STORMSHIELD

ARTICOLO DI OPINIONE

PROTEZIONE DEGLI ENDPOINT E ANTIVIRUS: QUAL È LA DIFFERENZA?

Julien Paffumi
Product Portfolio Manager,
Stormshield

A quasi un decennio dalla loro scomparsa, i software antivirus tradizionali sono ancora molto diffusi. Sebbene il termine antivirus sia comunemente utilizzato nel lessico del mondo informatico, ormai ha perso le sue credenziali. Capiamo insieme perché.

L'uso di software antivirus tradizionali sembra ormai obsoleto, soppiantato dai più moderni Next Generation Antivirus (NGAV), *Endpoint Protection Platform* (EPP) e *Endpoint Detection and Response* (EDR). Quali sono le differenze tra tutte queste tecnologie di rilevamento? Al giorno d'oggi abbiamo ancora bisogno di un software antivirus? Con questo documento cercheremo di rispondere a queste ed altre domande.

GLI ANTIVIRUS SONO ANCORA UN METODO DI PROTEZIONE AFFIDABILE?

Progettato per essere installato su singoli dispositivi come computer, tablet e telefoni, l'antivirus è un programma informatico che ha lo scopo di rilevare e rimuovere software malevoli. La prima azienda a svilupparlo è stata IBM nel 1987 in risposta al virus informatico «Brain», coniando così **il termine «antivirus» che nel corso degli anni si è diffuso notevolmente, fino a diventare nell'immaginario collettivo l'unica difesa contro gli attacchi informatici.**

Il principio dei programmi antivirus si basa sulla ricerca delle firme. « *Analogamente a un vaccino, l'antivirus dispone di un database di firme che gli consente di riconoscere il virus informatico. È quindi essenziale che la firma di questo virus specifico sia stata generata in precedenza*», afferma Stéphane Prévost, Product Marketing Manager di Stormshield. Un meccanismo che presenta diverse problematiche e molti limiti. Primo fra tutti: è necessario conoscere il virus per poterne identificare la firma (ed essere in grado di combatterlo). Il secondo limite, non meno importante, è l'avvento del polimorfismo, una tecnica per generare file malevoli dotati di una firma digitale unica per ciascuno di essi, ma il cui metodo di infezione e il carico utile rimangono comuni. Questo limite è ancora più significativo se si considera che ogni giorno vengono creati 450.000 nuovi malware, ovvero quasi 4 milioni al mese, secondo l'Istituto AV-TEST. Come diretta conseguenza di tale fenomeno, è tecnicamente impossibile per gli antivirus avere una conoscenza preventiva di tutte le firme... A peggiorare le cose, negli ultimi anni i metodi operativi dei criminali informatici hanno continuato ad evolversi fino ad annidarsi in punti ciechi degli algoritmi di rilevamento, generando attacchi informatici privi di file (*i cosiddetti malware fileless*). Di conseguenza, il meccanismo di rilevamento basato sulla ricerca delle impronte digitali in un file lascia passare una grande quantità di malware e deve essere integrato da altre tecniche di protezione.

L'evoluzione e la sofisticazione degli attacchi informatici stanno trasformando gli antivirus in un bersaglio. Ad esempio, in occasione della conferenza «Black Hat Europe» del dicembre 2022, un ricercatore di sicurezza ha rivelato una vulnerabilità inedita che riguarda diversi software antivirus. Una falla che consente di assumere il controllo dell'antivirus ed eliminare i file legittimi. Cosa fare, allora, quando il nostro principale strumento di protezione non svolge più il suo ruolo?

L'AVVENTO DEL RILEVAMENTO COMPORTAMENTALE NELLA PROTEZIONE DELLE POSTAZIONI DI LAVORO

In risposta a questa nuova situazione, **i fornitori di soluzioni di sicurezza informatica hanno dovuto riconsiderare il proprio approccio, passando dal fingerprinting all'analisi euristica basata sul comportamento dell'utente.** Chiamati *Next-Gen Antivirus* o NGAV, questi nuovi tipi di antivirus hanno gettato le basi per quello che diventerà il concetto di EPP (*Endpoint Protection Platform*). Le soluzioni *Endpoint Protection Platform* (EPP) saranno la prima risposta agli attacchi polimorfici e fileless, integrando nuove

funzionalità come il monitoraggio della memoria, l'analisi comportamentale o la verifica degli indicatori di compromissione (IoC). Nonostante tali progressi tecnologici, gli attacchi informatici continuano ad essere insidiosi e a sfuggire alle maglie della rete. Diventa pertanto indispensabile individuarli anche dopo il loro passaggio e porvi rimedio.

