

STORMSHIELD

Come scegliere una soluzione di Endpoint Protection

EDR o HIPS: quale approccio per bloccare efficacemente i cyber-attacchi sofisticati?

White paper



Nonostante il tema della sicurezza informatica continui ad essere sotto i riflettori, i criminali informatici tentano di passare inosservati. Per questo motivo, hanno bisogno di aggiornare costantemente le loro tecniche di attacco. E poiché conoscono bene i meccanismi di difesa, cercano di sviluppare strumenti malevoli per ingannare le soluzioni di cybersicurezza presenti sulle postazioni di lavoro.

Gli antivirus convenzionali e altri sistemi di rilevamento, specialmente quelli basati esclusivamente sulle firme, sembrano essere superati da tecniche complesse, come sfruttare bug o misconfigurazioni di applicazioni legittime per l'acquisizione di privilegi più elevati, così come dalle tecniche di occultamento del codice malevolo. Pertanto, le soluzioni incentrate sul rilevamento e la prevenzione degli attacchi noti stanno diventando inadeguate per affrontare questa nuova generazione di sofisticati cyber-attacchi.

Per le aziende è indispensabile implementare ***soluzioni che analizzino in modo molto dettagliato il comportamento dei processi in esecuzione al fine di individuare potenziali minacce.*** *La soluzione scelta deve quindi essere in grado di rilevare e bloccare comportamenti anomali in modo proattivo, automatico e in tempo reale per garantire un'efficace protezione in tempo reale.*

Il presente white paper illustra i vari meccanismi che un sistema di protezione delle postazioni di lavoro e dei server deve adottare per svolgere la sua funzione di rilevamento delle minacce e protezione.

É destinato ai responsabili della sicurezza dei sistemi informatici, ai quali fornirà gli elementi necessari per sostenervi al meglio nel processo decisionale in base alle vostre esigenze.

Indice

1

Cyber-attacchi: modus operandi?

2

Analisi comportamentale delle soluzioni

3

Endpoint Detection & Response

Un ideale di sicurezza ?

4

Le diverse tecniche di protezione HIPS

4.1 Approccio basato su regole

4.2 Approccio contestuale

4.3 « Hardening »

5

Stormshield Endpoint Security Evolution

La soluzione di protezione delle postazioni di lavoro

Cyber-attacchi: modus operandi

Secondo l'ANSSI, tra il 2019 e il 2020, il numero di vittime di cyber-attacchi è aumentato di quattro volte. Da un rapporto del Senato francese[2], è emerso che i cyber-criminali ne hanno approfittato, portando a un aumento degli attacchi di phishing del 667% registrato tra il 1° e il 23 marzo 2020.

Inoltre, sebbene la consapevolezza degli utenti sia gradualmente migliorata, nessun sistema o infrastruttura può essere sicuro al 100%. Questo è il motivo per cui gli avversari trovano sempre nuove tecniche per violare i sistemi informatici di aziende di qualsiasi entità in modo sempre più efficace.

Il 91%

degli attacchi mirati viene effettuato con il metodo di spear phishing

Il loro obiettivo? Esfiltrare una copia di dati sensibili (medici, bancari, industriali, ecc.) e crittografare l'originale, di modo da poter chiedere un riscatto per la decifratura o, in caso di rifiuto da parte della vittima, minacciare la pubblicazione della copia esfiltrata esponendo l'azienda alle sanzioni previste in materia di trattamento del dato. In alcuni caso l'attacco ha come obbiettivo danneggiare la produttività dell'azienda presa di mira (sito di e-commerce, linee di produzione, ecc.). A tal fine, ggli avversari cercano di bypassare i sistemi di sicurezza attivi per ottenere l'accesso sfruttando, ad esempio, le vulnerabilità del software o dei dispositivi installati.

Per capire meglio come funziona un attacco informatico, ci concentreremo sulle tre fasi cruciali che permettono a un avversario di raggiungere il suo obiettivo finale. La fase iniziale sarà la compromissione di una macchina, guadagnando un accesso iniziale al sistema, potenzialmente senza privilegi elevati. Nella seconda fase, l'avversario cerca di raggiungere gli obbiettivi più sensibili ottenendo credenziali di account con privilegi elevati e infettando altre macchine nella rete. Nella terza fase, l'avversario può procedere all'attacco portando eseguendo le azioni di esfiltrazione e cifratura citate in precedenza.

