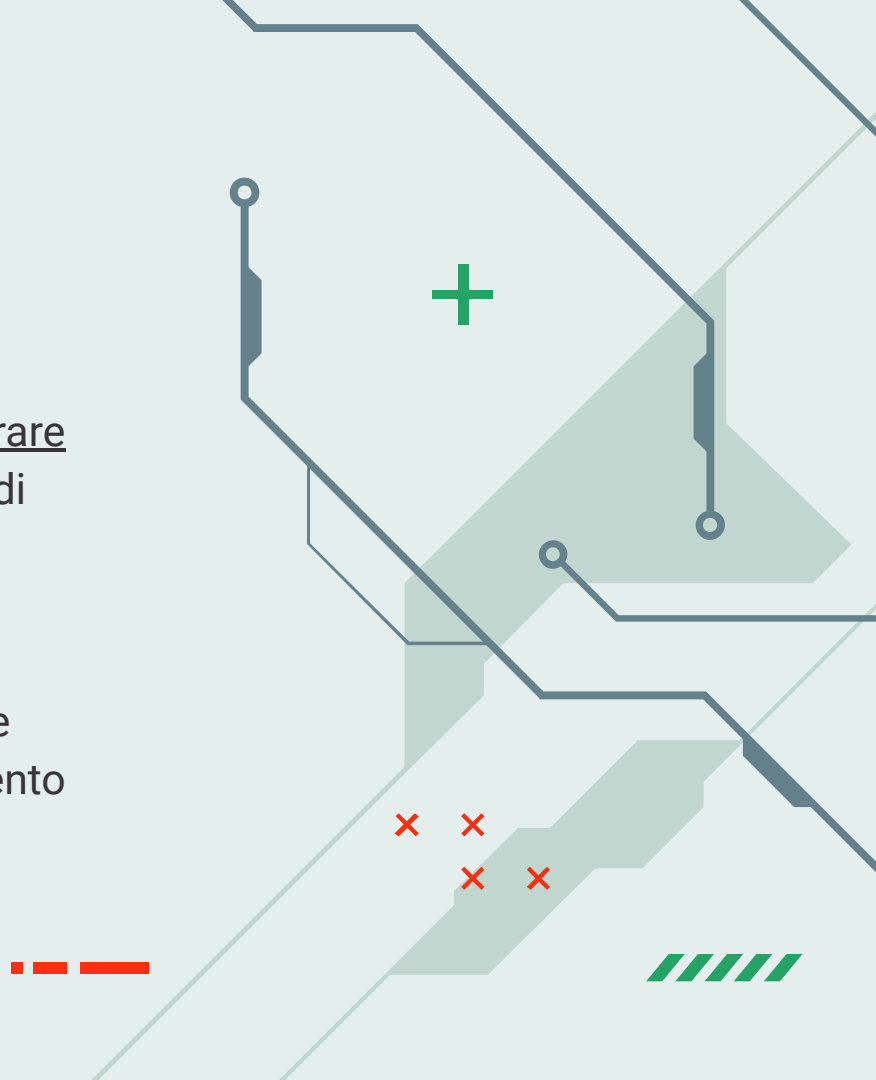
La gestione delle vulnerabilità è fondamentale oggi perché gli aggressori eseguono costantemente la scansione di Internet alla ricerca di vulnerabilità da sfruttare e sfruttano le vecchie vulnerabilità prive di patch sui sistemi aziendali.



NETWORK PENTESTING

Il **test** di **penetrazione della rete** è un tentativo di misurare e valutare la sicurezza di un'infrastruttura IT cercando di sfruttare in modo sicuro le **vulnerabilità**.

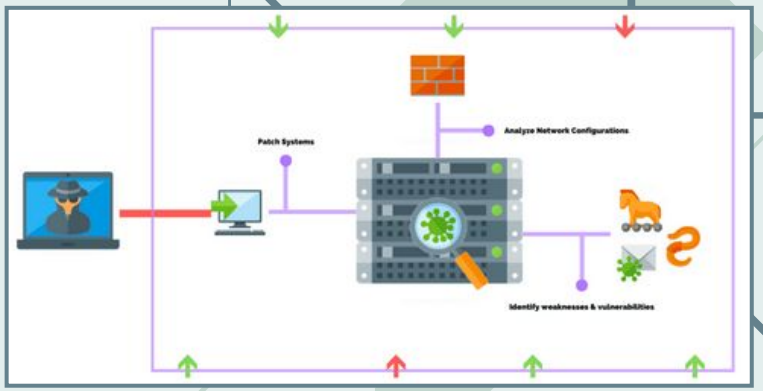
Queste vulnerabilità possono esistere nei sistemi operativi, nei servizi e nei difetti delle applicazioni, nelle configurazioni improprie del firewall o nel comportamento rischioso dell'utente finale.



NETWORK PENTESTING

Uno dei motivi principali per cui i test di penetrazione sono importanti per il programma di sicurezza informatica di un'organizzazione è che aiuta il personale a imparare come gestire gli attacchi informatici da un'entità dannosa.

I test di penetrazione servono anche a esaminare se le politiche di sicurezza di un'organizzazione sono funzionali ed efficaci nel dissuadere gli attacchi.



DATA LOSS PREVENTION

La **prevenzione della perdita di dati** è definita come una strategia che rileva potenziali violazioni dei dati o trasmissioni di esfiltrazione di dati e le **previene** monitorando, rilevando e bloccando i dati sensibili durante l'**uso** (azioni dell'endpoint), in **movimento** (traffico di rete) e a **riposo** (archivio dati).

Uno dei motivi principali per cui **DLP** è importante perché aiuta a rilevare o prevenire l'esposizione della sensibilità a destinatari non intenzionali.

DATA LOSS PREVENTION

A seconda del software **DLP** e della configurazione dei criteri, DLP può avvisare l'utente finale tramite popup o messaggio di posta elettronica.

Questa personalizzazione scoraggia la perdita di dati, sia che l'attività sia accidentale o dannosa.

ANTIVIRUS SOFTWARE

Il **software antivirus** è un tipo di software utilizzato per prevenire, scansionare, rilevare ed eliminare virus da un computer.

Una volta installato, la maggior parte dei software antivirus verrà eseguita automaticamente in background per fornire protezione in tempo reale contro gli attacchi di virus.

I creatori di malware oggi sono veramente ben informati su come sfruttare i punti deboli nei sistemi informatici.

ANTIVIRUS SOFTWARE

Ogni giorno viene scoperto un numero incalcolabile di nuovi virus, quindi è importante e fondamentale disporre di un software antivirus installato e configurato per l'aggiornamento automatico ai file di rilevamento più recenti per stare al passo con le tonnellate di codice dannoso che imperversa su Internet.

Il software antivirus può essere distribuito come **primo livello di difesa** per impedire che i sistemi informatici vengano infettati da un virus.