Su questi presupposti, nel 2013 fa la sua prima comparsa nelle analisi di Gartner la soluzione *Endpoint Threat Detection & Response* (ETDR), incentrata sui temi della risposta agli incidenti e dell'investigazione. Dal 2015, l'acronimo ETDR sarà sostituito da EDR, ovvero *Endpoint Detection & Response*. La particolarità di questo nuovo approccio risiede nella capacità di rilevare le minacce sconosciute e di rispondere ad esse in tempo reale in modo semi-autonomo, come sottolinea **Noël Chazotte**, Product Manager Stormshield: «*Se rileva una minaccia, l'antivirus blocca il programma a monte, talvolta mettendolo in quarantena. L'EDR, invece, entra in azione quando l'incidente di sicurezza viene rilevato o si è già verificato sulla macchina e cerca di determinare cosa è accaduto per aiutare gli operatori a prevenire la diffusione dell'infezione.*»

In che modo la tecnologia EDR rileva gli attacchi sofisticati? «*L'EDR individua i comportamenti anomali grazie agli indici di compromissione* (IoC)», spiega Stéphane Prévost. «*Non si tratta sempre di eventi eccezionali, ma di azioni comuni come l'apertura di una connessione a un server esterno.*» Da qui nasce l'importanza di definire con precisione il quadro operativo della soluzione durante la fase di apprendimento per evitare falsi allarmi (falsi positivi). Tuttavia, le soluzioni BDU e DPI restano complementari, come sottolinea Stéphane Prévost: «*Possiamo fare un paragone con la sicurezza fisica di un'azienda. La soluzione EDR consiste nelle telecamere di sorveglianza: esse consentono ad esempio di rilevare l'eventuale ingresso di un intruso nel sito produttivo. Ma per bloccarlo all'ingresso, è necessaria la presenza di un addetto alla sicurezza sul posto: questo è l'EPP.*»

E l'antivirus, che ruolo ha? Secondo il sito web security.org, nell'arco del 2023 tre americani su quattro riterranno opportuno dotarsi di un antivirus per poter utilizzare il proprio computer in tutta tranquillità. Alla luce dei progressi tecnologici sopra menzionati, la questione sorge sul piano professionale: **perché al giorno d'oggi abbiamo ancora bisogno di un antivirus?** Semplicemente perché fornisce un primo livello di sicurezza. Anche se questa soluzione non sarà efficace contro tutti gli attacchi informatici, garantisce un primo livello di protezione contro quelli meno sofisticati, con la certezza di evitare il problema dei falsi positivi e di occupare pochissime risorse sulla postazione di lavoro. Ma un primo livello di sicurezza ne implica altri. «*Spesso sulla stessa macchina sono installate diverse soluzioni di protezione*», spiega Noël Chazotte. «*Tuttavia, la loro combinazione non è sempre ottimale, in quanto alcune di esse possono portare a conflitti, lasciando un'ulteriore porta aperta ai criminali informatici.*»

NDR, XDR, MDR: VERSO UNA SPECIALIZZAZIONE DI DETECTION & RESPONSE

Nonostante la semplicità promessa da tali soluzioni, la loro gestione richiede la supervisione di esperti, come dimostra lo sviluppo di offerte EDR gestite o mini-SOC. **Oltre a perfezionare il rilevamento, è essenziale che gli strumenti di protezione degli endpoint includano funzionalità di rilevamento e risposta agli incidenti.** Inoltre, con il proliferare dei punti di raccolta degli incidenti, l'analista SOC deve avere accesso a tutti i dispositivi di rete e dell'infrastruttura.

Ad esempio, le soluzioni NDR (*Network Detection and Response*) analizzano i pacchetti TCP/IP che transitano sulla rete per rilevare attività sospette. La piattaforma XDR (*eXtended Detection and Response*) mira a riunire tutte le risorse informatiche interne ed esterne (rete, directory, risorse cloud, firewall, ecc.) in modo da fornire una visione globale degli eventi nel sistema informatico. Per Noël Chazotte, «*una piattaforma XDR è l'insieme dei punti di raccolta e soprattutto una piattaforma di correlazione per aiutare, mitigare il rischio e fornire elementi di risposta e rimedio*»

Negli ultimi anni sono emersi ulteriori acronimi, come l'MDR. Nella pratica, il *Managed Detection and Response* (MDR) è semplicemente un metodo di commercializzazione di un XDR in cui un team esterno gestisce gli avvisi. Qualunque sia lo strumento e la tecnologia, occorre tenere presente che il ruolo dell'analista rimane centrale e che nessuna soluzione è in grado di proteggere da sola una risorsa sensibile.

Secondo lo studio condotto da Survey Risk Alliance, solo il 12% dei professionisti della sicurezza informatica dichiara di aver adottato una soluzione XDR nella propria azienda nel 2022. Il restante 77% dichiara di avere intenzione di adottarla entro i prossimi 24 mesi. Si prevede quindi che la richiesta di esperti in sicurezza specializzati nel rilevamento e nella risposta agli incidenti continuerà a crescere nei prossimi anni. Questo perché, nonostante i progressi tecnologici, l'intervento umano rimane essenziale per l'analisi e la comprensione degli incidenti... Si tratta di profili molto ricercati per far fronte alla costante evoluzione delle modalità operative e i cui servizi saranno senza dubbio più facilmente accessibili alle aziende attraverso le offerte EDR gestite o di mini-SOC.