Analizzeremo queste tre fasi in modo più dettagliato.

[2] http://www.senat.fr/rap/r20-678/r20-678_mono.html

FASE 1

SCOPERTA E INFEZIONE PRIMARIA



In primo luogo, i criminali informatici svolgono indagini per individuare le vittime all'interno dell'azienda bersaglio. Infatti, l'aggressore cerca di implementare vettori di attacco di tipo umano e/o tecnologico.

A livello umano, l'aggressore utilizza tecniche di social engineering (LinkedIn, Facebook, ecc.) per raccogliere informazioni da utilizzare nell'attacco al fine di renderlo quanto più efficacie.

Egli induce con l'inganno il destinatario ad aprire un allegato o a cliccare su un link web malevolo. Una tecnica nota per la sua efficacia: Il 91% degli attacchi mirati[2] viene effettuato con questo metodo di spear phishing (phishing mirato).

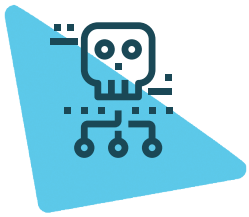
Ad esempio, l'attacco può prevedere che l'avversario si spacci per un mittente (istituto finanziario, fornitore, ecc.) noto alla persona presa di mira.

Dal punto di vista tecnologico, l'attaccante cerca di sfruttare le falle del sistema di protezione. Sfrutta i sistemi non adeguatamente protetti o mal configurati, come i server RDP accessibili da Internet. Può inoltre tentare di sfruttare i punti deboli delle applicazioni vulnerabili e non aggiornate. AD esempio, il Canadian Cyber Security Centre[3] ha emesso un comunicato nel marzo 2021 in cui raccomandava diversi aggiornamenti contro lo sfruttamento attivo delle vulnerabilità legate a Microsoft Exchange.

L'obiettivo: eseguire un codice malevolo per installare un programma nella macchina bersaglio che permette all'aggressore informatico di infiltrarsi.

[2] http://www.itpronews.fr/3648/2012/12/spear-phishing-plus-de-90-des-attaques-ciblees.html

[3] https://cyber.gc.ca/fr/avis/exploitation-active-des-vulnerabilites-de-microsoft-exchange



FASE 2

MOVIMENTI LATERALI

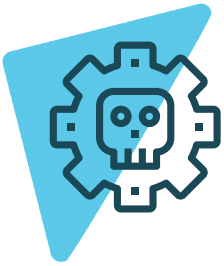
Una volta che la fase di infezione primaria è terminata, l'avversario cerca di scansionare la rete per conoscerla meglio. In questa fase, intende penetrare più profondamente nel sistema informatico per individuare i dispositivi e gli account utente o amministratore che possono essere utilizzati per raggiungere i suoi obiettivi.

Inizialmente, quindi, analizzerà diversi sistemi proverà inoltre ad installare da remoto i propri strumenti nel tentativo di sfruttare le vulnerabilità del sistema e recuperare credenziali utili.

L'obiettivo: penetrare in profondità nell'infrastruttura per individuare macchine bersaglio dove l'attacco avrà il massimo impatto.

In seguito, cerca di penetrare profondamente nel sistema. Utilizza le credenziali rubate di un utente legittimo, rendendo molto difficile il suo rilevamento. Ad esempio può eseguire un'elevazione dei privilegi e spacciarsi per un amministratore locale o prendere il controllo di un account utente che ha accesso a un particolare software. Combina anche tecniche di attacco nel tentativo di compromettere altre macchine vulnerabili.

Gli approcci comuni sono quelli di sfruttare le debolezze, le configurazioni errate dell'infrastruttura o le vulnerabilità esistenti. Ad esempio, una scarsa segmentazione all'interno della rete aziendale che permette l'accesso a macchine di suo interesse, come un server con dati sensibili.



