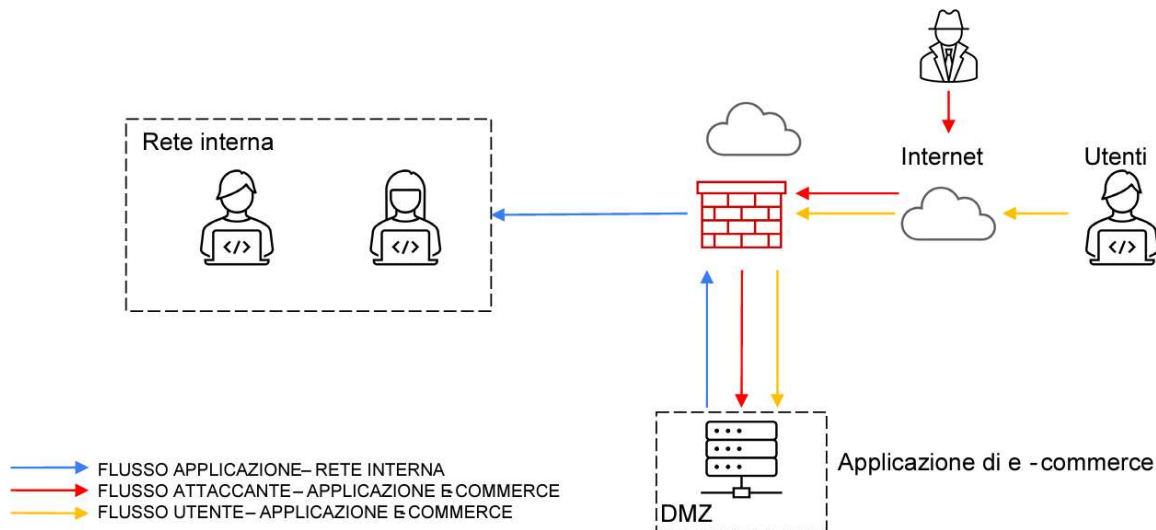


# PROGETTO S9/L5

## Architettura di rete:

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

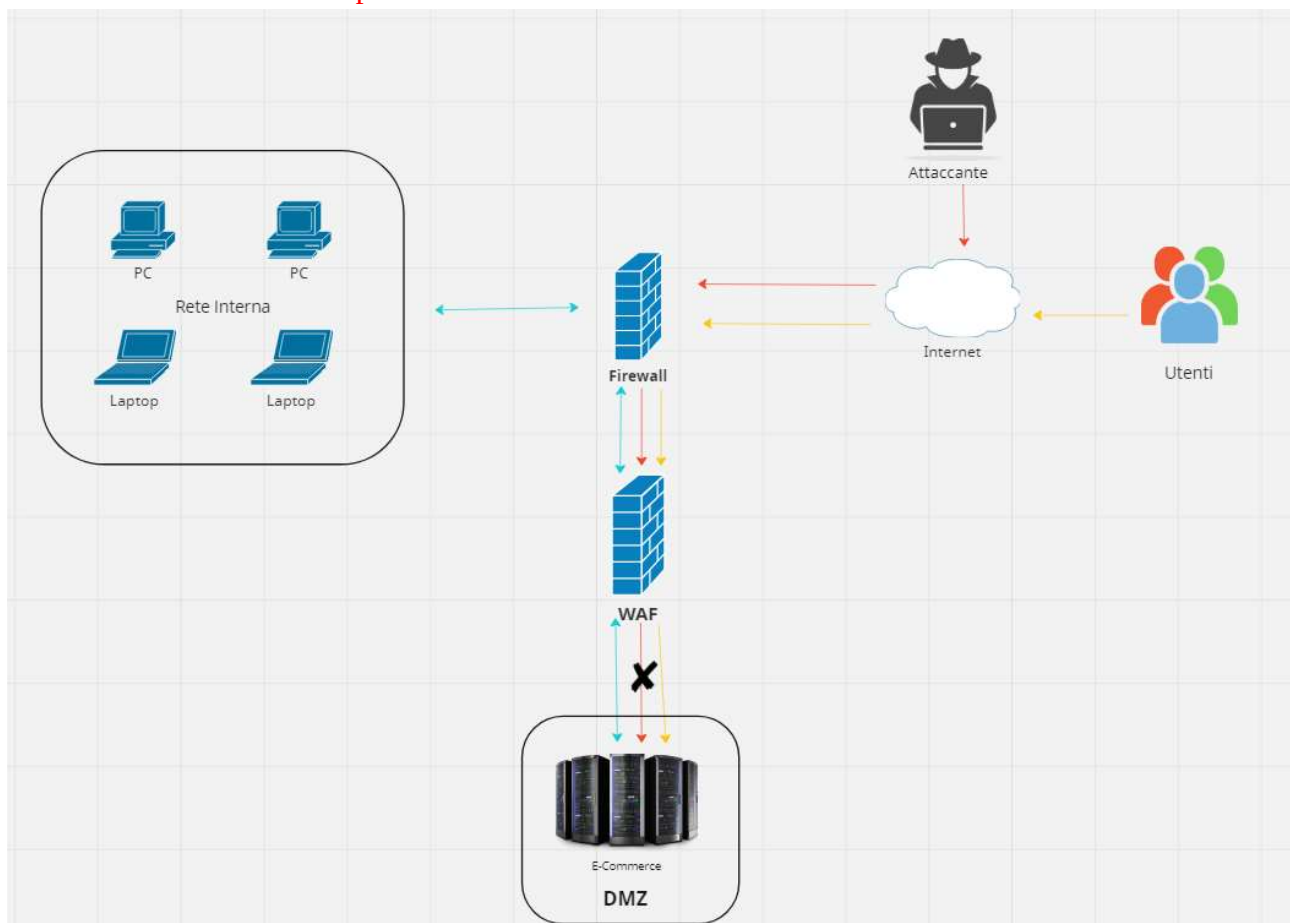
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



