A caccia di minacce con EDR, MDR e XDR

25 MARZO 2025

In questo articolo esamineremo due dei principali strumenti di identificazione e contrasto particolarmente indicati per le PMI:

- *Endpoint Detection and Response (EDR)*
- *Managed Detection and Response (MDR)*

Accenneremo anche brevemente a un terzo strumento con maggiori capacità e conseguente maggior costo, più adatto alle grandi strutture:

- *Extended Detection and Response (XDR)*

I CYBER CRIMINALI sono sempre più agguerriti, la tecnologia di cui dispongono sempre più evoluta, le minacce sempre più insidiose e capaci di procurare danni sempre più importanti. È diventata quindi vitale per ogni organizzazione una strategia di cybersecurity a tutto campo.

Secondo le stime di Statista il costo del crimine informatico nel mondo è destinato a moltiplicarsi negli anni a venire. Passiamo dai 14,57 trilioni di US$ (migliaia di miliardi) del 2024 ai 23,82 nel 2027, con un incremento costante poco oltre 3.000 miliardi/anno.

Un software antivirus di ultima generazione è tassello indispensabile, ma interviene essenzialmente dopo che il virus si è manifestato. Una buona strategia di security deve invece prevedere anche la capacità di rilevare le attività sospette che superano le barriere tradizionali e assicurare una risposta efficace.

Che cosa è EDR, Endpoint Detection and Response

Le soluzioni EDR hanno come scopo quello di garantire la sicurezza degli endpoint collegati alla rete: PC, laptop, server, l'Internet of Things (IoT) e via dicendo. Analizzano tutta l'attività degli endpoint e assicurano visibilità sul loro stato di salute in tempo reale.

In pratica riconoscono i comportamenti anomali, rilevano potenziali minacce e allertano il team di sicurezza con suggerimenti sui possibili rimedi. È infatti al team di sicurezza che compete ricevere gli avvisi e prendere gli opportuni provvedimenti per fermare un attacco in corso o limitarne la propagazione sulla rete.

Sono quindi soluzioni che richiedono l'**installazione di un agente** su ogni endpoint collegato in rete per rilevarne l'attività e l'**intervento di esperti** in grado di ricevere gli avvisi e agire di conseguenza in base ai suggerimenti. Tipicamente includono le funzionalità seguenti:

- Monitoraggio degli endpoint con registrazione degli eventi.
- Analisi delle anomalie e individuazione delle minacce potenziali.
- Invio di avvisi al team di security con raccomandazioni pratiche a supporto delle contromisure da adottare.
- Possibilità di reazione automatica alle minacce con eliminazione del malware o con l'isolamento dell'endpoint vulnerabile.

Che cosa è MDR, Managed Detection and Response

Occorre considerare che l'EDR genera una enorme quantità di dati, il cui esame, anche da parte di professionisti qualificati, porterebbe via tempi incredibilmente lunghi. Ecco che vengono in soccorso le soluzioni MDR, che all'atto pratico prendono in gestione le tecnologie di sicurezza degli endpoint, EDR incluso.

La gestione è affidata a team che lavorano da un SOC (Centro Operativo di Sicurezza), un'unità (non necessariamente interna agli stessi fornitori delle soluzioni EDR), responsabile di identificare e contrastare le minacce alla sicurezza.

Ci sono vendor – a titolo di esempio citiamo Bitdefender e Malwarebytes - che hanno un SOC interno e offrono quindi soluzioni chiavi in mano, mentre altri per politica scelgono di delegare la gestione a partner terzi dotati di SOC e know-how. Recentemente anche Trellix ha annunciato un proprio servizio MDR, di cui non si conoscono ancora tutti i particolari.

Il maggior vantaggio delle soluzioni MDR è naturalmente quello di affidare all'esterno la gestione dei rimedi, specialmente importante nel contesto odierno di crescente scarsità di figure professionali specializzate in cybersecurity, con particolare riferimento alla protezione degli ambienti cloud.

È fin troppo evidente, specie per le PMI, l'insostenibilità di assumere professionisti a tempo pieno in via esclusiva, mentre un SOC esterno lavora 24x7 e ripartisce i costi su più utenti.

Senza considerare un aspetto spesso trascurato, cioè che tutti gli utenti di un servizio gestito beneficiano singolarmente del multiforme patrimonio di esperienza e conoscenza accumulato dal gestore del servizio a contatto con le realtà più disparate.

Che cosa è XDR, Extended Detection and Response

Se, come abbiamo visto, le soluzioni EDR si concentrano unicamente sulla sicurezza degli endpoint, l'XDR estende le capacità di analisi per esempio agli utilizzi cloud dell'organizzazione e agli applicativi in uso.

I sistemi XDR non possono prescindere dall'impiego di personale altamente specializzato, una risorsa talmente rara sul mercato, da risultare difficile già il solo entrarci in contatto.

È pur vero che esistono soluzioni di XDR gestito (MXDR, Managed XDR), però la complessità organizzativa connessa e il loro costo le rendono adatte a grandi imprese che abbiano la necessità di unificare il contrasto a minacce provenienti dai molti singoli strumenti di security di cui si sono dotate.

In due parole

EDR è lo strumento base per il monitoraggio degli endpoint e il rilevamento delle minacce. Ogni strategia di cybersecurity dovrebbe includerlo. Funziona tramite agenti software o sensori installati su ogni endpoint per catturare dati che vengono inviati a un repository (archivio digitale) centralizzato per essere analizzati.

MDR è essenzialmente un EDR acquisito come servizio. Con un team dedicato di esperti in security, il servizio prende in carico la sicurezza degli endpoint, eliminando o mitigando le minacce.

XDR estende le capacità di EDR oltre la protezione degli endpoint e unifica la risposta a minacce segnalate da tutta l'infrastruttura aziendale.

Per quali organizzazioni è indicato l'EDR?

Fermo restando che la sicurezza degli endpoint non dovrebbe mai essere affidata unicamente a sistemi antivirus - per quanto di ultima generazione -, la scelta di una soluzione EDR è adatta a organizzazioni

- dotate di un team in grado di ricevere gli avvisi e agire in base alle raccomandazioni della soluzione stessa.
- grandi strutture che partono da questa fase iniziale per costruire una strategia di cybersecurity a più ampio raggio, usando l'EDR come fondamento per un'architettura di security scalabile.

Per quali organizzazioni è indicato l'MDR?

Con tutta evidenza le soluzioni MDR sono quelle più consigliabili alle piccole e medie imprese, che generalmente non dispongono di risorse e strumenti atti a contrastare efficacemente minacce avanzate.

Più in generale, l'MDR permette di introdurre in azienda nuove competenze e maggiore consapevolezza senza dover assumere altro personale. Attrarre risorse altamente specializzate diventa ogni giorno più problematico, mentre è vitale proteggersi dalle minacce più recenti.

Una buona misura dell'esposizione al cyber crimine può darla il nostro servizio gratuito SLED.

PS – Ci piacerebbe ricevere i tuoi commenti o domande via WhatsApp al nostro numero +39 351 4272010. Siamo qui per aiutarti a proteggere il tuo business. Inizia la scoperta ora

Contatto: Marcello Fontana
commerciale@gotech.it
+39 351 4272010