FASE 3

IMPACT

Questa terza fase rappresenta il culmine dell'attacco, dove il criminale informatico esegue azioni in linea con il suo obiettivo. Una volta attivato il cyber-attacco, è possibile che vengano **esfiltrati / trafugati dei dati, che vengano modificati i processi operativi o che venga disattivato un server essenziale** per il buon funzionamento della struttura aziendale.

In questa fase, l'attaccante tenta di mantenere un basso profilo e di compromettere quante più macchine possibile. Questo approccio consente di all'attaccante di sferrare attacchi efficaci e potenzialmente lasciare porte paerte per eventuali successive azioni malevole.[4]

È bene considerare che molto probabilmente si preoccuperà di eliminare i vari backup ed eventuali tracce di attività malevole.

L'obiettivo: minare l'infrastruttura per bloccare un elemento necessario alla produzione aziendale. Inoltre, esfiltrare i dati per la rivendita e/o la pubblicazione (come i dati sanitari sul dark web) o per la crittografia al fine di ottenere un riscatto da parte della struttura bersaglio.

[4] https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

Analisi comportamentale delle soluzioni

I criminali informatici sfruttano sofisticate tecniche di attacco per passare inosservati ed evitare il rilevamento del loro codice malevolo da parte delle varie soluzioni di sicurezza. **È quindi essenziale rilevare di comportamenti sospetti e poter sospendere attività potenzialmente pericolose.**

Pertanto, l' *Host Intrusion Prevention System* (HIPS) aiuta a proteggere le postazioni di lavoro e i server bloccando le attività sospette che possono colpirli.

"Alcuni sistemi di prevenzione dalle intrusioni permettono agli utenti di inviare i log delle attività dannose e le parti di codice sospetto direttamente al vendor per l'analisi e la possibile identificazione. "

Stephen J. Bigelow

Senior Technology Editor

Fonte: Techtarget

Di seguito, discuteremo gli aspetti principali dei diversi tipi di HIPS al fine di ornire un quadro completo delle soluzioni disponibili.

HIPS **con firma**

Si basano sulla **conoscenza delle vulnerabilità di un'applicazione e delle minacce conosciute** e bloccano il loro sfruttamento. Funzionano con un database che deve essere aggiornato regolarmente.

Individuano gli attacchi conosciuti. Tuttavia, **non possono rilevare** attacchi sconosciuti o Zero-day. Sono **poco adatti a situazioni in cui la postazione di lavoro deve essere scollegata** dal proprio server di aggiornamento.

Poche opzioni presenti nel sotware.

HIPS **comportamentale**

Blocco **in tempo reale di attacchi noti e 0 Day**: rilevamento di attività sospette in applicazioni e processi legittimi senza ricorrere a database di firme o anomalie applicative.

Alcuni HIPS combinano **metodi comportamentali ed euristici, protezione della memoria o potenziamento del sistema operativo** (OS) per garantire una migliore protezione contro le minacce.

Elevato livello di parametrizzazione delle liste o delle regole e filtri per adattarsi alle diverse realtà.

"Una soluzione di analisi comportamentale HIPS riconosce e blocca le tecniche di attacco comuni e sofisticate, come lo sfruttamento delle vulnerabilità delle applicazioni, per garantire una protezione efficace delle postazioni utente. "

Edouard Simpère

Responsabile del centro di sicurezza Stormshield

Il termine EDR (Endpoint Detection & Response[5]) negli ultimi anni è diventato onnipresente nel mondo della cybersicurezza. Questo software è utilizzato per rilevare e bloccare minacce note e sconosciute senza dover attendere patch o aggiornamenti. Di solito si tratta di agents distribuiti sui vari endpoint di una rete, in particolare su postazioni di lavoro, telefoni cellulari o i vari server dell'infrastruttura.

Una delle caratteristiche principali degli EDR consiste nel **monitoraggio continuo degli endpoint.** Inoltre, alcune soluzioni includono piattaforme EPP che offrono una protezione in tempo reale. Questa costituisce un'efficace barriera di protezione primaria contro la maggior parte delle minacce conosciute e alcune sconosciute.

Endpoint Detection & Response : un ideale di sicurezza?