3

1. **Azioni preventive** : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?  
Modificate la figura in modo da evidenziare le implementazioni

Grafico modificato e Risposta:



Generalmente per limitare queste tipologie di attacchi come l'SQL Injection o il Cross-Site Scripting è necessario implementare un WAF ossia un Web Application Firewall che se configurato correttamente, è in grado di filtrare ed analizzare il traffico di rete indirizzato alla web application, bloccandolo completamente nel caso riconosca pacchetti contenenti alcuni caratteri o codice malevolo in grado di sferrare un attacco SQLi o XSS.

2. **Impatti sul business** : l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti** .  
Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** sulla piattaforma di e-commerce . **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**

**Risposta:**

In questo caso, a seguito di un attacco DDoS all'applicazione Web, se si considera che ogni minuto gli utenti spendono in media 1500€ sulla piattaforma, basta moltiplicare questo dato per i minuti di disservizio dell'applicazione per ricavare l'impatto economico subito dall'azienda,

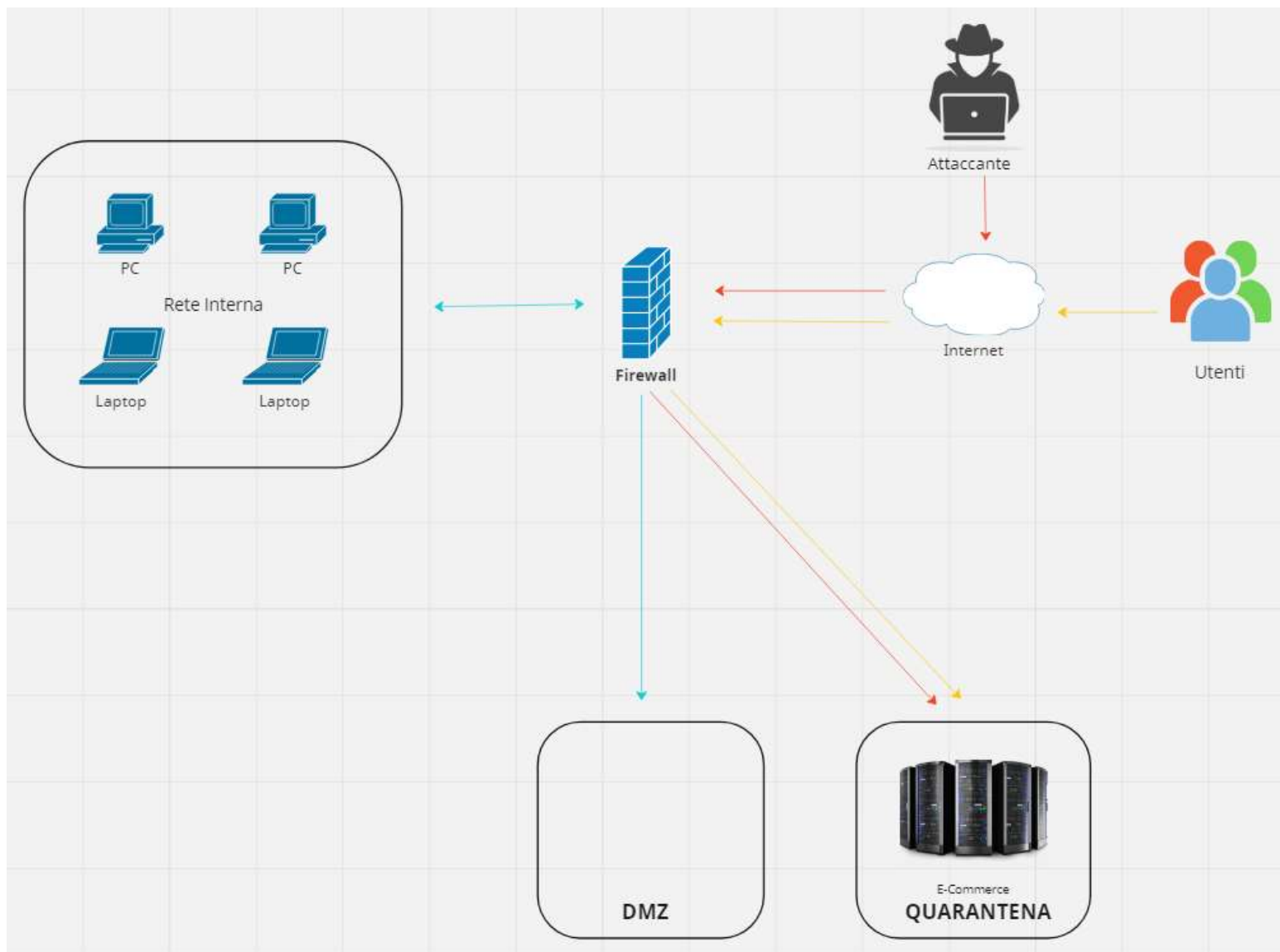
quindi:

$$1500€ \times 10 \text{ minuti} = 15000€$$