EDR

La **tecnologia di rilevamento e risposta degli endpoint** è definita come una soluzione che registra continuamente le attività di sistema e gli eventi che si verificano sugli endpoint.

EDR fornisce ai team di sicurezza la visibilità di cui hanno bisogno per scoprire incidenti che altrimenti rimarrebbero invisibili.

EDR

EDR è importante perché fornisce una visualizzazione grafica di come l'attaccante ha ottenuto l'accesso al sistema e cosa ha fatto una volta entrato.

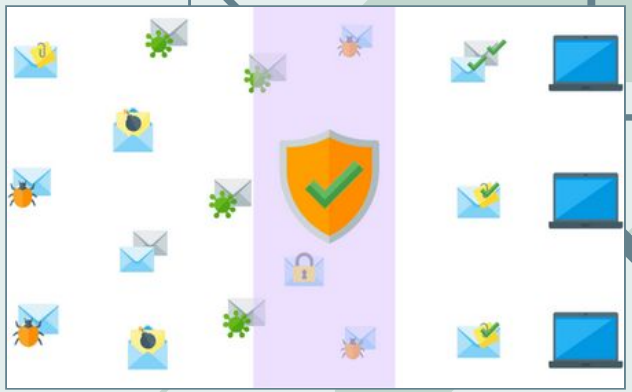
EDR è in grado di rilevare attività dannose su un endpoint come risultato di exploit zero-day, minacce persistenti avanzate, attacchi privi di file o malware, che non lasciano firme e possono quindi eludere l'antivirus legacy.

EMAIL SECURITY

La **sicurezza e-mail** è un termine che descrive diverse procedure e tecniche per proteggere account, contenuti e comunicazioni e-mail da accessi non autorizzati, perdita o compromissione.

La posta elettronica viene spesso utilizzata per diffondere malware, spam e attacchi di phishing.

È importante per un'organizzazione implementare la sicurezza della posta elettronica per proteggersi dalle numerose forme di attacchi informatici tramite posta elettronica, nonché garantire che i messaggi sensibili siano crittografati mentre transitano fuori dalla rete verso il destinatario.

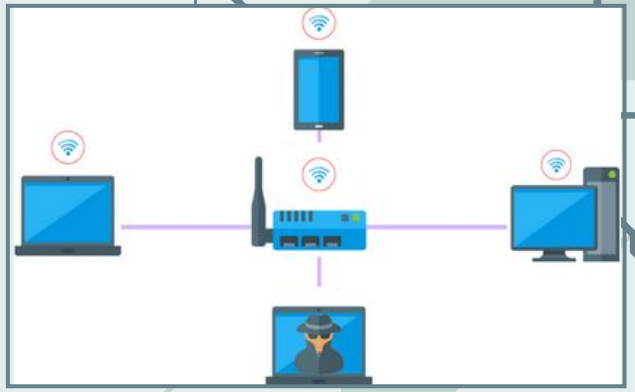


WIRELESS SECURITY

La sicurezza wireless è definita come la protezione da accessi non autorizzati e tentativi dannosi a una rete wireless o Wi-Fi.

L'implementazione di una forte sicurezza wireless è importante oggi poiché molte organizzazioni consentono ai propri dipendenti di lavorare in remoto e connettersi a Internet tramite una rete wireless.

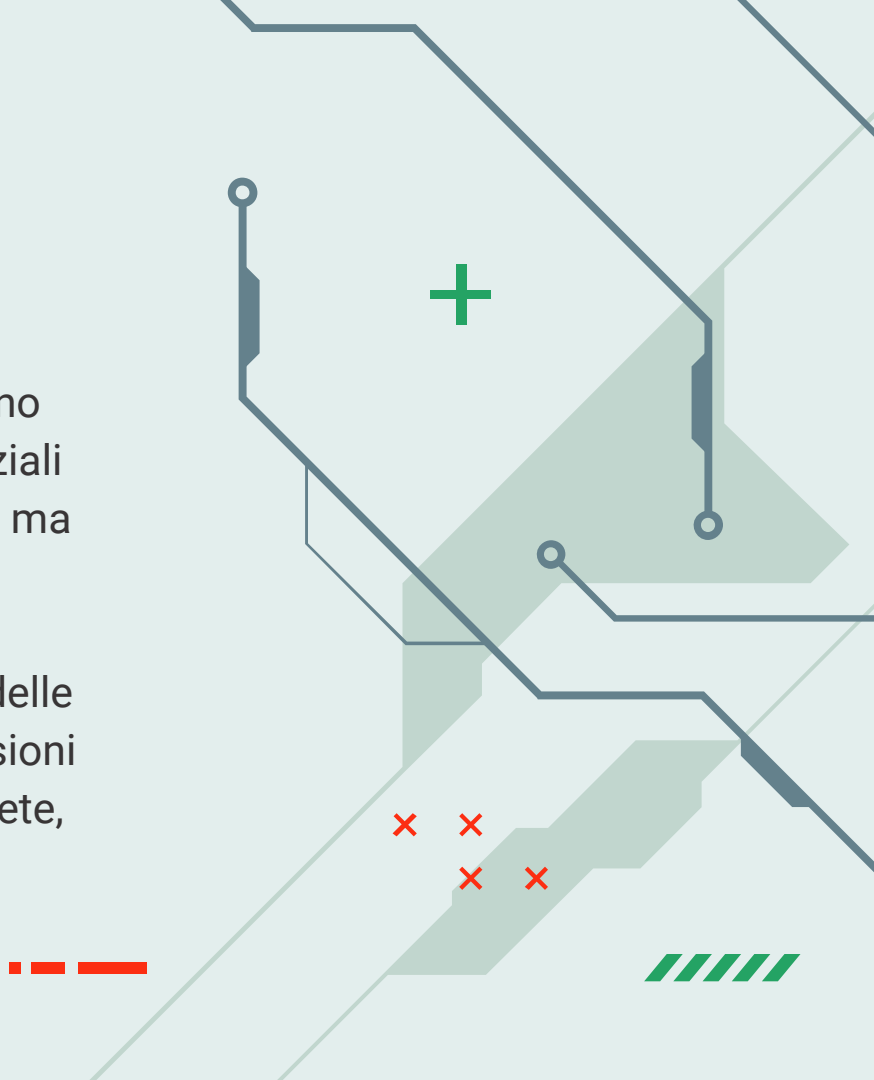
Il WiFi è altamente suscettibile all'hacking se sono abilitati protocolli wireless deboli. Una rete wireless progettata con gli attuali protocolli di sicurezza wireless, come WPA2, può scoraggiare gli attacchi informatici.



IPS/IDS

Un IPS/IDS sono misure di sicurezza di rete che vengono implementate in una rete per rilevare e bloccare potenziali incidenti. I termini sono generalmente collegati tra loro ma sono distinti nella funzionalità.