Come sottolinea l'ANSSI[6], queste soluzioni che gestiscono una grande quantità di dati offrono generalmente capacità di **rilevamento** (comportamento sospetto di applicazioni legittime, attacchi *fileless*[7]), di **indagine** (visualizzazione completa dell'attacco rilevato) e di **rimedio** (ripristino dei file, ecc.).

Di conseguenza, gli EDR attualmente completano le soluzioni tradizionali basate principalmente su database di firme. Questi software garantiscono una visibilità globale e generalmente sono in grado di rilevare comportamenti anomali anche nei processi legittimi. In seguito al rilevamento, la soluzione attua una risposta per interrompere l'attacco arrestando il processo malevolo, avvertendo inoltre l'amministratore in maniera automatica. Di conseguenza, utilizzando questi strumenti è possibile rilevare e bloccare i ransomware e gli attacchi polimorfici.

Dal punto di vista amministrativo, questi sistemi possono essere integrati con il SIEM aziendale per recuperare i log necessari ad aiutare gli analisti del SOC a ottimizzare l'efficienza nella ricerca degli attacchi.

[5] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[6] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[7] https://www.riskinsight-wavestone.com/2018/10/fileless-attack-le-retour-a-la-terre/

Inoltre, la maggior parte delle soluzioni EDR sul mercato odierno opta per un approccio *cloud-only* o *cloud-first*[8] per centralizzare la raccolta dei dati e analizzare e correlare gli elementi che indicano un attacco. In effetti, il cloud si presta a questa raccolta massiccia e all'analisi di grandi quantità di dati.

Tuttavia, in alcuni casi di utilizzo, non è possibile optare per questa soluzione a causa della sensibilità dei dati da trattare. Di conseguenza, **la modalità *on-premise* rappresenta l'unica opzione valida** (difesa, ministeri, industria, ecc.). Inoltre, è importante fare una distinzione tra analisi server based e analisi client based.

Analizzeremo le principali differenze tra i due approcci:

Protezione incentrata **sul server**

Secondo questo approccio, l'agent installato sulla postazione di lavoro **trasmette tutte le informazioni al server.** Non ha funzionalità estese.

Il server, sia on-premise che nel cloud, analizza i log trasmessi dall'agent alla ricerca di comportamenti dannosi, anomalie presenti su una particolare postazione di lavoro, ecc.

L'agent necessita **di una connessione permanente per riportare le informazioni.** Il fatto stesso che l'elaborazione è asincrona può generare ritardi nella detection.

Protezione incentrata **sull'agent**

L'agent sulla postazione di lavoro può prendere autonomamente delle decisioni e proteggerla senza la necessità di accedere al suo server.

Il server ha meno visibilità globale grazie alle **ampie capacità dell'agent** nel gestire la postazione di lavoro contro il malware.

L'agent può **lavorare in modo indipendente bloccando i comportamenti dannosi in tempo reale.**

Pertanto, per assicurare una protezione ottimale in qualsiasi momento, sono da preferire soluzioni in grado di rilevare il malware senza fare ricorso a una connessione di rete, al fine di garantire una protezione in tempo reale e affidabile della postazione di lavoro.

[8] https://www.pcpresse.com/wp-content/uploads/2020/10/LINFO-CR01_MD.pdf

04

Le diverse tecniche di protezione HIPS

I criminali informatici sono consapevoli che i loro attacchi non devono attirare l'attenzione per passare inosservati (fase 2: movimenti laterali). A tal fine, si adoperano costantemente per sviluppare nuove competenze, implementando diverse tattiche e tecniche di attacco per aggirare le protezioni tradizionali.

Parleremo delle principali tecniche utilizzate e di come l'aggressore le userà per cercare di contrastare le varie protezioni di sicurezza.

Il

255%

Questa cifra corrisponde all'aumento delle segnalazioni di ransomware nel 2020, secondo uno studio dell'ANSSI

Nella tabella sottostante, abbiamo osservato diverse tecniche utilizzate nel corso delle tre fasi di un attacco informatico. Si ricorda che nella terza fase l'attaccante ha già preso il controllo di diverse macchine e dà inizio alla fase di impatto, ovvero esfiltrazione o furto di dati. È opportuno notare che tali esfiltrazioni sono spesso complicate da rilevare perché gli aggressori utilizzano strumenti e identità che sono legittimi *a priori* .