Tra le azioni preventive che si possono applicare per limitare un eventuale attacco DDoS vi è l'implementazione di alcuni specifici servizi di protezione da questa tipologia di attacchi, che in alcuni casi sono già presenti all'interno di Firewall avanzati tramite la corretta configurazione di regole specifiche relative all'origine del traffico di rete e alla quantità di pacchetti in ingresso e dettagliata analisi, o attraverso la sottoscrizione di servizi di piattaforme come Cloudflare o FortiNet, o Microsoft Azure per esempio, che mettono a disposizione soluzioni specifiche come la mitigazione DDoS.

3. **Response** : l'applicazione Web viene infettata da un malware .  
La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.  
Modificate la figura in slide 2 con la soluzione proposta .

**Grafico modificato e risposta:**



In questo caso, seguendo la traccia, è stato scelto di isolare parzialmente l'applicazione web in una rete di quarantena, "filtrata" dal Firewall pre-esistente ma comunque raggiungibile dagli utenti così come dall'attaccante. Questo scenario non è comunque il più indicato, in quanto pur avendo salvaguardato la rete interna da potenziali altri attacchi, si sta lasciando la possibilità all'attaccante di continuare potenzialmente a recuperare dati sensibili dalla web app già compromessa o di provare altri attacchi che richiedono tempo per la riuscita, come nel caso di un Bruteforce. Potrebbe però essere utile nel caso in cui si voglia far credere all'attaccante di poter continuare ad agire indisturbato mentre si sta cercando di recuperare tracce o lasciare "trappole" per risalire alla sua identità.

