PROGETTO S1/L5 BCC ICCREA

TRACCIA:

La vostra organizzazione vi ha incaricato di svolgere un risk assessment sulla seguente azienda. Nome azienda: TechnoCorp Settore: Tecnologia dell'informazione e servizi IT

Descrizione: TechnoCorp è un'azienda di medie dimensioni che opera nel settore IT, fornendo servizi di consulenza, sviluppo software e gestione di infrastrutture tecnologiche a clienti di diverse industrie. Fondata 15 anni fa, l'azienda conta circa 500 dipendenti distribuiti tra la sede centrale e 3 filiali regionali.

Infrastruttura IT:

• Rete aziendale con server interni che ospitano applicazioni aziendali critiche, database e sistemi di archiviazione dati

• Utilizzo di cloud pubblici (AWS, Azure) per alcune applicazioni e servizi

• Rete wireless per dipendenti e guest

• Dispositivi personali (Bring Your Own Device) utilizzati dai dipendenti

• Numerosi laptop e workstation per sviluppatori e consulenti

• Sito web aziendale ospitato esternamente.

• Firewall perimetrale

• EDR/xDR su tutti i sistemi

Clienti e dati sensibili:

• TechnoCorp gestisce dati sensibili di clienti, come informazioni finanziarie, dati personali di dipendenti/clienti, proprietà intellettuale

• I principali clienti includono banche, assicurazioni, aziende sanitarie e produttori

Personale e accessi:

• Amministratori di sistema con accesso totale all'infrastruttura

• Sviluppatori con accesso ai sistemi di sviluppo

• Personale di supporto tecnico con accesso limitato

• Consulenti e collaboratori esterni con credenziali di accesso

• Politica di password e autenticazione a due fattori implementata.

Partendo dalla descrizione fornita, procedere con l'identificazione di uno scenario di rischio (Top-down) fino ad arrivare all'analisi del rischio di questo scenario.

- Identificazione del rischio
- Analisi degli asset
- Analisi delle vulnerabilità
- Analisi delle minacce
- Modellazione delle minacce
- Scenari di rischio
- Analisi del rischio qualitativa o semi-quantitativa

Per le probabilità di occorrenza, statistiche e stime, affidatevi a fonti note o studi di settore.

ANALISI DEGLI ASSET

Queste stime sono basate sulle dimensioni e sull'attività dell'azienda descritta e tengono conto della necessità di garantire un'adeguata sicurezza e funzionalità dei servizi IT offerti:

1.Rete aziendale con server interni:

Costo di acquisizione: 200.000 €

Costo di possesso annuale: 50.000 €

Costo di dismissione: 20.000 €

2.Utilizzo di Cloud pubblici (AWS, Azure)

Costo di acquisizione: Variabile, ipotizziamo circa 500 €

Costo di possesso annuale: Dipende dall'utilizzo, circa 2.000 €

3.Dispositivi personali utilizzati dai dipendenti

Costo di acquisizione: dipende dal tipo di dispositivo e dalla politica aziendale, ma potrebbe essere intorno ai 1000 € per dispositivo.

Costo di possesso annuale: Circa 300€ - 700€ per dispositivo per la manutenzione e il supporto tecnico.

Costo di dismissione: Non c'è un costo specifico di dismissione, ma potrebbe essere necessario cancellare i dati aziendali dai dispositivi al termine dell'impiego.

4.Reti wireless per dipendenti e guest

Supponiamo che TechnoCorp utilizzi una rete wireless di medie dimensioni per i dipendenti e gli ospiti nelle sedi aziendali, che include router, access point e dispositivi di sicurezza. Per una stima approssimativa, potremmo considerare un costo annuo di circa 5.000-10.000 euro per la gestione e la manutenzione della rete, inclusi eventuali costi di licenza per software di gestione della rete e soluzioni di sicurezza.

5.Laptop e workstation per sviluppatori e consulenti

Ipotizziano che l'azienda dispone di circa 300 laptop e workstation per i suoi sviluppatori e consulenti, che vengono rinnovati ogni 3-4 anni. Per una stima approssimativa, potremmo considerare un costo medio di circa 800-1200 euro per dispositivo, comprensivo di software e servizi di assistenza. Quindi, considerando un periodo di ammortamento di 3 anni e una sostituzione parziale ogni anno, il costo annuo totale potrebbe variare tra 80.000 e 120.000 euro.