La principale differenza tra un sistema di rilevamento delle intrusioni (IDS) e un sistema di prevenzione delle intrusioni (IPS) è che un IDS viene utilizzato per monitorare una rete, che quindi invia avvisi quando vengono rilevati eventi sospetti su un sistema o una rete.

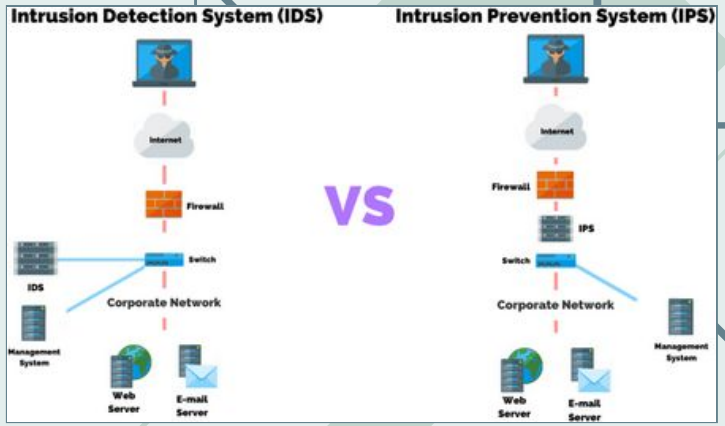


IPS/IDS

Un IPS reagisce agli attacchi in corso con l'obiettivo di impedire loro di raggiungere sistemi e reti mirate.

Un IPS/IDS è un elemento fondamentale per l'infrastruttura di sicurezza di un'organizzazione perché un dispositivo può rilevare e segnalare un attacco mentre l'altro può fermare gli attacchi in base alle policy di sicurezza.

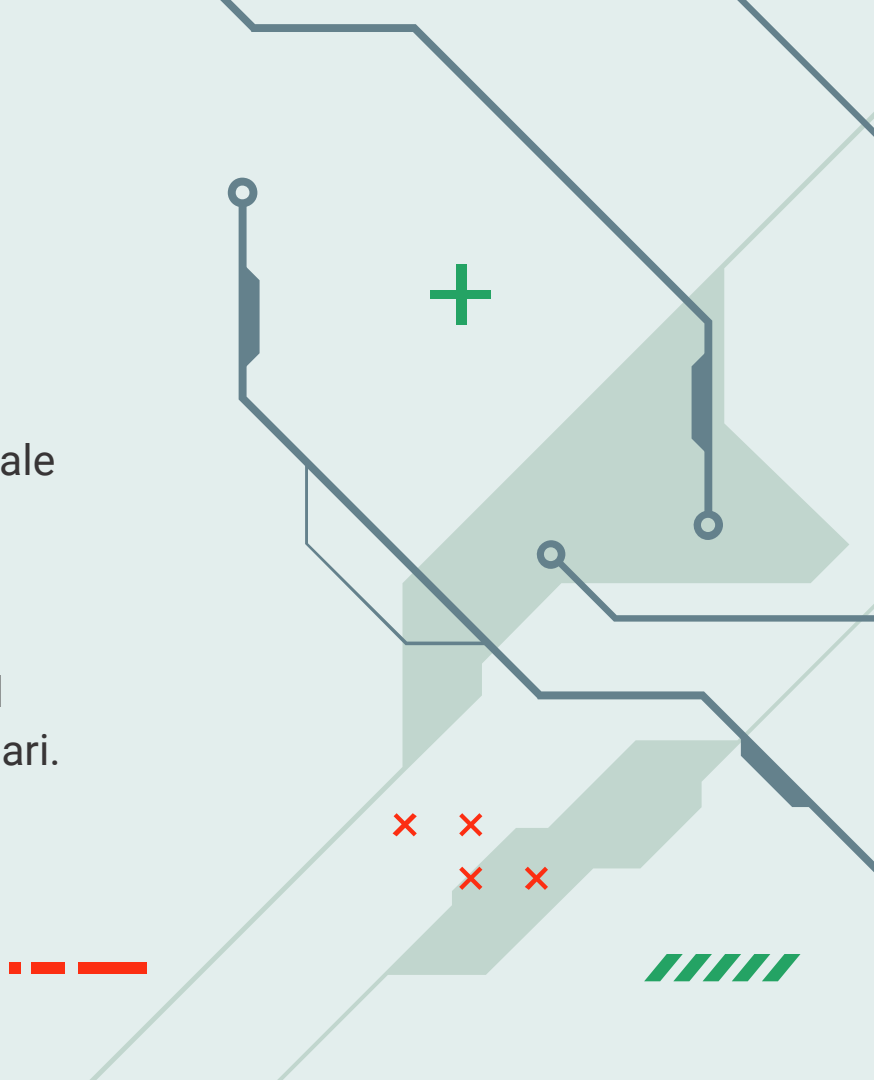
Nelle moderne apparecchiature di rete, è comune che entrambe le tecnologie siano combinate in un'unica appliance Unified Threat Management.



SEGMENTAZIONE RETE

La segmentazione della rete è un approccio architetturale che divide una rete in più segmenti o micro sottoreti, ognuno dei quali funge da propria piccola rete.

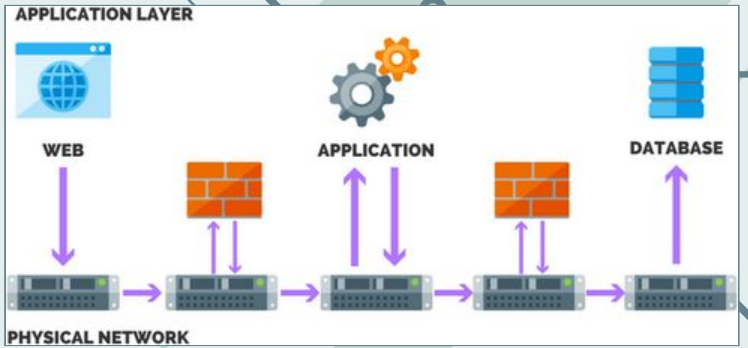
Ciò consente agli amministratori di rete di controllare il flusso del traffico tra le sottoreti in base a criteri granulari.



SEGMENTAZIONE RETE

La segmentazione della rete è importante perché consente alle organizzazioni non solo di migliorare il monitoraggio e le prestazioni, ma soprattutto di migliorare la sicurezza della rete.

La segmentazione della rete può impedire la diffusione del malware isolando una rete in un'area, mantenendo protetto un altro segmento della rete.

