swisscom

Comunicato stampa

Managed Endpoint Detection & Response: così Swisscom offre più sicurezza alle imprese

Notebook, desktop e smartphone sono i bersagli prediletti dei cybercriminali. Da sole, le misure preventive non sono sufficienti a fermali. Per contrastare efficacemente i cyberattacchi più raffinati servono misure di protezione supplementari come un sistema di Endpoint Detection & Response (EDR). E Swisscom lo propone alle imprese come nuovo managed service.

Strano a dirlo, eppure spesso in principio ci sta il terminale: circa il 70 percento dei cyberattacchi ha come primo bersaglio proprio l'endpoint, ovvero notebook, PC, smartphone e server locali sulla rete aziendale. A questa conclusione è giunto uno studio di Absolute Software, azienda statunitense specializzata in sicurezza informatica. Gli attacchi diventano sempre più sofisticati e a diffondersi sono in particolare le varianti senza file annessi. Si tratta ad esempio in codici di programmazione che agiscono solo nella memoria di lavoro del computer, senza lasciare tracce nell'archivio dei file. «Per molti programmi antivirus un attacco di questa natura è invisibile, e spesso anche i firewall non intervengono», spiega Cyrill Peter, responsabile Enterprise Security Services di Swisscom. «Per questo è importante proteggere bene i terminali, identificare gli attacchi e prevenirli tempestivamente.»

L'integrazione per una soluzione di security completa

Endpoint Detection & Response (EDR) viene a colmare questa lacuna nella security. Al contrario dei software antivirus basati su firme, analizza il comportamento del terminale alla ricerca di anomalie. «I nostri clienti vedono tutto in tempo reale su un dashboard», spiega Peter. «Così vengono alla luce le potenziali falle di sicurezza di qualsiasi terminale. Le notifiche di sicurezza vengono rilevate e se possibile risolte in automatico, cosa che sgrava il team addetto alla sicurezza in azienda.»

Tuttavia, un sistema EDR non identifica e respinge per forza tutti gli attacchi; al contrario, deve essere integrato in altre soluzioni per la sicurezza, collegato a un Security Operation Center (SOC) e spesso sottoporre i comportamenti sospetti sugli endpoint alla valutazione finale degli esperti analisti di security. Grazie a EDR, questi professionisti si possono concentrare su pochi attacchi potenziali (alert

predisposti) senza dover passare in rassegna migliaia di eventi e log. Questo snellisce enormemente il loro lavoro. Se succede qualcosa, il team security dispone di un colpo d'occhio sull'infrastruttura IT monitorata da EDR ed è in condizione di reagire immediatamente su tutti gli endpoint, ad esempio isolando un terminale attaccato da malware o spostando file sospetti in una cartella per la quarantena.

Ben lungi dall'essere una soluzione standalone, quindi, EDR va integrato in soluzioni e processi di sicurezza preesistenti. Swisscom, ad esempio, propone di combinare EDR con SOC as a Service o CSIRT as a Service. In questo modo, i clienti Swisscom si proteggono efficacemente da attacchi fileless come malware, software dannosi ed exploit zero-day.

Endpoint Detection & Response: ecco come funziona

I dispositivi connessi alle reti sono potenziali bersagli di cyberattacchi complessi e rappresentano i cosiddetti endpoint. Endpoint Detection & Response (EDR) monitora in tempo reale tutte le attività sugli endpoint, compresa l'interfaccia con la rete, per rilevare e risolvere in automatico le notifiche di sicurezza. In questo modo tutti i punti di accesso alla rete vengono protetti da cyberattacchi complessi.

Whitepaper (in francese):
https://www.swisscom.ch/fr/business/enterprise/downloads/security/endpoint-detection-response.html

Pagina web del prodotto EDR:
https://www.swisscom.ch/it/business/enterprise/offerta/security/edr.html

Pagina web del prodotto SOC Services:
https://www.swisscom.ch/it/business/enterprise/offerta/security/threat-detection-and-response.html

Berna, 14 ottobre 2020