## ESERCIZIO BONUS S9 L5

## TRACCIA:

Siete chiamati a progettare le difese di questo scenario:

L'Azienda Mak produce dei macchinari e il cliente vuole mettere in sicurezza tutto l'ecosistema.
Abbiamo da una parte l'azienda Mak, poi c'è il macchinario e dall'altra parte c'è il cliente che lo utilizza.
Il macchinario è bastato su Windows 10, ha porta di rete (usata solo per gli aggiornamenti e la diagnostica remota), porta USB (sono disabilitate le pendrive, ovviamente).
La diagnostica remota è fatta attraverso la VPN del cliente, il macchinario è sostanzialmente bloccato – La partizione del sistema operativo non è scrivibile mentre c'è una seconda partizione per il software di gestione del macchinario.
Il software di gestione è realizzato con il linguaggio C99.
Il macchinario è installato nelle varie aziende clienti.

## *Consegna:*

1. Valutare le eventuali vulnerabilità e punti di attacco

2. Proporre al cliente soluzioni di sicurezza Esercizio Bonus

3. Progettare un sistema di monitoraggio del traffico (Windows 10 è bloccato dalla casa madre, non è modificabile). Proponente al cliente due soluzioni, una economica (massimo 500 euro) e una più costosa (massimo 2500 euro) Eventuali altre specifiche richieste (non specificate) potete inventarle.

## *SVOLGIMENTO:*

Per affrontare questa richiesta aziendale, dividerò la risposta in tre sezioni principali:

1. **Valutazione delle vulnerabilità e punti di attacco**
2. **Proposte di soluzioni di sicurezza**
3. **Progettazione di un sistema di monitoraggio del traffico**

### 1. Valutazione delle vulnerabilità e punti di attacco

**Punti di attacco principali:**

- **Rete (porta di rete):**
  La connessione di rete viene utilizzata per aggiornamenti e diagnostica remota tramite VPN, ma rimane un potenziale punto di attacco. Se la VPN non è configurata correttamente o se ci sono vulnerabilità nel sistema di autenticazione, un attaccante può sfruttare l'accesso remoto per infiltrarsi nel sistema.

- **Software di gestione:**
  Il software di gestione del macchinario è sviluppato in C99, il che potrebbe essere un potenziale rischio se non è stato adeguatamente testato per vulnerabilità come buffer overflow, iniezione di codice, o problemi legati alla gestione della memoria.
  Se il software non fosse regolarmente aggiornato, potrebbe contenere vulnerabilità note che potrebbero essere sfruttate da un attaccante.

- **Porta USB**
  Sebbene le pendrive siano disabilitate, è possibile che ci siano altre modalità di interazione tramite USB, come dispositivi di

diagnostica, periferiche, o strumenti di gestione che potrebbero essere vulnerabili a exploit fisici.

- **Sistema operativo Windows 10**
  Windows 10 è bloccato dalla casa madre, ma potrebbe comunque essere vulnerabile a exploit noti, specialmente se non vengono applicati aggiornamenti di sicurezza regolari. Anche con la partizione di sistema non scrivibile, eventuali vulnerabilità potrebbero essere sfruttate tramite il software di gestione del macchinario o attraverso altre applicazioni che interagiscono con il sistema operativo.

- **VPN**
  La VPN utilizzata per la diagnostica remota potrebbe essere soggetta ad attacchi di tipo Man-in-the-Middle (MitM) se non è implementata con protocolli sicuri come OpenVPN o IPsec. Inoltre, se l'autenticazione della VPN non è configurata correttamente (ad esempio, utilizzo di credenziali deboli), gli attaccanti potrebbero compromettere la connessione remota.

**2. Proposte di soluzioni di sicurezza**

**Soluzione economica (fino a 500 euro):**

1. **Rafforzamento della VPN:**

- **Protocolli sicuri**: Assicurarsi che la VPN utilizzi protocolli sicuri come OpenVPN o IPsec con crittografia forte (AES-256).
- **Autenticazione multifattoriale**: Implementare l'autenticazione multifattoriale per l'accesso remoto tramite la VPN. Ad esempio, utilizzare un’app di autenticazione basata su token (come Google Authenticator) per aggiungere un ulteriore strato di sicurezza.
- **Controllo delle sessioni VPN**: Limitare l'accesso alla VPN solo agli indirizzi IP aziendali o a un elenco di host predefiniti.