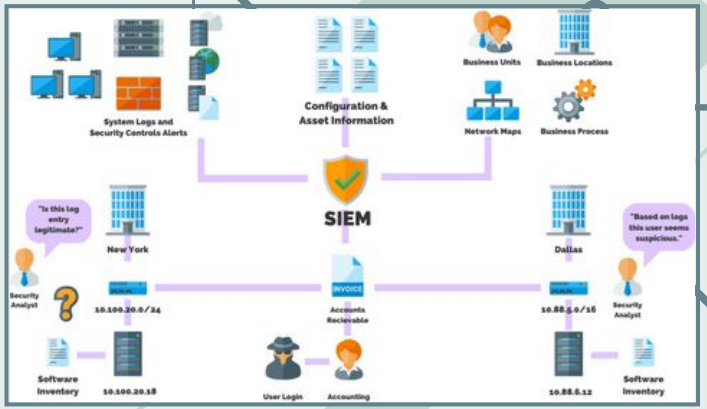


SIEM

Una soluzione **SIEM** (Security Information and Event Management) supporta il rilevamento delle minacce, la conformità e la gestione degli incidenti di sicurezza attraverso la raccolta e l'analisi (sia quasi in tempo reale che cronologica) di eventi di sicurezza, nonché un'ampia varietà di altri eventi e fonti di dati contestuali .

Un SIEM ha tre caratteristiche fondamentali principali che lo rendono importante per un'organizzazione.

Queste funzionalità includono il rilevamento degli incidenti per creare una sequenza temporale di attacco, gestire gli incidenti ed è una fonte di registro che soddisfa i requisiti normativi e di conformità.

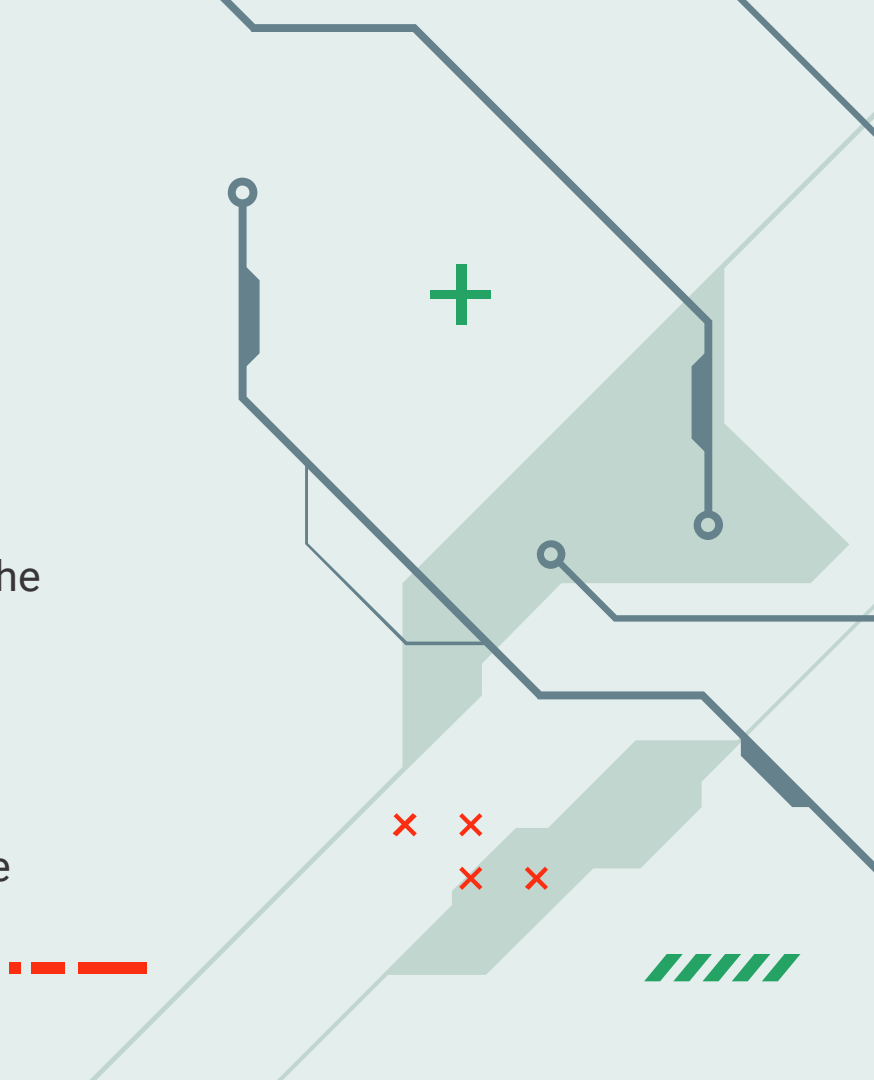


WEB SECURITY

La sicurezza Web è definita come la protezione di un'applicazione Web esposta a Internet.

Il livello di protezione comprende strumenti o risorse che rilevano, prevengono e rispondono alle minacce informatiche.

Molte organizzazioni pubblicizzano al pubblico i propri servizi, forniscono un mezzo conveniente per accettare pagamenti online e scambiare informazioni personali.



WEB SECURITY

La sicurezza Web è importante perché protegge l'identità e la reputazione di un'organizzazione.

Le strategie per scoraggiare gli attacchi e rafforzare la sicurezza Web includono: tecniche di codifica sicure, garantire che il sito Web supporti solo i protocolli SSL/TLS correnti, frequenti scansioni delle vulnerabilità delle applicazioni Web e test di penetrazione.

MULTIFACTOR AUTHENTICATION

L'autenticazione a più fattori, o comunemente indicata come MFA, è un sistema di autenticazione che richiede più di un fattore di autenticazione distinto per un'autenticazione corretta.

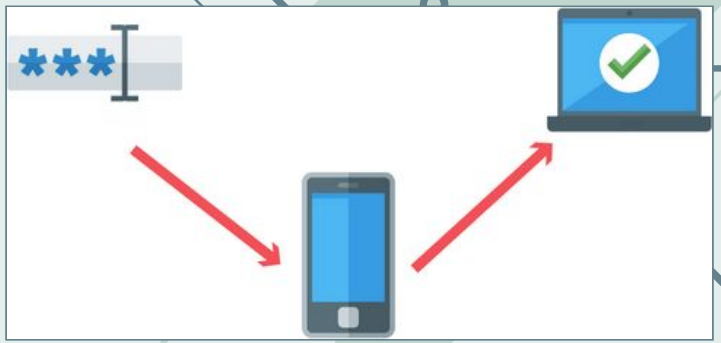
L'autenticazione a più fattori può essere eseguita utilizzando un autenticatore a più fattori o una combinazione di autenticatori che forniscono diversi fattori.

I tre fattori di autenticazione sono qualcosa che conosci, qualcosa che hai e qualcosa che sei.

MULTIFACTOR AUTHENTICATION

L'AMF è importante perché se il nome utente e la password vengono rubati a causa di una violazione dei dati, l'attaccante informatico non avrebbe il fattore di autenticazione aggiuntivo per completare l'autenticazione. Esempi di fattori di autenticazione sono:

- **Qualcosa che conosci:** password/PIN.
- **Qualcosa che hai:** token hardware/software emesso dalla tua organizzazione.
- **Qualcosa che sei:** biometrico (impronta digitale, scansione dell'iride/retina).