Fase	Tecniche	Come lo utilizza l'aggressore?	Impatti
Fase 1: scoperta e infezione primaria	Buffer overflow. Esempio: - Stack Pivot	L'attaccante utilizza un buffer overflow fornendo dati di input mal formattati per far sì che l'applicazione presa di mira scriva dati in memoria oltre il normale limite. In questo modo si sovrascrivono i dati corretti e si permette all'attaccante di prendere il controllo del flusso di esecuzione dell'applicazione.	Il codice inserito dall'attaccante nell'applicazione bersaglio permette di ottenere l'accesso remoto e/o scaricare ed eseguire altri file malevoli (payload).
Fase 1: scoperta e infezione primaria	Packing Malware	Questa tecnica consiste nell'impedire l'analisi del file malevolo da parte delle soluzioni di sicurezza caricando dinamicamente l'insieme delle funzioni.	I packer rendono più difficile per i team addetti alla sicurezza individuare il malware e aumentano il tempo di analisi. Inoltre, comprimere un file consente di eludere le soluzioni basate su firma.
Fase 1: scoperta e infezione primaria	Process Hollowing. Esempi: - RunPE - Doppelgänging	Il principio è quello di far eseguire al sistema un codice malevolo camuffandolo con l'identità di un processo legittimo. Da un lato, la tecnica RunPE abusa delle debolezze del sistema di caricamento del codice eseguibile. Dall' altro, la tecnica Doppelgänging sfrutta il meccanismo di Windows Transactional NTFS (TxF) per ignettare codice malevolo sfruttando un processo legittimo.	Il process hollowing consente all'attaccante di sfuggire ai controlli delle soluzioni di sicurezza che generalmente ignorano i processi legittimi di sistema.
Fase 2: lateral movement	Privilegi elevati Esempi: - DLL hijacking - Access token manipulation	L'attaccante tenta di ottenere un accesso di livello superiore a una postazione di lavoro o a un sistema per raggiungere i suoi obiettivi. Con la tecnica di DLL hijacking, l'attaccante manipola un'applicazione con privilegi elevati facendole caricare una DLL dannosa. Con l'altra, sfrutta la manipolazione dei token di accesso. L'attaccante può sottrarre o duplicare i token di accesso per modificare il contesto di esecuzione dell'applicazione bersaglio, permettendogli di acquisire ulteriori permessi.	Una volta ottenuti privilegi elevati (diritti di amministratore o di sistema), l'aggressore ha pieno potere nella macchina bersaglio. Questi privilegi elevati facilitano l'estensione dell'attacco.
Fase 2: lateral movement	Pass the hash	L'aggressore usa un hash legittimo al posto di credenziali plain text per ottenere un'accesso privilegiato.	Questa tecnica permette all'aggressore di autenticarsi su altri computer usando questa identità rubata. L'obiettivo è quello di infettare nuove macchine.
Fase 2: lateral movement	Scoprire la rete dalla riga di comando	L'attaccante usa dei comandi (come il comando ping) per rilevare le postazioni di lavoro sulla stessa rete.	L'attaccante può avere un'idea più precisa delle postazioni vicine a quella compromessa.
Fase 3: impatto	Crittografia dei dati	L'aggressore cripta i dati memorizzati sulle macchine (postazione di lavoro e server) per renderli inaccessibili alla vittima. Di solito sfrutta tecniche crittografiche legittime legate alle API di Windows.	Questa strategia è utilizzata negli attacchi ransomware in cui il criminale informatico chiede un riscatto per il recupero dei dati.

4.1

Approccio basato su regole: un metodo efficace

Sono presenti diverse soluzioni che utilizzano regole per eseguire il rilevamento sulle postazioni di lavoro. Tuttavia, in alcuni casi per gli amministratori non è possibile accedervi. Effettivamente l'implementazione di queste regole è piuttosto semplice, ma non possono essere applicate ai molteplici usi aziendali con particolari strutture di sicurezza.

