



TechNova
Solutions

TECHNOVA SOLUTIONS



OVERVIEW

01

About Us

02

Obbiettivo

03

Regole di ingaggio

04

Processo Effettuato

05

Rimedi

06

Conclusioni



ABOUT US

NOME:

TechNova Solutions

SETTORE:

Tecnologia e sviluppo software

TechNova Solutions è un'azienda di tecnologia e sviluppo software con sede a Milano. Specializzata in soluzioni software personalizzate per clienti di vari settori, TechNova Solutions si impegna a fornire prodotti innovativi e di alta qualità, con un forte focus sulla sicurezza informatica e la protezione dei dati.



OBIETTIVO

Sono stato incaricato da TechNova Solutions di condurre un penetration testing (pentesting) e un vulnerability assessment per valutare la sicurezza dei loro sistemi informatici e della rete aziendale. Questo incarico ha l'obiettivo di identificare eventuali vulnerabilità e punti deboli che potrebbero essere sfruttati da potenziali aggressori. Nel presente report, fornirò una descrizione dettagliata delle regole di ingaggio che abbiamo stabilito, del processo metodico che ho seguito per eseguire i test, delle soluzioni proposte per mitigare le vulnerabilità riscontrate e dei costi associati a queste misure di sicurezza. L'obiettivo finale è garantire che TechNova Solutions possa rafforzare la propria postura di sicurezza e proteggere efficacemente i propri dati e sistemi critici.

REGOLE DI INGAGGIO

01

Obiettivi

- Identificare le vulnerabilità nei sistemi informatici e nella rete.
- Valutare il livello di sicurezza attuale.
- Proporre soluzioni per mitigare le vulnerabilità identificate.

02

Scopo

- Sistemi inclusi: Server, workstation, dispositivi di rete, applicazioni web.
- Tipi di test: Test di intrusione esterni ed interni, test delle applicazioni web, analisi delle configurazioni di rete.

03

Limitazioni

- Nessuna interruzione delle operazioni aziendali.
- Accesso limitato agli ambienti di produzione per minimizzare i rischi.
- Riservatezza su tutte le informazioni raccolte durante i test.

04

Autorizzazioni

- Accesso autorizzato ai sistemi e alle risorse necessarie per eseguire i test.
- Informazioni di contatto per il team di sicurezza IT interno in caso di emergenze.

PROCESSO EFFETTUATO

Identificare le vulnerabilità presenti nei sistemi e nella rete di TechNova Solutions.

Scansione delle vulnerabilità: Utilizzo di scanner di vulnerabilità per rilevare porte aperte, servizi in esecuzione e vulnerabilità note. Per la scansione ho usato Nmap

Per prima cosa ho eseguito un ping da dentro la rete LAN per verificare se fossi connesso correttamente alla rete e poi ho effettuato una scansione con Nmap usando gli switch -sV per avere più informazioni sui servizi attivi nelle porte e -o per creare un file in cui salvare la scansione.

```
(kali㉿kali)-[~/Desktop/Epicode/S9]
$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=3.94 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=3.96 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=4.67 ms
^C
--- 192.168.240.150 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 3.941/4.190/4.669/0.338 ms

(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -sV -o Report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:08 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up (0.0023s latency).

Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.04 seconds
```

Come si può vedere ci sono tre porte aperte:

- Porta 135/tcp (msrpc): Questa è la porta utilizzata per il servizio Microsoft Remote Procedure Call (RPC). RPC è un protocollo che consente a un programma su una macchina di richiedere un servizio da un programma situato su un'altra macchina in una rete. Tuttavia, può essere sfruttato da attaccanti per eseguire codice arbitrario o effettuare attacchi di denial of service (DoS).

- Porta 139/tcp (netbios-ssn): Questa porta è associata al servizio Microsoft NetBIOS Session Service (netbios-ssn). Il servizio NetBIOS gestisce le sessioni di comunicazione tra computer in una rete locale. Tuttavia, è noto che NetBIOS presenta vulnerabilità di sicurezza e può essere utilizzato per condurre attacchi come lo sniffing di dati di rete o l'esecuzione di code arbitrarie.

- Porta 445/tcp (microsoft-ds): Questa porta è utilizzata per il servizio Microsoft-DS (Directory Services) su sistemi operativi Windows. Questo servizio consente la condivisione di file e stampanti in una rete locale. Tuttavia, la porta 445 è nota per essere vulnerabile a svariate forme di attacco, inclusi attacchi di tipo ransomware come WannaCry, e può essere sfruttata per ottenere l'accesso non autorizzato ai file e alle risorse condivise sul sistema.