2. **Antivirus e Firewall per il macchinario**

- **Antivirus**: Installare un antivirus economico che possa rilevare e prevenire attacchi malware sul macchinario. Esistono soluzioni con licenze mensili o annuali che rientrano nel budget.
- **Firewall Windows 10**: Configurare correttamente il firewall di Windows per limitare il traffico non autorizzato e bloccare le porte non necessarie.

3. **Aggiornamenti e gestione dei software**

- **Aggiornamenti regolari**: Verificare che tutti i software di gestione e il sistema operativo siano sempre aggiornati con le patch di sicurezza. Questo può essere automatizzato, così da evitare vulnerabilità note.
- **Gestione delle vulnerabilità**: Utilizzare strumenti di scansione delle vulnerabilità (come ***Nessus***, versione gratuita) per analizzare il software di gestione e il sistema operativo.

4. **Controllo degli accessi USB**

- Utilizzare un software che disabiliti il supporto per dispositivi USB non autorizzati, come la gestione tramite Group Policy di Windows, oppure tramite software di terze parti (ad esempio, "USB Block").

---

**Soluzione più costosa (fino a 2500 euro):**

1. **Sistemi di Intrusion Detection (IDS)**

- **Sistemi IDS/IPS**: Implementare una soluzione di Intrusion Detection/Prevention System, come Snort, Suricata o una soluzione commerciale (ad esempio, Cisco Firepower o Palo Alto). Questi sistemi possono monitorare e bloccare attacchi in tempo reale sulla rete, rilevando anomalie o attività sospette.

2. **Monitoraggio e auditing delle connessioni VPN**

- Implementare un sistema di monitoraggio delle connessioni VPN, per tenere traccia degli accessi remoti. Strumenti come **Splunk** o **ELK Stack,** possono essere usati per centralizzare i log, monitorare e generare avvisi in caso di attività sospette.

3. **Sicurezza a livello di endpoint**

- **Endpoint Detection and Response (EDR)**: Implementare una soluzione EDR, come CrowdStrike o SentinelOne, per monitorare in tempo reale e bloccare comportamenti dannosi sul macchinario, fornendo anche funzionalità di indagine post-incidente.

4. **Controllo USB avanzato**

- Soluzioni di gestione avanzata degli accessi USB che possano limitare ulteriormente l'accesso fisico. Una soluzione come **Device Control** di McAfee può permettere di impostare policy come il blocco di periferiche USB non aziendali o la registrazione di ogni dispositivo USB connesso.

5. **Backup sicuro e resilienza**

- **Backup crittografato**: Creare backup periodici crittografati delle partizioni di gestione del macchinario. Utilizzare soluzioni come **Veeam** o **Acronis** che consentano di eseguire backup sicuri e facili da ripristinare in caso di incidente.
- **Piano di recupero in caso di disastro**: Stendere e testare un piano di recupero in caso di disastro (DRP), che includa il ripristino delle configurazioni e dei dati critici in caso di attacco.

---

**3. Progettazione di un sistema di monitoraggio del traffico**

**Soluzioni proposte**:

1. **Soluzione Economica (fino a 500 euro):**

- **Wireshark (gratuito)**: Utilizzare Wireshark per il monitoraggio del traffico di rete, limitato agli aggiornamenti e alla diagnostica remota. Può essere configurato per analizzare specifici protocolli e identificare traffico sospetto.
- **Sysmon (gratuito)**: Installare Sysmon per raccogliere informazioni dettagliate sui processi di sistema, file e connessioni di rete. I log possono essere inviati a un server centralizzato per l'analisi.

2. **Soluzione Costosa (fino a 2500 euro)**

- **Palo Alto Networks (o alternativa)**: Una soluzione come Palo Alto Networks o Cisco potrebbe essere implementata per monitorare il traffico di rete in tempo reale, analizzando il flusso di dati e rilevando attività sospette o potenziali minacce.
- **Splunk**: Implementare Splunk per raccogliere e analizzare i log di rete e del sistema, con il supporto di algoritmi di machine learning per identificare comportamenti anomali. Può essere utilizzato anche per analizzare i log della VPN e del traffico remoto.

---

## *Conclusioni:*

- La **soluzione economica** si concentra su strumenti di monitoraggio di base e sull'implementazione di misure di sicurezza efficaci, come la configurazione della VPN e la gestione delle USB.
- La **soluzione costosa** offre protezioni avanzate come sistemi di rilevamento delle intrusioni, monitoraggio avanzato del traffico e

protezione endpoint, per garantire una difesa robusta contro le minacce.

Entrambe le soluzioni dovrebbero essere adeguate in base al budget e alle esigenze specifiche dell’azienda cliente.