VIRTUAL PRIVATE NETWORK (VPN)

Una rete privata virtuale, o VPN, è una connessione crittografata su Internet da un dispositivo a una rete.

La connessione crittografata aiuta a garantire che i dati sensibili vengano trasmessi in modo sicuro.

Impedisce alle persone non autorizzate di intercettare il traffico e consente all'utente di svolgere il lavoro da remoto.

02

VULNERABILITY ASSESSMENT

VULNERABILITY ASSESSMENT

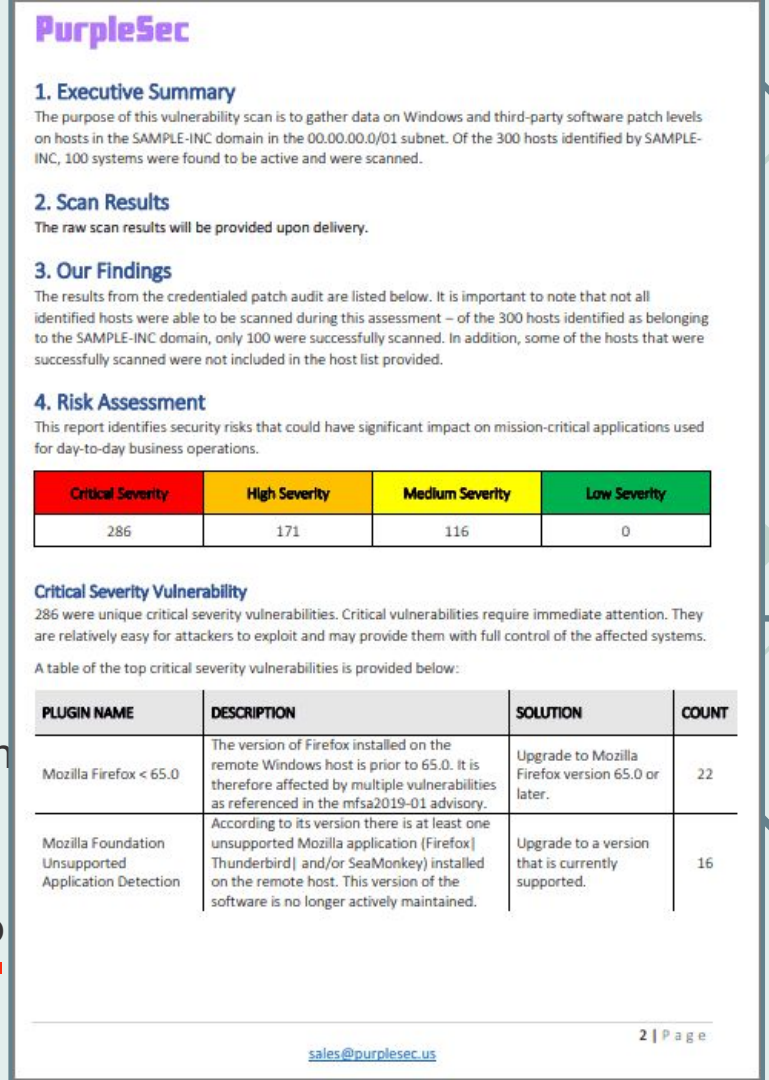
Ci sono 8 passaggi per eseguire una valutazione della vulnerabilità della sicurezza di rete:

1. Condurre l'identificazione e l'analisi dei rischi
2. Sviluppare criteri e procedure di scansione delle vulnerabilità
3. Identificare il tipo di scansione delle vulnerabilità
4. Configurare la scansione
5. Eseguire la scansione
6. Valutare i rischi
7. Interpretare i risultati della scansione
8. Creazione di un piano di riparazione e mitigazione

VULNERABILITY ASSESSMENT

Una **valutazione della vulnerabilità** è un processo di identificazione delle vulnerabilità di sicurezza nei sistemi, quantificazione e analisi, e correzione di tali vulnerabilità sulla base di rischi predefiniti.

Un esperto di sicurezza conduce un'analisi della vulnerabilità delle scansioni di rete per stabilire la priorità delle minacce identificate. Da questo, è possibile creare un piano d'azione con passaggi per rimediare alle vulnerabilità. Ad esempio, mantenere aggiornate le patch e implementare una procedura di gestione delle patch può essere una valida raccomandazione.



PurpleSec

1. Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and third-party software patch levels on hosts in the SAMPLE-INC domain in the 00.00.00.0/01 subnet. Of the 300 hosts identified by SAMPLE-INC, 100 systems were found to be active and were scanned.

2. Scan Results

The raw scan results will be provided upon delivery.

3. Our Findings

The results from the credentialed patch audit are listed below. It is important to note that not all identified hosts were able to be scanned during this assessment – of the 300 hosts identified as belonging to the SAMPLE-INC domain, only 100 were successfully scanned. In addition, some of the hosts that were successfully scanned were not included in the host list provided.

4. Risk Assessment

This report identifies security risks that could have significant impact on mission-critical applications used for day-to-day business operations.

Critical Severity	High Severity	Medium Severity	Low Severity
286	171	116	0

Critical Severity Vulnerability

286 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems.

A table of the top critical severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Mozilla Firefox < 65.0	The version of Firefox installed on the remote Windows host is prior to 65.0. It is therefore affected by multiple vulnerabilities as referenced in the mfsa2019-01 advisory.	Upgrade to Mozilla Firefox version 65.0 or later.	22
Mozilla Foundation Unsupported Application Detection	According to its version there is at least one unsupported Mozilla application (Firefox| Thunderbird| and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained.	Upgrade to a version that is currently supported.	16