RIMEDI

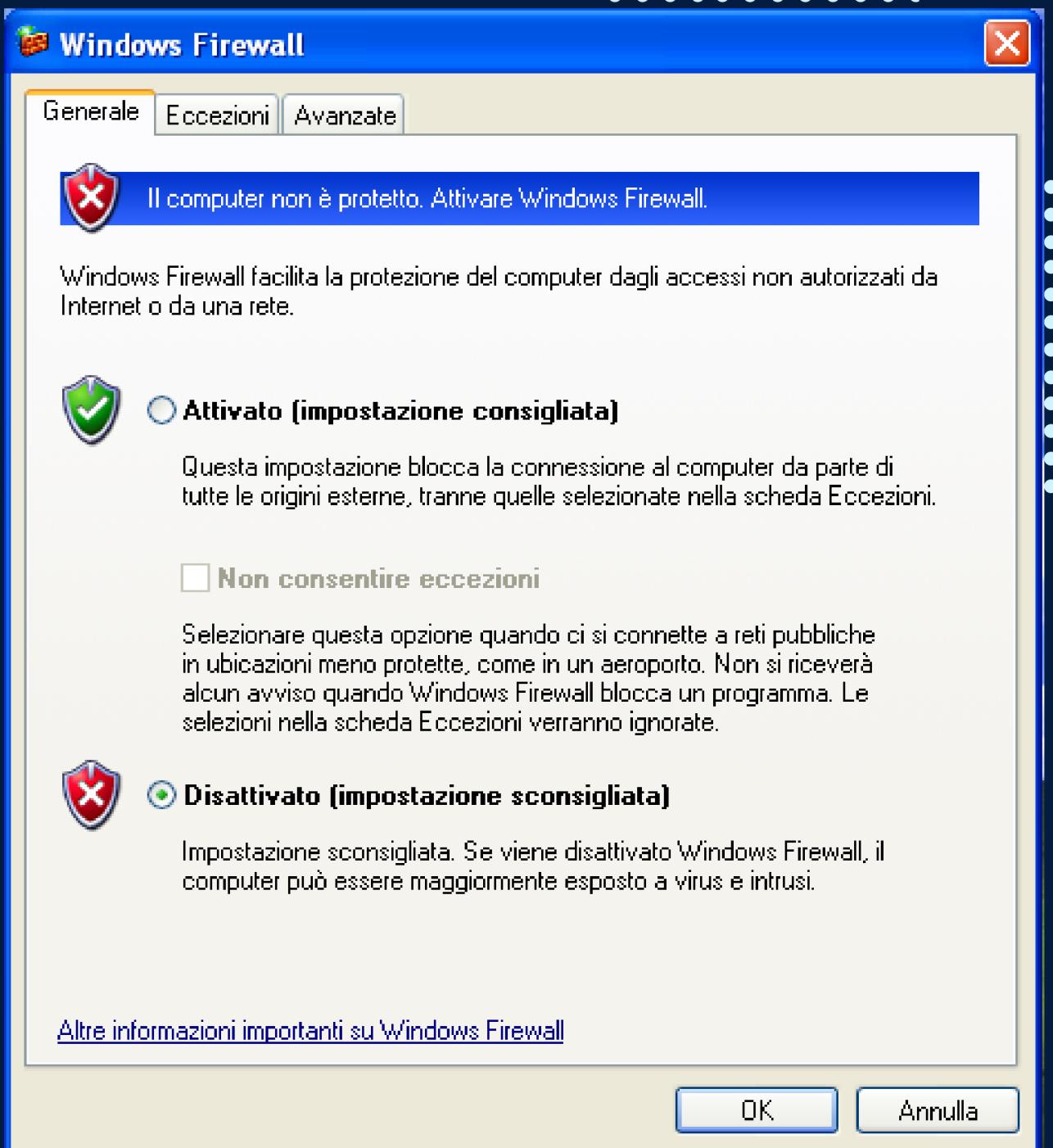
La soluzione più semplice e sicura per affrontare le potenziali vulnerabilità sarebbe quella di migrare verso un sistema operativo più recente e supportato, beneficiando così delle ultime patch di sicurezza e delle funzionalità di protezione avanzate. Tuttavia, comprendendo che l'azienda è completamente strutturata su Windows XP e desidera continuare ad utilizzarlo per motivi di compatibilità o legacy, si è reso necessario esaminare più attentamente le regole del firewall per implementare misure di sicurezza aggiuntive.

Andando a controllare il Firewall esso risultava disabilitato, quindi sono andato ad attivarlo e a riprovare la scansione.

```
(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -sV -o Report.txt 192.168.240.150 | Plain text document
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:30 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds

(kali㉿kali)-[~/Desktop/Epicode/S9]
$ nmap -Pn -sV -o Report.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 09:30 EDT
Nmap scan report for 192.168.240.150 (192.168.240.150)
Host is up.
All 1000 scanned ports on 192.168.240.150 (192.168.240.150) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.79 seconds
```



Andando a rieseguire lo scan ci dice le porte blocano il ping, quindi provo a ad usare lo switch -Pn che non completa la connessione TCP ma le porte sono filtrate quindi non abbiamo nessuna informazione.

