RISK MANAGEMENT

ASSET ORGANIZZATIVI, MINACCE E VULNERABILITÀ

MARIA HUAPAYA

INDICE

TRACCIA

Un’azienda vi ha incaricato di svolgere un’analisi delle vulnerabilità e delle minacce sui propri asset organizzativi. L’azienda opera nel settore metalmeccanico, produzione di ingranaggi, ha circa 200 impiegati ed un proprio e-commerce. Sono presenti circa 200 pc (1.000 €/pc) e 30 server (3.000 €/server). I servizi di cui dispone sono: sito e-commerce (fatturato 10.000 €/giorno), ERP di gestione aziendale (30.000€), server di posta elettronica (5.000€) e un sistema di sicurezza composto da firewall, IDS e SIEM di (25.000€).
Nella gestione del rischio, l’identificazione degli asset, l’analisi delle minacce e delle vulnerabilità avviene in contemporanea e si integrano a vicenda.

Creare un report in cui includere:

1. Identificazione e valore degli asset
2. Analisi delle vulnerabilità
3. Analisi delle minacce

Siete liberi di estendere ed ipotizzare lo scenario, il numero di asset da cui partire è a vostra scelta.
Potete utilizzare qualsiasi supporto come CVE, CVSS, tabelle NIST SP 800-30, ecc.

INTRODUZIONE

1.1 Presentazione dell’azienda

L’azienda in questione è la “MetalGear S.p.A.”, un’importante realtà nel settore metalmeccanico con sede in Italia. Fondata nel 1980, MetalGear S.p.A. si è specializzata nella produzione di ingranaggi di alta qualità utilizzati in una vasta gamma di settori, tra cui l’automobilistico, l’aerospaziale e l’industriale. Con circa 200 impiegati, l’azienda ha costruito una solida reputazione per la qualità dei suoi prodotti e l’eccellenza del suo servizio clienti.

1.2 Descrizione del contesto

MetalGear S.p.A. opera in un ambiente altamente tecnologico e competitivo. Per rimanere competitiva, l’azienda ha investito significativamente nella digitalizzazione dei suoi processi aziendali e nella creazione di un robusto e-commerce per servire i suoi clienti in tutto il mondo. L’infrastruttura IT dell’azienda comprende circa 200 personal computer (valore unitario di 1.000 €) e 30 server (valore unitario di 3.000 €) che supportano una serie di servizi critici. Tra questi, il sito di e-commerce (che genera un fatturato di 10.000 € al giorno), un sistema ERP per la gestione aziendale (valore di 30.000 €), un server di posta elettronica (valore di 5.000 €) e un sistema di sicurezza composto da firewall, IDS e SIEM (valore di 25.000 €).

1.3 Obiettivi del report

Illustrare chiaramente gli obiettivi dell'analisi, che includono l'identificazione e la valutazione degli asset critici, l'analisi delle vulnerabilità presenti e delle minacce potenziali, al fine di migliorare le strategie di sicurezza aziendale.

IDENTIFICAZIONE E VALORE DEGLI ASSET

2.1 Cosa sono gli asset

Gli asset in un contesto di sicurezza informatica si riferiscono a qualsiasi risorsa di valore per l'organizzazione che deve essere protetta. Questi possono includere hardware fisico come computer e server, software come applicazioni e database, dati aziendali e informazioni sensibili, servizi online come l'e-commerce e l'infrastruttura di rete, tra gli altri.

2.2 Elenco degli asset dell'azienda

Nel contesto di MetalGear S.p.A., gli asset identificati includono:

- Computer: circa 200 personal computer utilizzati dai dipendenti per le operazioni quotidiane.
- Server: 30 server che ospitano vari servizi e applicazioni.
- Sito e-commerce: un sito di e-commerce che genera un fatturato significativo per l'azienda.
- ERP di gestione aziendale: un sistema ERP (Enterprise Resource Planning) utilizzato per la gestione delle operazioni aziendali.
- Server di posta elettronica: un server dedicato alla gestione della posta elettronica aziendale.
- Sistema di sicurezza: un sistema di sicurezza composto da firewall, IDS (Intrusion Detection System) e SIEM (Security Information and Event Management).