sales@purplesec.us

1) RISK IDENTIFICATION

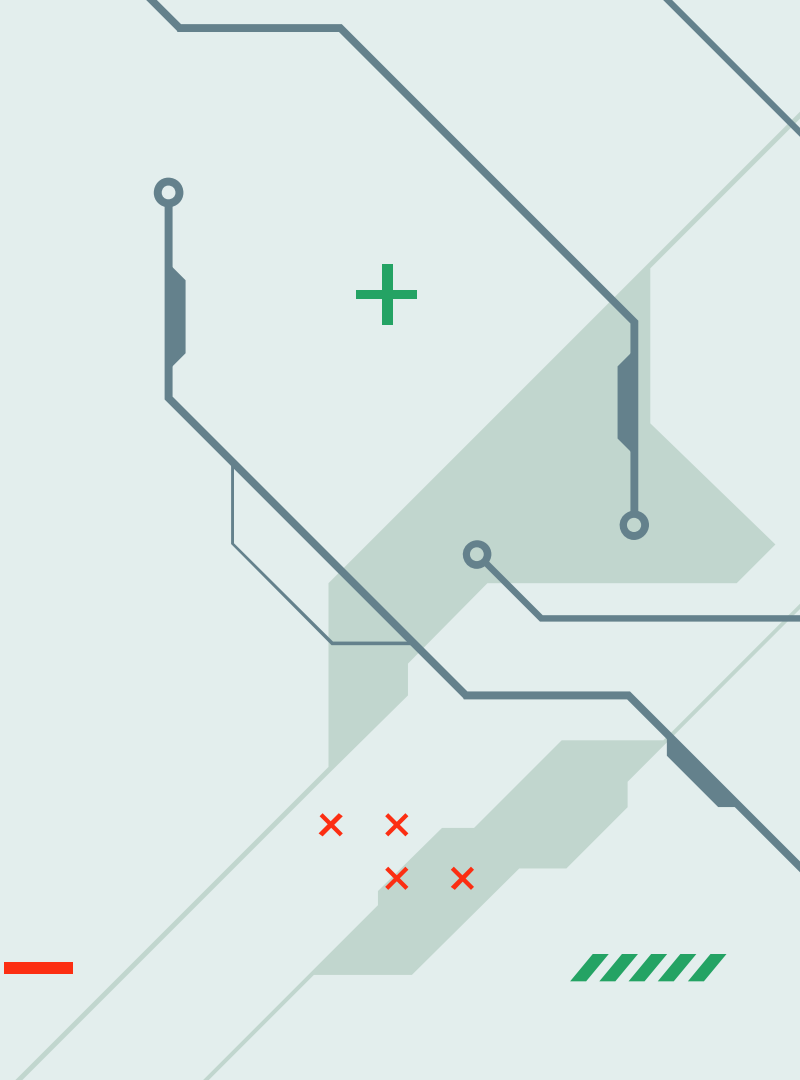
Il processo di identificazione e analisi dei rischi inizia con l'identificazione di tutti gli asset che fanno parte di un sistema informativo in un'azienda. Con un elenco completo di tutte le apparecchiature IT, le aziende possono iniziare ad assegnare i rischi a ciascuna risorsa per tenere conto della maggior parte delle situazioni che possono verificarsi.

Successivamente, l'assegnazione del valore e l'esecuzione dell'analisi determineranno il rischio effettivo che ogni asset deve affrontare. Con i rischi identificati e analizzati, il processo di valutazione della vulnerabilità inizia a prendere forma e l'attenzione si sposta lentamente sugli asset con il maggior livello di rischio.

2) VULNERABILITY SCANNING

Le politiche e le procedure scritte sono la spina dorsale di ogni azione importante che si prevede di intraprendere. Pertanto, tutte le attività svolte dovrebbero rientrare nei limiti di tali politiche e procedure.
La scansione delle vulnerabilità non è diversa.

Strutturando l'intero processo all'interno di una politica o di una procedura, avrai un determinato insieme di regole e passaggi che devono essere presi e punti che specificano il comportamento proibito.
Inutile dire che, prima di avviare qualsiasi scansione di vulnerabilità, dovrebbero esistere politiche e procedure esistenti che affrontino l'intero processo di scansione.



3) VULNERABILITY SCANNING

A seconda della parte del sistema che si desidera scansionare, le scansioni delle vulnerabilità sono suddivise in due categorie, esterne e interne. Le scansioni esterne comprendono tutte le risorse disponibili pubblicamente, mentre le scansioni interne prendono di mira tutte le risorse interne inaccessibili da Internet.

Per aggiungere, a seconda di chi sta conducendo la scansione della vulnerabilità, può essere classificata come scansione interna o come scansione di terze parti. Le scansioni delle vulnerabilità vengono in genere eseguite da personale di sicurezza qualificato e configurate in vari strumenti disponibili come soluzione software a pagamento o in forma open source.

STEP 1: RISK IDENTIFICATION

Identificare i rischi per ogni asset e le possibili minacce che devono affrontare è un compito complesso.

La cosa più importante è strutturare bene il processo in modo che nulla di importante sfugga.

Le aziende possono ottenere questo risultato strutturando i propri registri delle risorse con colonne aggiuntive per minacce e vulnerabilità.

STEP 1: RISK IDENTIFICATION

In questo modo avrai un documento centralizzato con tutte le informazioni necessarie. Dopo aver assegnato minacce e vulnerabilità alle tue risorse, puoi iniziare la fase di analisi in cui assegni i rischi alle risorse determinando l'impatto e la probabilità che ogni minaccia si materializzi.

Una volta completato, puoi finalmente concentrarti sull'assegnazione della priorità alle risorse a cui è stato assegnato il rischio più elevato e a quelle maggiormente colpite da debolezze o vulnerabilità note.

STEP 2: VULNERABILITY SCAN

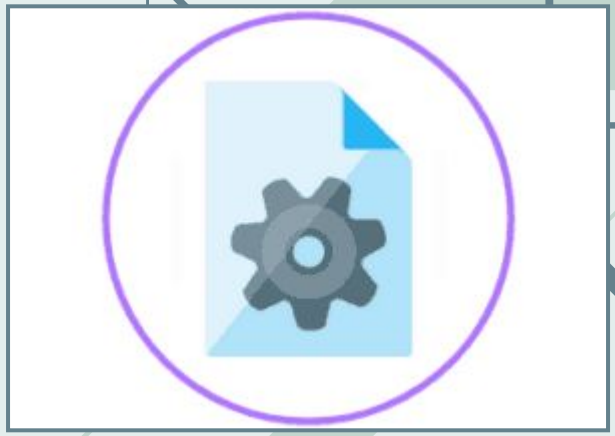
Per avere una metodologia di scansione strutturata e di successo, devono esistere politiche e procedure per avere una linea d'azione predeterminata da intraprendere. Ciò include tutti gli aspetti della scansione delle vulnerabilità.

Per cominciare, la politica o una procedura dovrebbe avere un proprietario ufficiale responsabile di tutto ciò che è scritto all'interno. La politica dovrebbe anche essere approvata dall'alta direzione prima di entrare in vigore. Anche la definizione della frequenza della scansione è importante per il rispetto della conformità.

STEP 2: VULNERABILITY SCAN

Da un punto di vista tecnico, tutto ciò che riguarda la configurazione e la funzionalità della scansione delle vulnerabilità dovrebbe essere enfatizzato e annotato. Il documento dovrebbe includere anche i passaggi da eseguire dopo il completamento della scansione.

I fattori più importanti sono i tipi di scansioni che verranno condotte, le modalità di esecuzione delle scansioni, le soluzioni software utilizzate, le vulnerabilità che hanno la precedenza sulle altre e i passaggi che devono essere eseguiti dopo il completamento della scansione.



STEP 3: IDENTIFY VULNERABILITY

La scansione delle vulnerabilità è un processo in cui il software di scansione delle vulnerabilità viene utilizzato per identificare i punti deboli della sicurezza nei sistemi informativi. La scansione delle vulnerabilità può essere eseguita dagli amministratori di rete, dagli analisti della sicurezza delle informazioni e da tutto il personale tecnico IT addestrato e incaricato di condurre una scansione delle vulnerabilità.