6.Sito web ospitato esternamente

Costo di acquisizione: Circa 5.000 € per lo sviluppo e la configurazione iniziale del sito.

Costo di possesso annuale: Circa 2.500€ per la gestione del contenuto, l'hosting e gli aggiornamenti di sicurezza.

Costo di dismissione: Non abbiamo un costo specifico, ma può esserci un costo associato alla migrazione del sito verso un'altra piattaforma.

7. Firewall perimetrale

Costo di acquisizione: Tra 10.000€ e 15.000€ per l'hardware e il software del firewall.

Costo di possesso annuale: Circa 4.000 € per la manutenzione, gli aggiornamenti e la gestione delle regole.

Costo di dismissione: Non c'è un costo specifico di dismissione, ma potrebbe essere necessario sostituire il firewall con una soluzione più recente alla fine del suo ciclo di vita.

8. EDR/xDR su tutti i sistemi

Costo di acquisizione: Circa 50.000 € per l'acquisto e l'implementazione delle soluzioni EDR/xDR.

Costo di possesso annuale: Circa 30.000 € per il monitoraggio continuo, gli aggiornamenti delle minacce e la gestione delle soluzioni.

Potremmo poi andare ad effettuare un'analisi degli asset relativi alle componenti hardware e ai servizi in base al costo di sostituzione per gli hardware e al contributo del fatturato annuo per i servizi:

Componenti hardware:

PC per i dipendenti

Costo di sostituzione: In media, considerando i costi di acquisto e installazione, potrebbe essere di circa 700 € per PC.

Con 500 dipendenti, il costo totale di sostituzione dei PC potrebbe essere di circa 350.000 €

Server interni:

Costo di sostituzione: Dipende dalle specifiche dei server e dalla complessità dell'infrastruttura, ma potrebbe essere intorno ai 4.000€ per server.

Servizi:

Servizi di consulenza IT:

Contributo al fatturato annuo: Supponiamo che i servizi di consulenza IT rappresentino il 30% del fatturato annuo dell'azienda, che ad esempio potrebbe essere di 10 milioni di euro. Il contributo al fatturato annuo da parte dei servizi di consulenza IT sarebbe di circa 3 milioni di euro.

Sviluppo software

Contributo al fatturato annuo: Sviluppo software rappresenta il 40% del fatturato annuo dell'azienda. Il contributo al fatturato annuo da parte dello sviluppo software sarebbe di circa 4 milioni di euro.

Gestione di infrastrutture tecnologiche

Contributo al fatturato annuo: Gestione delle infrastrutture tecnologiche rappresenti il restante 30% del fatturato annuo dell'azienda. Il contributo al fatturato annuo dalla gestione delle infrastrutture tecnologiche sarebbe di circa 3 milioni di euro.

Infine, nell'analisi degli asset è importante ricordare che il personale rappresenta un valore fondamentale, in questo caso si potrebbe effettuare una stima (500 dipendenti) in base o al costo di assunzione/formazione o in base alla produttività e al contributo economico.

IDENTIFICAZIONE DEL RISCHIO

Per l'identificazione del rischio, andiamo ad utilizzare un approccio top-down nella definizione degli scenari di minaccia. Per prima cosa consideriamo quali potrebbero essere gli obiettivi strategici di TechnoCorp:

- Fornire servizi IT di alta qualità ai clienti.
- Proteggere i dati sensibili dei clienti e garantire la conformità normativa.
- Mantenere l'affidabilità e la sicurezza dell'infrastruttura IT.
- Preservare la reputazione aziendale e la fiducia dei clienti

Da essi, verifichiamo quali potrebbero essere le potenziali minacce o eventi che potrebbero impedire il raggiungimento di questi obiettivi:

- Violazione della sicurezza dei dati sensibili dei clienti: comprende accessi non autorizzati, perdita o furto di dati, attacchi informatici.
- Interruzioni dei servizi IT: possono essere causate da attacchi DDoS, malfunzionamenti hardware/software, errori umani.
- Compromissione della reputazione aziendale: derivante da violazioni della sicurezza dei dati, prestazioni deludenti dei servizi IT, pubblicità negativa.