Analisi delle Regole del Firewall:

Quindi per diminuire i rischi bisogna attivare il firewall ed impostare correttamente delle regole in modo da permettere alle persone autorizzate di usare i servizi e bloccare gli estranei.

- Porta 135/tcp (msrpc): È consigliabile limitare l'accesso alla porta 135 solo ai server o ai servizi specifici che ne necessitano, riducendo così l'esposizione a potenziali attacchi. Inoltre, è possibile implementare regole di filtraggio per bloccare il traffico proveniente da fonti non attendibili o non autorizzate.
- Porta 139/tcp (netbios-ssn): Poiché NetBIOS è noto per le sue vulnerabilità, si consiglia di disabilitare il servizio se non è strettamente necessario per le operazioni aziendali. Se la disabilitazione non è un'opzione, è fondamentale implementare regole di firewall rigorose per limitare l'accesso solo ai dispositivi e agli utenti autorizzati.
- Porta 445/tcp (microsoft-ds): Essendo vulnerabile a svariate forme di attacco, è vitale applicare regole di firewall che limitino l'accesso alla porta 445 solo ai servizi essenziali e ai dispositivi di rete fidati. Inoltre, è consigliabile considerare l'implementazione di una VPN per proteggere il traffico di rete sensibile e mitigare i rischi associati alla condivisione di file e stampanti su questa porta.

CONCLUSIONI

Questo approccio consente di mantenere l'infrastruttura operativa su Windows XP, pur introducendo misure di sicurezza aggiuntive attraverso le regole del firewall, al fine di mitigare i rischi di sicurezza associati alle vulnerabilità identificate durante il processo di scansione dei servizi.

In conclusione, l'esame delle regole del firewall svolge un ruolo fondamentale nel garantire la sicurezza delle infrastrutture IT, specialmente in contesti in cui l'utilizzo di sistemi operativi legacy come Windows XP è inevitabile. Nonostante le potenziali vulnerabilità associate ai servizi identificati durante la scansione, è possibile implementare misure di sicurezza aggiuntive attraverso il firewall per mitigare i rischi e proteggere l'azienda da possibili attacchi esterni. Tuttavia, è importante sottolineare che l'adozione di un sistema operativo più moderno e supportato rimane la soluzione più efficace per garantire un livello ottimale di sicurezza informatica. Pertanto, si consiglia vivamente a TechNova Solutions di pianificare una strategia di migrazione verso sistemi operativi aggiornati, lavorando in collaborazione con i reparti IT e di sicurezza per garantire una transizione fluida e sicura.

Nel frattempo, l'implementazione di regole del firewall rigorose e la costante vigilanza sulle minacce informatiche consentiranno a TechNova Solutions di mantenere un ambiente IT sicuro e resiliente, proteggendo i propri dati e sistemi critici dagli attacchi esterni.

BUSINESS CONTINUITY & DISASTER RECOVERY

Questo report fornisce una valutazione quantitativa dell'impatto di diversi disastri sugli asset di TechNova Solutions, con l'obiettivo di implementare strategie efficaci di Business Continuity e Disaster Recovery (BCDR). Attraverso l'analisi dei rischi di inondazioni, terremoti e incendi, e utilizzando il metodo Annual Loss Expectancy (ALE), calcoleremo la perdita annuale stimata per l'azienda, fornendo raccomandazioni per mitigare tali rischi.

Metodologia

Per valutare l'impatto dei disastri, utilizzeremo il metodo Annual Loss Expectancy (ALE), che si basa su due componenti principali:

- Single Loss Expectancy (SLE): La perdita finanziaria associata a un singolo evento disastroso.
- Annualized Rate of Occurrence (ARO): La frequenza annua con cui si prevede che l'evento disastroso si verifichi.