STEP 3: IDENTIFY VULNERABILITY

La maggior parte degli hacker malintenzionati tenta di mappare una rete scansionando il sistema e cercando di trovare possibili vulnerabilità per ottenere l'accesso non autorizzato ai sistemi informativi. Se gli hacker malintenzionati che stai cercando di difenderti utilizzano tecniche di scansione delle vulnerabilità, non hai altra scelta che impiegarle anche per stare al passo con il loro gioco.

A seconda del software in esecuzione sul sistema che è necessario scansionare e proteggere, è necessario determinare il tipo di scansione da eseguire per ottenere i massimi vantaggi.

TIPI COMUNI DI SCAN:

Network Vulnerability Scans

Il tipo più comune di scansione delle vulnerabilità è una **scansione basata sulla rete**. Questa scansione include le reti, i loro canali di comunicazione e le apparecchiature di rete utilizzate in un ambiente.

Alcuni dei principali dispositivi software e hardware che rientrano nell'ambito di una scansione di rete sono hub, switch, router, firewall, cluster e server. Una scansione di rete rileverà e classificherà tutte le vulnerabilità che trova su questi dispositivi.

TIPI COMUNI DI SCAN:

Host Based Vulnerability Scans

La **scansione basata su host** viene spesso erroneamente interpretata come la stessa di una scansione di rete. Lontano dalla verità, le scansioni basate su host risolvono le vulnerabilità relative agli host sulla rete, inclusi computer, laptop e server.

Più specificamente, questa scansione esamina la configurazione dell'host, le sue directory utente, i file system, le impostazioni della memoria e altre informazioni che possono essere trovate su un host. Questa scansione si concentra maggiormente sugli endpoint e sulla loro configurazione e funzionalità del sistema interno.

TIPI COMUNI DI SCAN:

Wireless Based Vulnerability Scans

Per eseguire correttamente una **scansione della vulnerabilità wireless** è necessario conoscere tutti i dispositivi wireless presenti nella rete. Inoltre, è necessario mappare gli attributi per ciascun dispositivo per sapere come configurare correttamente la scansione.

Il passaggio successivo consiste nell'identificare eventuali punti di accesso rouge che potrebbero trovarsi nella rete e isolare i dispositivi sconosciuti. È importante rimuovere questi dispositivi dalla rete in quanto potrebbero ascoltare il traffico wireless.

In seguito, puoi iniziare a testare i tuoi punti di accesso wireless e la tua infrastruttura LAN wireless.

TIPI COMUNI DI SCAN:

Application Based Vulnerability Scans

Questo tipo di scansione delle vulnerabilità viene spesso dimenticato ed è all'ombra di un test di penetrazione dell'applicazione. Tuttavia, se non stai conducendo un test di penetrazione dell'applicazione, la scansione delle tue applicazioni alla ricerca di vulnerabilità dovrebbe essere in cima alla tua lista di priorità.

Scegliendo tra una varietà di strumenti di scansione delle vulnerabilità delle applicazioni, puoi automatizzare le tue attività di sicurezza e aumentare la sicurezza delle tue applicazioni. Esiste una varietà di strumenti che è possibile utilizzare per condurre una vera scansione della vulnerabilità dell'applicazione.

STEP 4: CONFIGURE THE SCAN

Anche se ci sono molti fornitori di vulnerability scan tra cui scegliere, la configurazione di qualsiasi scansione può comunque essere affrontata identificando gli obiettivi generali e il tipo di sistema che si desidera scansionare.

CONFIGURAZIONE

- **Aggiungere un elenco di IP di destinazione**: gli indirizzi IP in cui sono ospitati i sistemi di destinazione devono essere inseriti nel software di scansione delle vulnerabilità per poter eseguire una scansione.
- **Definizione dell'intervallo di porte e dei protocolli**: dopo aver aggiunto gli IP di destinazione, è importante specificare l'intervallo di porte che si desidera scansionare e quale protocollo si desidera utilizzare nel processo.

CONFIGURAZIONE

- **Definizione degli obiettivi:** è necessario specificare se gli IP di destinazione sono database, server Windows, applicazioni, dispositivi wireless, ecc. Rendendo la scansione più specifica, si ottengono risultati più accurati.
- **Impostazione dell'aggressività della scansione, dell'ora e delle notifiche:** la definizione dell'aggressività della scansione può influenzare le prestazioni dei dispositivi che si intende scansionare. Per evitare tempi di inattività sui sistemi di destinazione, si può impostare una scansione da eseguire in un determinato momento, in genere non lavorativo. Inoltre, si può configurare per ricevere una notifica quando la scansione è completa.

STEP 5: PERFORM THE SCAN

Dopo aver determinato il tipo di scansione che si desidera eseguire e dopo aver impostato la configurazione della scansione, è possibile salvare la configurazione ed eseguirla come desiderato. A seconda delle dimensioni del target impostato e dell'intrusività della scansione, il completamento può richiedere da minuti a ore.

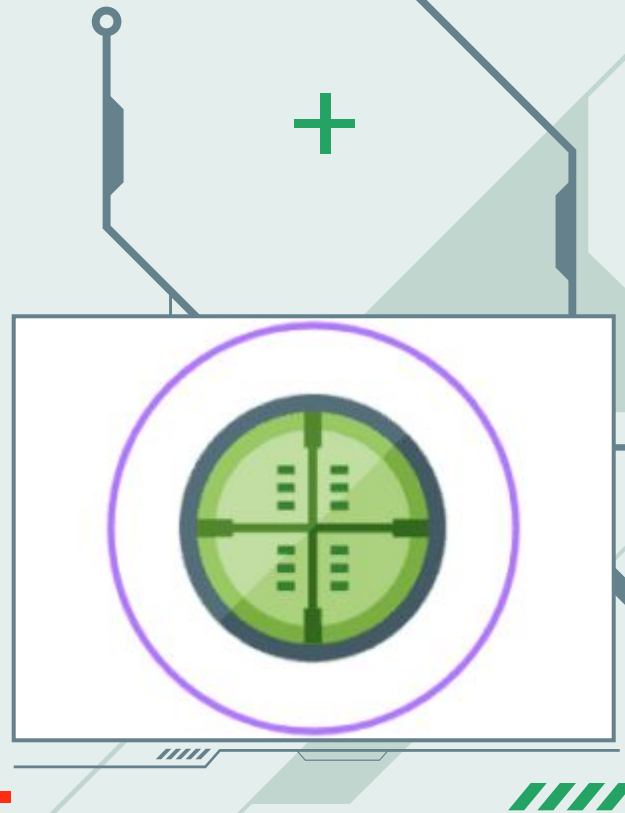
Ogni scansione di vulnerabilità può essere suddivisa in tre fasi:

- **Scansione**
- **Enumerazione**
- **Rilevamento vulnerabilità**

STEP 5: PERFORM THE SCAN

Nella **fase di scansione**, lo strumento che stai utilizzando eseguirà l'impronta digitale degli obiettivi specificati per raccogliere informazioni di base su di essi.