Procedendo da uno scenario più globale, identifichiamo ora rischi più specifici:

1. Violazione dei dati sensibili dei clienti attraverso un attacco informatico mirato.

Descrizione: Un attacco informatico mirato compromette i server interni di TechnoCorp, consentendo l'accesso non autorizzato e la sottrazione di dati sensibili dei clienti.

Potenziali conseguenze: Perdita di fiducia dei clienti, sanzioni legali, danni finanziari.

Probabilità: Media.

Impatto: Molto alto.

2. Interruzione dei servizi IT a causa di un attacco DDoS.

Descrizione: Un attacco DDoS mirato al sito web aziendale di TechnoCorp provoca interruzioni dei servizi per i clienti, impedendo loro di accedere ai servizi e ai dati.

Potenziali conseguenze: Perdita di clienti, danni finanziari, compromissione della reputazione.

Probabilità: Bassa.

Impatto: Alto.

3. Compromissione della reputazione aziendale a seguito di una violazione della sicurezza dei dati.

Descrizione: Una violazione della sicurezza dei dati sensibili dei clienti viene resa pubblica, causando preoccupazioni per la privacy dei clienti e danneggiando la reputazione di TechnoCorp.

Potenziali conseguenze: Perdita di clienti, azioni legali, danni alla reputazione.

Probabilità: Media.

Impatto: Alto.

ANALISI DELLE VULNERABILITA'

PC e Server con Software non Aggiornato: Potenziale esposizione a vulnerabilità note non corrette da aggiornamenti.

Impatto: Possibile accesso non autorizzato ai sistemi.

Priorità di Mitigazione: Media

Possibile Mitigazione: Implementazione di un processo di gestione delle patch per garantire l'aggiornamento regolare del software, più l'utilizzo di strumenti di scansione per identificare e correggere le vulnerabilità.

Password Deboli sui PC e Server: Rischio di accesso non autorizzato.

Impatto: Possibile compromissione dei dati sensibili.

Priorità di Mitigazione: Alta

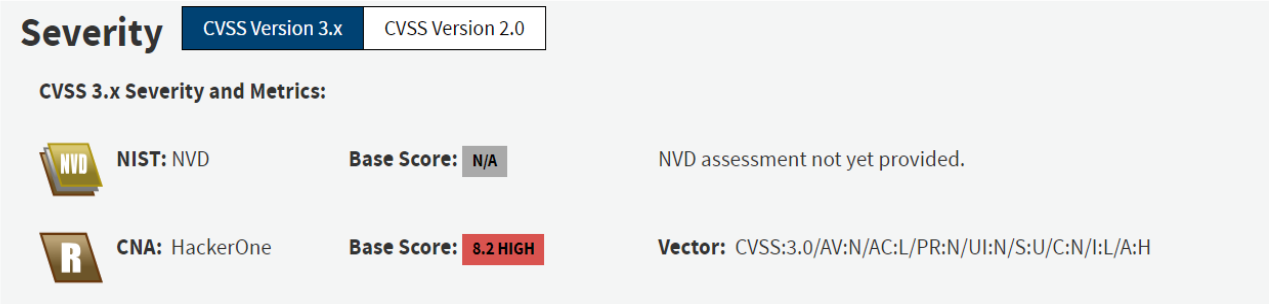
Possibile Mitigazione: Implementazione di politiche di password robuste. Richiesta di cambiamento periodico delle password

Inoltre, andando più nello specifico, ipotizziamo che TechnoCorp, potrebbe essere vulnerabile agli attacchi DDoS che mirano a interrompere i suoi servizi critici, come il sito web aziendale e le applicazioni clienti. Possiamo utilizzare strumenti come il Common Vulnerabilities and Exposures (CVE) e il National Vulnerability Database (NVD).