In altre soluzioni, tuttavia, è possibile trovare un buon grado di parametrizzazione per adattarsi al meglio alle realtà in cui la soluzione viene implementata. Così, oltre alle regole fornite dal vendor, l'amministratore può aggiungere regole specifiche basate sulle esigenze e la struttura dell'organizzazione stessa.

Infatti, alcuni sistemi HIPS combinano diverse tecniche di protezione sotto forma di parametri o regole che costituiscono la cosiddetta "politica di sicurezza della soluzione". In questo modo l'amministratore può adattarla al processo aziendale da proteggere. Per alcune soluzioni, è possibile personalizzare i diversi parametri o regole, garantendo così un migliore adattamento e protezione per l'organizzazione.

Lo sapevate?

Le regole comportamentali applicate direttamente dall'agent offrono una protezione immediata della postazione di lavoro per limitare l'impatto di un attacco.

La granularità delle soluzioni di protezione utilizzate

Alcune soluzioni propongono liste di regole predefinite che possono essere estese dall'amministratore per contrastare i malware.

Come osservato in precedenza, sono da preferire le soluzioni HIPS che forniscono **un insieme di regole configurabili e ben definite per controllare qualsiasi azione eseguita sulle postazioni di lavoro**, come il monitoraggio dei processi in esecuzione, dei file e delle chiavi di registro, l'elevazione dei privilegi, ecc.

Questa granularità permette agli amministratori di ottenere un alto grado di personalizzazione e, più in generale, la possibilità di implementare una politica di sicurezza che sia il più vicino possibile alle necessità e ai requisiti aziendali.

Di norma, una postazione di lavoro o un server dovrebbero essere considerati in base al loro contesto (ad esempio, esterni o interni alla rete aziendale) e al loro livello di esposizione alle minacce.

4.2 Approccio contestuale: comprendere meglio il contesto

Poiché ogni azienda è strutturata in modo univoco con esigenze specifiche, la soluzione di protezione deve essere in grado di adattarsi ai diversi casi d'uso al suo interno. Di conseguenza, occorre **adattare il tipo di protezione scelto per le postazioni di lavoro e i server al contesto d'uso individuale e prendere in considerazione i diversi scenari di mobilità.** Ad esempio, controllare le reti Wi-Fi autorizzate e disabilitarle quando una connessione LAN è attiva. Oppure bloccare qualsiasi connessione diversa dalla VPN quando questa è attiva.

Quindi, è necessario implementare una soluzione di sicurezza capace di cambiare le proprie politiche di protezione dinamicamente. Ovvero, deve **individuare l'ubicazione della postazione di lavoro e adattarne la sicurezza al contesto in cui si trova.**