Con queste informazioni, lo strumento procederà all'**enumerazione** degli obiettivi e alla raccolta di specifiche più dettagliate come porte e servizi attivi e funzionanti. Infine, dopo aver determinato le versioni del servizio e la configurazione di ciascun IP di destinazione, lo strumento di scansione delle vulnerabilità di rete procederà a mappare le vulnerabilità nelle destinazioni, se presenti.



STEP 6: EVALUATE RISKS

I **rischi associati** all'esecuzione di una scansione di vulnerabilità riguardano principalmente la disponibilità del sistema di destinazione. Se i collegamenti e le connessioni non sono in grado di gestire il carico di traffico generato dalla scansione, la destinazione remota può arrestarsi e diventare non disponibile.

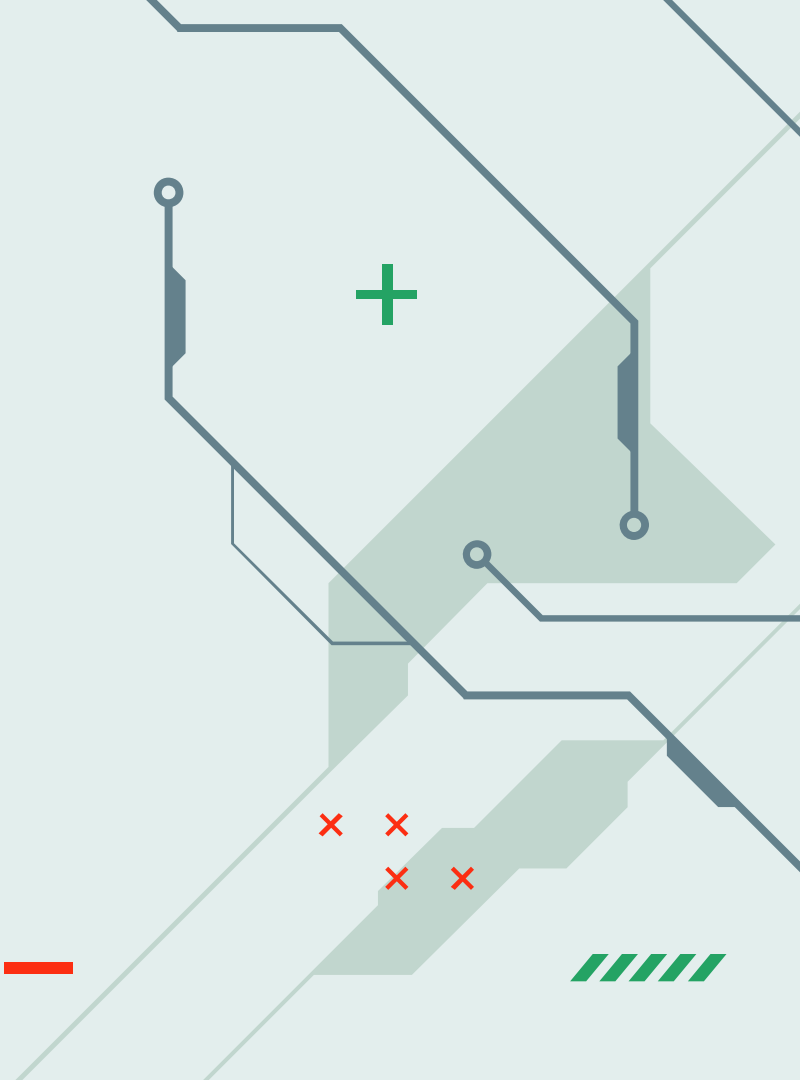
Quando si esegue una scansione su sistemi critici e sistemi di produzione, è necessario prestare particolare attenzione e la scansione deve essere eseguita dopo ore in cui il traffico verso la destinazione è minimo, al fine di evitare il sovraccarico.

STEP 7: INTERPRET RESULTS

La cosa più importante è che personale qualificato configuri, esegua e analizzi i risultati di una scansione delle vulnerabilità.

La conoscenza del sistema sottoposto a scansione è importante per stabilire correttamente la priorità degli sforzi di riparazione.

Anche se ogni strumento di scansione delle vulnerabilità assegnerà automaticamente la priorità alle vulnerabilità, a determinati tipi di vulnerabilità dovrebbe essere data priorità.



STEP 7: INTERPRET RESULTS

Ad esempio, le vulnerabilità legate all'esecuzione di codice in modalità remota dovrebbero avere la precedenza sulle possibili vulnerabilità di crittografia e DDOS. È importante considerare la probabilità e lo sforzo necessario affinché un hacker sfrutti la vulnerabilità rilevata.

Se è disponibile un exploit pubblico per una vulnerabilità che hai trovato nel tuo sistema, dare priorità a quella vulnerabilità dovrebbe avere la precedenza su altre vulnerabilità individuate che sono sfruttabili ma con uno sforzo molto maggiore.

STEP 8: MITIGATION PLAN

Dopo aver interpretato i risultati, il personale addetto alla sicurezza delle informazioni dovrebbe dare la priorità alla mitigazione di ogni vulnerabilità rilevata e lavorare con il personale IT per comunicare le azioni di mitigazione. Il personale della sicurezza delle informazioni e il personale IT devono comunicare e lavorare a stretto contatto nella fase di mitigazione della vulnerabilità per rendere il processo rapido e di successo.

Di solito vengono eseguite numerose scansioni di follow-up durante la risoluzione dei problemi avanti e indietro tra i team fino a quando tutte le vulnerabilità che devono essere mitigate non compaiono più nei report.

CVSS DATABASE

(sistema di punteggio di vulnerabilità comune)

Come accennato, durante la fase di interpretazione dei risultati della scansione delle vulnerabilità, il personale qualificato leggerà il report prodotto dalla scansione delle vulnerabilità e deciderà le azioni più critiche da intraprendere per prime. Il **database CVSS** può aiutare il personale nella sua decisione in quanto aiuta a valutare la gravità di ogni vulnerabilità.

Il database CVSS è uno standard del settore per la valutazione delle vulnerabilità della sicurezza che assegna un numero di punteggio a ciascuna vulnerabilità rilevata. Contribuisce alla definizione delle priorità delle vulnerabilità e accelera il processo di riparazione.

CVSS DATABASE

Sulla base di una scala da 0 a 10, il database CVSS assegna un valore numerico a ciascuna vulnerabilità in base a vari fattori come la gravità, la parte del sistema di sicurezza interessata, l'exploit pubblico disponibile per una determinata vulnerabilità e la complessità di un possibile attacco.

THANKS!