2.3 Valutazione del valore degli asset

La valutazione del valore degli asset è un passaggio cruciale nell'analisi del rischio. Il valore di un asset non è solo il suo costo fisico, ma include anche il costo di sostituzione o riparazione, il valore dei dati o delle informazioni che contiene, l'impatto sulla reputazione dell'azienda in caso di perdita o compromissione, e altri fattori correlati. nel contesto di MetalGear S.p.A., i valori degli asset sono i seguenti:

- Computer: 200 unità x 1.000 €/unità = 200.000 €
- Server: 30 unità x 3.000 €/unità = 90.000 €
- Sito e-commerce: fatturato di 10.000 €/giorno. Il valore di questo asset può essere molto più elevato considerando l'impatto sulla reputazione e la perdita di affari in caso di interruzione del servizio.

- ERP di gestione aziendale: 30.000 €
- Server di posta elettronica: 5.000 €
- Sistema di sicurezza: 25.000 €

ANALISI DELLE VULNERABILITÀ

3.1 Cosa sono le vulnerabilità

Le vulnerabilità sono debolezze o difetti in un sistema, in una procedura o in un controllo di sicurezza che, se sfruttati da una minaccia, possono portare a un impatto negativo sull'organizzazione. Le vulnerabilità possono essere di natura tecnica (ad esempio, un bug in un software), organizzativa (ad esempio, procedure di sicurezza insufficienti) o fisica (ad esempio, accesso fisico non protetto a un server).

3.2 Metodologia di analisi delle vulnerabilità

L'analisi delle vulnerabilità adottata da MetalGear S.p.A. si basa su un approccio metodico e strutturato, che combina diverse tecniche e strumenti per garantire una copertura completa. Inizialmente, scanner di vulnerabilità automatizzati vengono utilizzati per esaminare sistemi informatici alla ricerca di vulnerabilità conosciute. Questi strumenti eseguono una scansione delle reti aziendali, identificando le debolezze a livello di software e hardware. Successivamente, test di penetrazione manuali mettono alla prova la robustezza delle difese esistenti, simulando attacchi cyber contro i sistemi aziendali per scoprire vulnerabilità non ancora note o non rilevate dagli scanner automatici. Una revisione manuale delle configurazioni di sistema e del codice sorgente consente di identificare lacune potenziali nelle policy di sicurezza e nelle pratiche di programmazione. Infine, la consultazione dei database pubblici di vulnerabilità, in particolare il Common Vulnerabilities and Exposures (CVE) e il National Vulnerability Database (NVD), fornisce informazioni aggiornate sulle vulnerabilità note e le relative soluzioni

3.3 Risultati dell'analisi delle vulnerabilità

Dai risultati, presentati nella "Tabella delle Vulnerabilità Identificate" allegata, emerge che:

- La vulnerabilità SQL Injection nei server ERP potrebbe avere un costo di riparazione e ripristino dati di 1.000 € per server, con un totale di 30.000 € per tutti i 30 server (1.000 € x 30 server).

- Per l'aggiornamento dei sistemi operativi dei computer, con 200 unità da aggiornare e un costo di 500 € per sistema, si arriva a un costo totale di 100.000 € (500 € x 200 computer).

Tabella delle Vulnerabilità Identificate

Asset	Vulnerabilità	Descrizione	Impatto Potenziale	Azioni di Mitigazione Raccomandate
Server ERP	CVE-XXXX-XXXX	Vulnerabilità a SQL Injection	Alto	Patch immediato del software
Sito E-commerce	Configurazione non sicura	Server web esposti a attacchi DDoS	Medio	Implementazione di servizi Anti DDoS
Computer	Sistema operativo obsoleto	Mancanza di supporto e aggiornamenti di sicurezza	Alto	Aggiornamento a versioni supportate

ANALISI DELLE MINACCE

4.1 Cosa sono le minacce

Una minaccia in termini di sicurezza informatica è un evento potenziale che può causare un impatto negativo sugli asset di un'organizzazione. Le minacce possono essere intenzionali, come gli attacchi informatici, o non intenzionali, come errori umani o disastri naturali.

4.2 Metodologia di analisi delle minacce

Parallelamente, l'analisi delle minacce viene condotta con un processo strutturato per valutare potenziali pericoli che potrebbero sfruttare le vulnerabilità rilevate.

