BCC Iccrea - Progetto
S1/L2
Sara Spaccialbelli

ASSET ORGANIZZATIVI, MINACCE E VULNERABILITA’

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: sitoe-commerce (fatturato10.000 €/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.

Report:
1-Identificazione e valore degli asset

Hardware:

200 PC (valore stimato: 1.000 €/pc) 200 x 1.000 = 200.000 €

30 Server (valore stimato: 3.000 €/server) 30 x 3.000 = 90.000 €

Servizi:

Sito e-commerce (fatturato 10.000 €/giorno) 10.000€ x 365 = 3.650.000€ all'anno

ERP di gestione aziendale (valore stimato: 30.000 €)

Server di posta elettronica (valore stimato: 5.000 €)

Sistema di sicurezza (firewall, IDS, SIEM) (valore stimato: 25.000 €)

Personale:

200 impiegati

- **Totale PC e Server = 290.000€**
- **Totale Servizi all'Anno = 3.710.000€**

Approccio alla Valutazione:

PC e Server: Questi asset sono valutati in base al costo di sostituzione. Se tutti i PC/server dovessero essere persi o danneggiati, il costo di sostituzione sarebbe quello calcolato.

Servizi: I servizi come il sito e-commerce, l'ERP, il server di posta e il sistema di sicurezza sono valutati in base al loro contributo al fatturato annuo dell'azienda.

2-Analisi delle vulnerabilità

CVE (Common Vulnerabilities and Exposures)
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, + l’utilizzo di strumenti di scansione per identificare e correggere le vulnerabilità.

CVE-2021-31174	Microsoft Excel Information Disclosure Vulnerability **Published:** May 11, 2021; 3:15:09 PM -0400	*V3.1:* **5.5 MEDIUM** *V2.0:* **2.1 LOW**

2-Analisi delle vulnerabilità

Password Deboli sui PC e Server:
Rischio di accesso non autorizzato.
Valutazione: Alta
Impatto: Possibile compromissione dei dati sensibili.
Priorità di Mitigazione: Alta
Possibile Mitigazione:
Implementazione di politiche di password robuste.
Richiesta di cambiamento periodico delle password.

CVE-2023-32784	In KeePass 2.x before 2.54, it is possible to recover the cleartext master password from a memory dump, even when a workspace is locked or no longer running. The memory dump can be a KeePass process dump, swap file (pagefile.sys), hibernation file (hiberfil.sys), or RAM dump of the entire system. The first character cannot be recovered. In 2.54, there is different API usage and/or random string insertion for mitigation. **Published:** May 15, 2023; 2:15:10 AM -0400	*V3.1:* **7.5 HIGH** *V2.0:*(not available)

2-Analisi delle vulnerabilità

Mancanza di Backup Regolari:
Rischio di perdita di dati critici in caso di incidente.
Valutazione: Alta
Impatto: Potenziale interruzione delle attività.
Priorità di Mitigazione: Media
Possibile Mitigazione:
Implementazione di backup regolari e test di ripristino.
Conservazione dei backup in un luogo sicuro e fuori sede.

3-Analisi delle minacce

Tipo di Minaccia	Descrizione	Vettore di Attacco	Fonte della Minaccia	Probabilità (Prima)	Controllo di Mitigazione e Costo	Probabilità (Dopo)
Phishing	Tentativo di ottenere informazioni sensibili tramite ingegneria sociale	Email, Siti Web Falsi	Attaccante Esterno	Media	Sensibilizzazione dei Dipendenti	Bassa
Ransomware	Software malevolo che blocca l'accesso ai dati fino al pagamento di un riscatto	Email, Download di File Infetti	Attaccante Esterno	Alta	Backup Regolari e Anti-Ransomware	Media

3-Analisi delle minacce

Tipo di Minaccia	Descrizione	Vettore di Attacco	Fonte della Minaccia	Probabilità (Prima)	Controllo di Mitigazione e Costo	Probabilità (Dopo)
Furti Fisici	Furto o smarrimento fisico di dispositivi contenenti dati sensibili	Smarrimento, Furto	Attaccante Esterno/Interno	Media	Sicurezza Fisica (Lucchetti, Accesso Controllato)	Bassa
Malware	Software malevolo progettato per danneggiare, rubare o controllare un sistema	Download di File Infetti, USB Infetti	Attaccante Esterno	Alta	Antivirus e Antimalware	Bassa
Vulnerabilità del Software	Esposizione a vulnerabilità nel software non corrette da patch	Exploit di Vulnerabilità, Codice Malevolo	Attaccante Interno/Esterno	Alta	Gestione delle Patch	Media

ISO 27005 –Annex C –Esempi di minacce tipiche

A = accidentale, D = deliberato, B = ambientale

Tipo di Danno	Minaccia	Origine (A/D/B)	Descrizione
Fisico	Incendio	A	Rischio di incendio negli ambienti di produzione a causa di cortocircuiti o guasti elettrici.
Naturale	Tempesta	B	Danneggiamento delle strutture e interruzioni delle attività a causa di tempeste e venti forti.
Tecnologico	Interruzione Connessione	A	Interruzione della connessione internet, con conseguente blocco delle operazioni online.
Umano	Accesso non Autorizzato	D	Tentativi deliberati di accesso non autorizzato ai sistemi interni da parte di personale interno o esterno.

Grazie

Sara Spaccialbelli