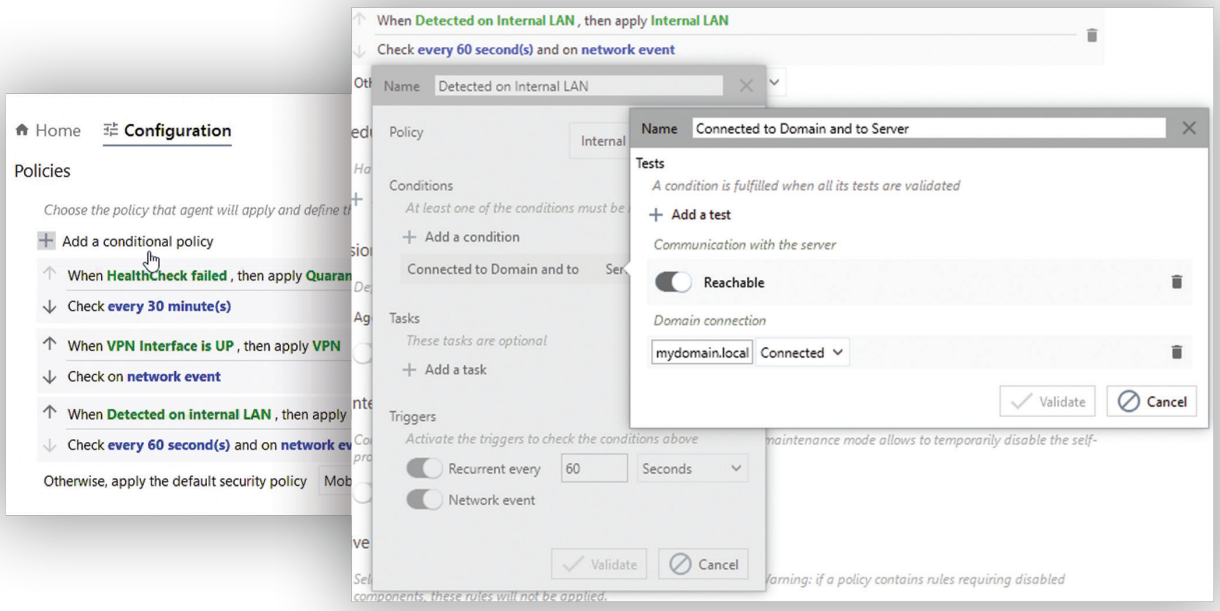


Figura 1

Soluzione di protezione degli endpoint con diverse politiche di sicurezza

4.3
"Hardening" per la protezione del sistema stesso

Le soluzioni di sicurezza rappresentano un bersaglio per gli attacchi dei criminali informatici. Questi ultimi cercano di invalidare la protezione o di approfittare dei diritti privilegiati di queste soluzioni facendone un uso improprio. Inoltre, come sottolinea l'ANSSI[9], è necessario verificare il software (e l'hardware) di un'infrastruttura e hardenizzarne la configurazione prima dell'utilizzo.

Occorre altresì valutare la superficie d'attacco. Gli esperti concordano sul fatto che ogni nuovo componente (hardware e software) aggiunto all'infrastruttura aumenta il rischio di bug o vulnerabilità relativi a tale componente, permettendone lo sfruttamento da parte di un aggressore informatico.

Per limitare la superficie di attacco e rafforzare la difesa delle postazioni di lavoro, alcune soluzioni di protezione integrano nel loro sviluppo l'approccio *Security by design*[10]. Si tratta di soluzioni in cui la sicurezza e i rischi associati vengono integrati e studiati fin dalla fase di progettazione del prodotto.

[9] https://www.ssi.gouv.fr/uploads/2020/08/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.1.pdf

[10] https://www.securecontrolsframework.com/security-privacy-design-principles

[11] https://www.zdnet.fr/actualites/une-faille-0day-de-l-antivirus-trend-micro-utilisee-dans-le-piratage-de-mitsubishi-electric-39898077.htm

Attacco informatico alla Mitsubishi Electric[11]

La casa automobilistica giapponese ha ammesso di aver subito un attacco informatico nel giugno 2019. Secondo un'indagine durata mesi, gli aggressori hanno avuto accesso alla rete interna aziendale, trafugando 200 MB di file sensibili relativi a migliaia di dipendenti e informazioni tecniche riservate.

Com'è potuto succedere?

Un gruppo di criminali informatici con base in Cina ha presumibilmente sfruttato una vulnerabilità 0-Day nel software antivirus aziendale per installare file dannosi. Secondo il produttore del software violato, i criminali hanno sfruttato una vulnerabilità di directory traversal per estrarre i file da una cartella zip arbitraria e trasferirli in una cartella specifica sul server dell'antivirus. Questa operazione potrebbe aver causato l'esecuzione di codice remoto o *Remote Code Execution*.

A tal fine, l'architettura generale di questo tipo di soluzioni deve essere sviluppata secondo le regole di programmazione di un'architettura di sicurezza con microservizi. È proprio qui che si applica il principio del minimo privilegio.

L'architettura basata sul modello dei micro servizi è un'architettura divisa in diversi servizi indipendenti per garantire la massima sicurezza, ognuno con un ruolo specifico e privilegi limitati. In questo modo, ad esempio, il modulo che gestisce la connessione al server di configurazione non deve essere quello incaricato all'interpretazione della stessa. Oppure il servizio che gestisce i log si occupa esclusivamente di questo incarico e non può accedere alle policy di sicurezza in atto.