#### 4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

##### Risposta:

In realtà una volta configurato il WAF, l'attaccante perderebbe comunque la possibilità di accedere alla web App, quindi a meno che non venga configurato in modo tale da rendere comunque possibile l'accesso solo dall'attaccante alla rete di quarantena e rendere comunque possibile lo scenario visto nel punto 3.

5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2)

**Risposta:**

Per rendere più aggressiva tutta l'infrastruttura sarebbe necessario sicuramente l'implementazione di diverse misure di sicurezza e servizi in aggiunta per prevenire e gestire in maniera adeguata un potenziale attacco all'azienda.

Innanzitutto sarebbe utile una migliore "segmentazione" della rete aziendale in diverse LAN e VLAN per rete ospiti correttamente configurate e gestite da Firewall perimetrali per poter isolare meglio uno specifico servizio o dispositivo in caso di compromissione da un attacco esterno ed evitare così eventuali altri attacchi a catena su altre macchine e/o servizi.

Secondariamente, ci sono diversi servizi che possono essere implementati per gestire e limitare i danni, tra questi:

- L'implementazione di un IPS/IDS ossia un sistema in grado di monitorare gli eventi relativi alla sicurezza in tempo reale e prevenire eventuali attacchi o segnalare attraverso alert immediati al sistemista di rete;

- L'implementazione come accennato prima di un WAF e di un Next Generation Firewall (NGFW) in grado di analizzare i flussi dati con un dettaglio maggiore, per esempio analizzando anche i livelli della pila ISO/OSI dei pacchetti dati;

- Effettuando regolari Penetration test sugli end-point presenti sulla rete aziendale;

- Aggiornando regolarmente i propri software e OS presenti sulle macchine aziendali mediante una corretta Patch Management;

- Implementando un sistema centralizzato di log SIEM/SOAR per monitorare costantemente e in real-time tutti gli asset e servizi aziendali e centralizzare e registrare i log provenienti da più sorgenti come Firewall, Proxy e i vari eventuali servizi Terzi a cui si appoggia l'azienda.

**BONUS**

**Bonus:**

Analizzare le seguenti segnalazioni caricate su anyrun e fare un **piccolo report** di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

<https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>

<https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

## Risposta:

Per quanto riguarda la prima segnalazione, si tratta di un file eseguibile, con nome:

PERFORMANCE\_BOOSTER\_v3.6.exe

The screenshot displays the ANY.RUN malware analysis platform. The top navigation bar includes the logo, the text 'ANALYZE MALWARE', and links to 'Huge database of samples and IOCs', 'Unlimited submissions', 'Custom VM setup', and 'Interactive approach'. A 'Sign up, it's free' button is also present.

The main content area is divided into two sections:

### General Info

**File name:** PERFORMANCE\_BOOSTER\_v3.6.exe  
**Full analysis:** <https://app.any.run/tasks/c03f447c-e6ca-4b9f-880a-017b3bd30f6e>  
**Verdict:** Malicious activity  
**Analysis date:** October 10, 2020 at 15:04:30  
**OS:** Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)  
**Indicators:**   
**MIME:** application/x-dosexec  
**File info:** PE32 executable (console) Intel 80386, for MS Windows  
**MD5:** 166903C9A390527CCD7728AE799A9D87  
**SHA1:** 2400F579ACC5B52C995230928EC5000DE6D807ED  
**SHA256:** 5E0D3D5A14069AB763731C7EB80922EF25F3EA081B9B2D961EFD25A743244C2A  
**SSDEEP:** 3072:mqFfhgTWmCRkGbKLeNTBfhUQOYsgHXzO/C08:F5aWbksiNTBZxMgHXo8