Dove:

- Valore dell'Asset: Il valore monetario totale dell'asset in questione.
- Fattore di Esposizione (EF): La percentuale di perdita che si prevede che l'asset subisca in caso di disastro.
- La formula per calcolare il SLE è: $SLE = \text{Valore dell'Asset} \times \text{Fattore di Esposizione (EF)}$
- La formula per calcolare l'ALE è: $ALE = SLE \times ARO$

Per effettuare questi calcoli ho usato un foglio Excel in modo da farli in automatico, potendo cambiare anche i dati se necessario, ad avere una tabella riassuntiva con tutti i valori

ASSET	VALORE	EXPOSURE FACTOR			SLE			ALE		
		Terremoto	Incendio	Inondazione	Terremoto	Incendio	Inondazione	Terremoto	Incendio	Inondazione
Edificio primario	350.000 €	80%	60%	55%	280.000 €	210.000 €	192.500 €	9.333 € /anno	10.500 € /anno	3.850 € /anno
Edificio secondario	150.000 €	80%	50%	40%	120.000 €	75.000 €	60.000 €	4.000 € /anno	3.750 € /anno	1.200 € /anno
Datacenter	100.000 €	95%	60%	35%	95.000 €	60.000 €	35.000 €	3.167 € /anno	3.000 € /anno	700 € /anno
ARO		1 volta ogni 30 anni	1 volta ogni 20 anni	1 volta ogni 50 anni						

RACCOMANDAZIONI

Per minimizzare l'impatto finanziario e operativo di questi disastri, si raccomanda di implementare le seguenti misure:

O1 Piano di Business Continuity e Disaster Recovery (BCDR):

- Sviluppo e Mantenimento: Sviluppare e mantenere un piano BCDR aggiornato che includa procedure specifiche per rispondere a ciascun tipo di disastro.
- Esercitazioni di Emergenza: Eseguire regolari esercitazioni di emergenza per assicurare che il personale sia preparato a rispondere rapidamente ed efficacemente in caso di emergenza.

O2 Ridondanza e Backup dei Dati:

- Soluzioni di Backup: Implementare soluzioni di backup regolari e sicure per garantire che i dati critici possano essere ripristinati rapidamente in caso di perdita o danneggiamento.
- Ridondanza Geografica: Considerare la ridondanza geografica per i datacenter per assicurare la continuità operativa anche in caso di disastri locali.

O3

Miglioramento delle Infrastrutture Fisiche:

- Protezione Anti-Incendio: Installare sistemi di protezione anti-incendio avanzati negli edifici primari e secondari.
- Barriere Anti-Inondazione: Implementare barriere anti-inondazione e sistemi di drenaggio avanzati per proteggere gli edifici dalle inondazioni.

O4

Formazione e Sensibilizzazione del Personale:

- Programmi di Formazione: Organizzare programmi di formazione regolari per il personale su come reagire in caso di disastri.
- Sensibilizzazione: Promuovere una cultura di sensibilizzazione alla sicurezza e alla preparazione alle emergenze all'interno dell'azienda.

L'analisi quantitativa delle perdite annuali stimate (ALE) per TechNova Solutions evidenzia l'importanza di implementare misure efficaci di Business Continuity e Disaster Recovery. Attraverso l'adozione delle raccomandazioni sopra descritte, TechNova Solutions può minimizzare l'impatto finanziario e operativo dei disastri, garantendo la resilienza dei propri sistemi e la continuità delle operazioni aziendali.

THREAT INTELLIGENCE & IOC

L'analisi del traffico di rete è una componente essenziale della sicurezza informatica per rilevare attività sospette e proteggere le risorse aziendali. Questo rapporto documenta l'analisi del traffico di rete catturato tramite Wireshark per TechNova Solutions, evidenziando eventuali anomalie e fornendo raccomandazioni per migliorare la sicurezza della rete.

8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e

I pacchetti 8, 9, 10, e 11 sono richieste e risposte ARP, utilizzate per mappare gli indirizzi IP agli indirizzi MAC. Possiamo vedere che 192.168.200.100 e 192.168.200.150 si chiedono il MAC.

24	36.774700464	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Ci sono tante richieste TCP da parte di 192.168.200.100 e questo può indicare un tentativo di scansione della rete verso 192.168.200.150, che risponde con un SYN, ACK, questo potrebbe indicare che la porta risulta aperta, con un RST, ACK quando la porta è chiusa oppure filtrata.

AZIONI RACCOMANDATE

01

Monitoraggio e Logging: Continuare a monitorare il traffico di rete e mantenere log dettagliati delle attività per identificare pattern simili in futuro.

02

Controllo degli Accessi: Implementare regole di firewall per limitare le connessioni alle porte critiche solo ai dispositivi autorizzati.

03

Analisi dei dispositivi: Eseguire un'analisi completa sui dispositivi coinvolti per identificare potenziali compromissioni.

04

Aggiornamento delle Sicurezze: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza e che le configurazioni di rete seguano le migliori pratiche di sicurezza.

L'analisi del traffico di rete di TechNova Solutions ha rivelato tentativi di connessione ripetuti e falliti tra 2 dispositivi , che potrebbero indicare attività sospette come scansioni di rete o tentativi di accesso non autorizzati. Implementare le raccomandazioni sopra indicate contribuirà a migliorare la sicurezza della rete e a proteggere le risorse aziendali da potenziali minacce.