La raccolta di dati avviene attraverso fonti di intelligence sulle minacce, che offrono indicazioni su nuovi vettori di attacco e metodi operativi degli aggressori. Le tendenze di sicurezza emergenti forniscono contesto e aiutano a predire possibili evoluzioni nel panorama delle minacce. I database di vulnerabilità e gli archivi degli incidenti noti sono esaminati per comprendere le correlazioni tra vulnerabilità specifiche e gli attacchi reali che hanno avuto successo in passato. La conoscenza interna e il feedback dai team di sicurezza sono impiegati per personalizzare l'analisi in base all'ambiente specifico di MetalGear S.p.A., mentre le ricerche su potenziali attori di minaccia offrono insight sui motivi e le capacità degli avversari. Test di penetrazione aggiuntivi vengono eseguiti per valutare la reattività dell'organizzazione di fronte a minacce simulate.

4.3 Risultati dell'analisi delle minacce

Secondo la "Tabella delle Minacce Identificate" allegata, i costi di mitigazione stimati includono:

- Per il phishing, soluzioni di sicurezza anti-phishing per 5.000 € e formazione del personale per 15.000 €, sommando a un totale di 20.000 €.
- Per gli attacchi DDoS al sito e-commerce, il costo di implementazione delle soluzioni di mitigazione è stimato in 50.000 €.
- La prevenzione della perdita di dati, con soluzioni DLP implementate sui 30 server, ha un costo stimato di 40.000 € (1.000 € per server più costi operativi).

Tabella delle Minacce Identificate

Minaccia	Descrizione	Probabilità	Contromisure	Costo Mitigazione
Phishing	Email ingannevoli per furto di credenziali	Alta	Formazione dei dipendenti, filtri email	Medio
Attacchi DDoS	Sovraccarico del sito E-commerce	Media	Soluzioni di mitigazione DDoS	Alto
Perdita di dati	Furto di dispositivi portatili o data breach	Bassa	Crittografia, controllo degli accessi	Alto

CONCLUSIONI

5.1 Sintesi dei risultati

La presente sezione riassume i risultati delle approfondite analisi delle vulnerabilità e delle minacce condotte per MetalGear S.p.A., le quali rivelano esposizioni significative a rischi informatici. Le principali vulnerabilità, elencate nella "Tabella delle Vulnerabilità Identificate", includono sistemi operativi obsoleti sui computer aziendali e configurazioni non sicure sui server, che richiedono immediati aggiornamenti e patch. Tra le minacce più rilevanti, evidenziate nella "Tabella delle Minacce Identificate", vi sono attacchi DDoS mirati al sito e-commerce, che potrebbero portare a interruzioni del servizio e perdite economiche, e campagne di phishing contro i dipendenti, che rischiano di compromettere dati sensibili.

5.2 Raccomandazioni per la mitigazione dei rischi

Sulla base dei dati analizzati, si consigliano i seguenti interventi per mitigare i rischi identificati:

- Aggiornamenti e Patch Management: E' essenziale stabilire una politica di aggiornamento regolare e sistematico per tutti i sistemi operativi e le applicazioni, per correggere tempestivamente le vulnerabilità note.
- Formazione sulla Sicurezza: Fondamentale è anche organizzare sessioni di formazione continue per tutti i dipendenti, allo scopo di migliorare la consapevolezza sui rischi di sicurezza, come il riconoscimento di attacchi di phishing e l'adozione di comportamenti sicuri online.
- Soluzioni Anti-DDoS: Per proteggere l'infrastruttura critica come il sito e-commerce, si raccomanda l'adozione di soluzioni avanzate di mitigazione DDoS, che possano assorbire e neutralizzare il traffico malevolo.
- Backup e Ripristino: Implementare una strategia di backup e ripristino affidabile per garantire la salvaguardia e il recupero dei dati in caso di incidenti, inclusi attacchi ransomware.
- Risposta agli Incidenti: Sviluppare un piano di risposta agli incidenti che includa protocolli chiari e procedure di emergenza per una risposta rapida ed efficace in caso di attacchi informatici.

GRAZIE

MARIA HUAPAYA