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

### Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Executes PowerShell scripts • cmd.exe (PID: 3624)	Uses ATTRIB.EXE to modify file attributes • cmd.exe (PID: 3624)	Reads Microsoft Office registry keys • regedit.exe (PID: 2784)
Runs PING.EXE for delay simulation • cmd.exe (PID: 3624)	Executed as Windows Service • vssvc.exe (PID: 896)	
	Starts CMD.EXE for commands execution • PERFORMANCE_BOOSTER_v3.6.exe (PID: 2616)	
	Reads default file associations for system extensions • regedit.exe (PID: 2784)	
	Reads Internet Cache Settings • regedit.exe (PID: 2784)	
	Creates files in the user directory • powershell.exe (PID: 2168)	
	Searches for installed software • regedit.exe (PID: 2784)	

Si tratta di uno Spyware che riesce a svolgere diverse attività critiche a livello di sistema tra cui:


- Eseguire Script PowerShell
- Recuperare informazioni sul Registro di Sistema
- Leggere i Software installati, la Internet Cache, le chiavi di registrazione per Microsoft Office
- Creare file all'interno della directory dell'utente.

Per la seconda segnalazione invece, si tratta di un file scaricabile da una fonte non attendibile che si camuffa da aggiornamento del browser Microsoft Edge:



## General Info

✓ Add for printing

URL: <https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE>  
Full analysis: <https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e>  
Verdict: **Malicious activity**  
Analysis date: February 08, 2024 at 18:37:44  
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)  
Indicators:   
MD5: C588D543062B963EA0BE6F0EF0130AED  
SHA1: BFE2CADDE63BE754783E8D725CCE54639B15BABA  
SHA256: 009163E614BEB5FEC5A8DAE5B31DFAFC613A2E3BAB9FBCE1DA8DA2EC8C778F90  
SSDEEP: 3:N8qDLIWkF80arQ+dWVqg:2qXylarQwZg

**ANY RUN** is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. **ANY RUN** does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

## Behavior activities

✓ Add for printing

### MALICIOUS

Drops the executable file immediately after the start

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

### SUSPICIOUS

Process drops legitimate windows executable

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Executable content was dropped or overwritten

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

Starts a Microsoft application from unusual location

- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Disables SEHOP

- MicrosoftEdgeUpdate.exe (PID: 4040)

Starts itself from another location

- MicrosoftEdgeUpdate.exe (PID: 4040)

Creates/Modifies COM task schedule object

- MicrosoftEdgeUpdate.exe (PID: 4012)

Creates a software uninstall entry

- MicrosoftEdgeUpdate.exe (PID: 4040)

### INFO

Executable content was dropped or overwritten

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Drops the executable file immediately after the start

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Application launched itself

- iexplore.exe (PID: 1632)

The process uses the downloaded file

- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)

Checks supported languages

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4012)
- MicrosoftEdgeUpdate.exe (PID: 4040)
- MicrosoftEdgeUpdate.exe (PID: 2436)
- MicrosoftEdgeUpdate.exe (PID: 2812)
- MicrosoftEdgeUpdate.exe (PID: 3408)
- MicrosoftEdgeUpdate.exe (PID: 3796)

Anche in questo caso si tratta di uno Spyware che può svolgere diverse attività critiche all'interno del sistema, tra cui:

- E' in grado di disattivare il seHOP (Structured Exception Handling Overwrite Protection), un tool integrato di Windows per proteggere il sistema da alcuni exploit che sfruttano la sovrascrittura SEH;
- Crea nei task nello scheduler di Windows;
- Può sovrascrivere o eliminare file di aggiornamento legittimi (Microsoft Edge)
- Recupera informazioni circa le impostazioni del browser, dei certificati scaricati e sul sistema operativo.

Per entrambi i casi, ci sono diversi accorgimenti che si possono intraprendere per evitare nuovi attacchi in futuro, tra cui:

-Implementare su tutti gli asset aziendali un sistema Anti-Virus aggiornato, che riconoscano non solo i malware dalla loro firma hash ma analizzandone il comportamento ed eventualmente bloccandone le funzionalità o informando l'utente.

-Introdurre il blocco del download di file eseguibili non autorizzati tramite Group Policy

-Evitare di scaricare file da fonti non sicure.