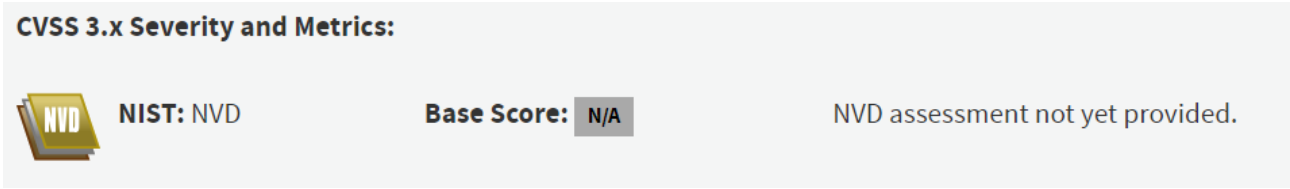
Dunque, identifichiamo e analizziamo le vulnerabilità che potrebbero essere sfruttate per condurre un attacco DDoS contro l'infrastruttura IT dell'azienda. Questo ci consente di sviluppare strategie di mitigazione mirate per proteggere i servizi IT e ridurre il rischio di interruzione dei servizi.

Per esempio: vulnerabilità nel protocollo HTTP/2, un nuovo vettore per attacchi DoS, rinominata Continuation Flood, potrebbe condurre ad attacchi DoS causando il crash del server web. Ciascuna di queste varianti della vulnerabilità "Continuation Flood" corrisponde a differenti implementazioni del protocollo HTTP/2 e consentono vari livelli di attacchi:

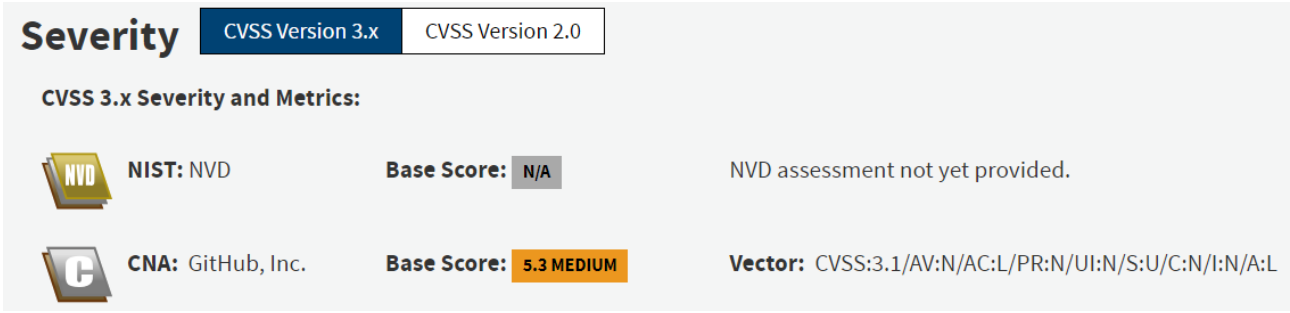
- CVE-2024-27983: colpisce il server HTTP/2 di Node.js. L'invio di alcuni frame HTTP/2 può causare una perdita di memoria dovuta a una condizione di conflitto, con conseguente potenziale DoS.



- CVE-2023-45288: colpisce i pacchetti net/http e net/http2 di Go. Consente a un utente malintenzionato di inviare un insieme arbitrariamente grande di intestazioni, causando un consumo eccessivo di CPU.



- CVE-2024-28182: espone un'implementazione che utilizza la libreria nghttp2, che continua a ricevere frame di CONTINUATION senza un corretto callback di reset dello stream, portando quindi a un DoS.



Come riportato anche nel bollettino di sicurezza del CERT-CC, la vulnerabilità Continuation Flood risulta essere più grave delle vulnerabilità sfruttate in attacchi precedenti, questo perché le richieste malevole potrebbero non essere visibili nei log di accesso se l'analisi avanzata dei frame non è abilitata sul server, condizione piuttosto comune. Gli amministratori (con accesso totale al sistema) sono incoraggiati ad aggiornare il software interessato all'ultima versione disponibile per mitigare le potenziali minacce.