Figura 2
Soluzione di protezione suddivisa in diversi servizi indipendenti

Per raggiungere un elevato livello di affidabilità, i processi di sviluppo del software di protezione devono inoltre stabilire rigide regole di codifica e prevedere l'uso di varie opzioni di compilazione ed esecuzione. Queste opzioni limitano i rischi di creare bug sfruttabili durante un attacco e riducono anche il numero di errori, aumentando i controlli prima e durante l'esecuzione.

In sintesi, le soluzioni hardenizzate basate su questi principi garantiscono una migliore protezione contro gli attacchi informatici.

Stormshield Endpoint Security Evolution : la soluzione di protezione delle postazioni di lavoro

Stormshield Endpoint Security Evolution **protegge gli ambienti sensibili** bloccando gli attacchi al principio, ben prima che possano arrecare danni

Analisi comportamentale avanzata in grado di bloccare le minacce note, gli attacchi Zero-Day e le aggressioni di tipo *fileless*.

Soluzione autonoma che opera e garantisce la sicurezza degli endpoint anche in assenza di una connessione di rete.

Controllo avanzato dei dispositivi. Il controllo dei dispositivi e delle connessioni include la verifica delle reti Wi-Fi e delle chiavette USB, nonché l'accesso al volume del disco fisso e le connessioni di rete.



Il **91%**

degli attacchi informatici segue il metodo dello **spear phishing**

Il **40%**

delle infezioni primarie utilizza la tecnica del **process hollowing**

255%

Aumento delle segnalazioni di ransomware nel 2020 (secondo uno studio realizzato dall'ANSSI)

ALCUNI ESEMPI DI ATTACCHI

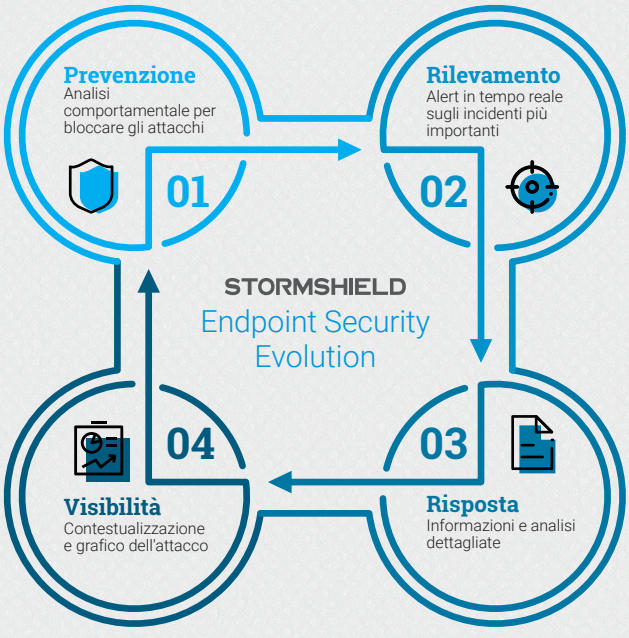
- WORM
- MALWARE (VIA E-MAIL)
- DISPOSITIVI INFETTI
- FURTO DI PASSWORD
- SCANSIONE DEL SISTEMA
- ATTACCHI FILELESS
- SPEAR PHISHING
- SOCIAL ENGINEERING
- CAVALLO DI TROIA
- DATA LEAK
- SFRUTTAMENTO DELLE VULNERABILITÀ
- ...

ALCUNI CONSIGLI INDISPENSABILI

Fate attenzione alle e-mail sospette con allegati o link sospetti.

Effettuate **backup regolari**.

Aggiornate le vostre applicazioni, plugin e sistemi operativi.



LA **SCELTA EUROPEA** DELLA **SICUREZZA INFORMATICA**

www.stormshield.com

Qualsiasi diffusione, riproduzione o rappresentazione, anche parziale, del presente white paper per scopi diversi dall'uso privato su qualsiasi supporto è vietata e può comportare la responsabilità civile e penale per chiunque non si attenga a tale divieto.

Copyright © 2022 Stormshield