ANALISI DELLE MINACCE

Analisi delle minacce per l'azienda, utilizzando il sistema di categorizzazione delle minacce definite nell'ISO 27005 Annex C (Accidentale, Deliberato, Ambientale):

Minaccia	Vettore di attacco	Fonte della minaccia	Probabilità (prima)	Controllo di mitigazione e costo	Probabilità (dopo)
Attacco DDos (deliberato)	Saturazione CPU, sovraccarico del server	Black hat	alta	Implementazione di regole più efficaci del firewall per filtrare traffico sospetto	moderata
Phishing (deliberato)	e-mail fraudolente	Attaccanti esterni	media	Formazione dipendenti	bassa
Attacco ransomware (deliberato)	e-mail di phishing, exploit vulnerabilità, download file dannosi	Gruppo hacker	media	Back-up regolari, aggiornamenti dei software e sistemi operativi	bassa
Furti fisici (deliberato)	Furto, smarrimento	Attaccante interno/esterno	media	Sicurezza fisica (lucchetti, accesso controllato)	bassa
Malware (deliberato)	Download file o usb infette	Attaccante esterno	alta	Antimalware e antivirus	bassa
Incidente di perdita di dati (ambientale)	Allagamenti, calamità naturali	Eventi catastrofici, errori di progettazione	media	Investimento e implementazione di sistemi di allarme antincendio e di sistemi di protezione da allagamenti	bassa
Perdita di dati (accidentale)	Errore umano, guasto hardware/software	Dipendenti, errori di configurazione	media	Implementazione di test dei processi di ripristino dei dati	bassa

MODELLAZIONE DELLE MINACCE

Per condurre un'analisi della modellazione delle minacce (Threat Modeling) utilizziamo il framework di Shostack, rispondendo alle quattro domande chiave:

1.su cosa stiamo lavorando?

TechnoCorp è un'azienda di consulenza IT che fornisce servizi di sviluppo software, gestione delle infrastrutture tecnologiche e consulenza informatica a clienti di diverse industrie. Lavoriamo sull'implementazione e sulla gestione di sistemi IT critici per i nostri clienti, compresi server, reti, applicazioni web e servizi cloud.

2.cosa può andare storto?

Le minacce potenziali includono attacchi informatici come DDoS, phishing, ransomware e accesso non autorizzato. Possibili eventi negativi potrebbero includere la perdita o il furto di dati sensibili dei clienti, interruzioni dei servizi IT critici, danni alla reputazione dell'azienda e perdite finanziarie.

3.che cosa faremo a riguardo?

Considerando che, l'azienda utilizza già un firewall perimetrale e l'autenticazione a due fattori come misura di sicurezza, possiamo ipotizzare altre azioni tra le quali:

- Implementazione di una politica rigorosa di gestione delle patch e degli aggiornamenti software per assicurarci che tutti i sistemi e le applicazioni siano protetti dalle ultime vulnerabilità note.
- Penetration testing e valutazioni della sicurezza per identificare e correggere eventuali vulnerabilità prima che possano essere sfruttate dagli attaccanti.
- Adozione di una politica di accesso privilegiato basata sul principio del privilegio minimo, limitando l'accesso agli account e alle risorse solo al necessario per svolgere le attività lavorative, per cui non ai consulenti esterni.
- Implementazione di un sistema di monitoraggio di sicurezza avanzato, che possa rilevare e rispondere prontamente a comportamenti anomali o potenziali attacchi informatici.
- Formazione continua ai dipendenti sull'importanza della sicurezza informatica e sulle migliori pratiche per proteggere i dati aziendali e sensibilizzare sulle minacce informatiche.

4.abbiamo fatto un buon lavoro?

Monitoreremo costantemente l'efficacia delle nostre contromisure di sicurezza e valuteremo regolarmente il nostro livello di preparazione e resilienza contro le minacce informatiche. Sarà importante condurre revisioni e aggiornamenti periodici del nostro approccio alla sicurezza per garantire che rimanga adeguato alle minacce in evoluzione.

Possiamo quindi procedere attribuendo un punteggio e calcolo della media ponderata, moltiplicando l'efficacia potenziale di ciascuna azione proposta per il suo peso corrispondente, e sommando i risultati di queste moltiplicazioni, dividiamo per la somma dei pesi.

Azione proposta	Efficacia potenziale (1-5)
Politica di gestione delle patch e aggiornamenti software	4
Penetration testing	5
Politica di accesso privilegiato (privilegio minimo)	4
Implementazione sistema di monitoraggio della sicurezza avanzato	5
Formazione continua dei dipendenti sulla sicurezza informatica	4

$$\text{Media} = \frac{(4\times4)+(5\times5)+(4\times4)+(5\times4)+(4\times5)}{4+5+4+5+4} = \frac{16+25+16+20+20}{22} = \frac{97}{22} \approx 4.41$$

Il valore unico della minaccia dell'attacco DDoS, dopo l'implementazione delle azioni proposte, sarebbe quindi approssimativamente 4.41.

SCENARIO DI RISCHIO

Dopo aver identificato gli asset, le minacce, le vulnerabilità, possiamo dunque definire lo scenario di rischio, attraverso l'approccio top-down, per cui riprendendo quanto detto sopra con il focus per l'ipotesi di attacco DDoS, possiamo suddividere lo scenario di rischio in sottocategorie più specifiche che riflettano le possibili conseguenze e gli obiettivi dell'attaccante:

Interruzione dei servizi critici → L'attacco mira a sovraccaricare i server o le reti dell'azienda, causando l'interruzione dei servizi critici offerti ai clienti. Questo potrebbe includere l'impossibilità di accedere al sito web aziendale, ai servizi cloud o alle applicazioni aziendali, compromettendo la continuità operativa dell'azienda e danneggiando la sua reputazione.

Perdita di dati sensibili → L'attacco potrebbe essere utilizzato come diversivo per mascherare altri tentativi di violazione della sicurezza, come l'accesso non autorizzato ai dati sensibili dell'azienda. In questo caso, lo scenario di rischio potrebbe includere la perdita o il furto di informazioni finanziarie, dati personali dei clienti o proprietà intellettuale dell'azienda, con conseguenze finanziarie e legali significative.

Impatto finanziario → Un attacco DDoS che causa un'interruzione prolungata dei servizi aziendali potrebbe avere un impatto significativo sul fatturato annuo dell'azienda, con perdite economiche dovute alla mancata erogazione dei servizi, alla perdita di clienti e alla necessità di investire risorse aggiuntive per mitigare gli effetti dell'attacco.

Degrado della reputazione → Un attacco DDoS di successo potrebbe danneggiare la reputazione dell'azienda agli occhi dei clienti, dei partner commerciali. Lo scenario di rischio potrebbe quindi includere il rischio di perdere la fiducia dei clienti, di subire un calo delle vendite e di essere oggetto di pubblicità negativa, con ripercussioni a lungo termine sulla posizione competitiva dell'azienda nel mercato.

ANALISI DEL RISCHIO QUALITATIVA O SEMI-QUANTITATIVA

L'analisi qualitativa si concentra su valutazioni soggettive. In questo caso, non avendo a disposizione dati quantitativi accurati, possiamo utilizzare la scala di Likert (1=molto basso, 5=molto alta) per un'analisi del rischio qualitativo, dove il rischio è stimato come la relazione tra la stima della verosimiglianza e la stima dell'impatto.

Scenario di rischio 1 : Interruzione dei servizi IT a causa di un attacco DDoS.

Verosimiglianza: 2 (Bassa) - Sebbene gli attacchi DDoS siano una minaccia esistente, le misure di sicurezza implementate possono ridurre significativamente la probabilità di successo di un attacco.

Impatto: 4 (Alto) - Anche se la probabilità di un attacco DDoS è bassa, le conseguenze di un'interruzione dei servizi IT sarebbero significative per l'azienda e i suoi clienti.

Scenario di rischio 2: Compromissione della reputazione aziendale a seguito di una violazione della sicurezza dei dati.

Verosimiglianza: 3 (Media) - Date le minacce esistenti nel panorama della sicurezza informatica, c'è una probabilità moderata che si verifichi una violazione della sicurezza dei dati.

Impatto: 4 (Alto) - La perdita di reputazione è un rischio significativo per TechnoCorp e potrebbe avere conseguenze finanziarie a lungo termine.

Dopo aver assegnato i punteggi di Likert per la verosimiglianza e l'impatto di ciascuno scenario di rischio, possiamo valutare il rischio complessivo moltiplicando i due punteggi. Ad esempio, per il primo scenario di rischio, con attacco DDoS il punteggio è: Verosimiglianza x Impatto = 2 x 4 = 8. Per il secondo è, 3 x 4 = 12

Questo approccio ci consente di valutare il rischio complessivo in base alla sua probabilità e al suo potenziale impatto, consentendoci di identificare e prioritizzare le azioni di mitigazione necessarie.

Sara Spaccialbelli