swisscom

Medienmitteilung

Swisscom bringt mit Managed Endpoint Detection & Response mehr Sicherheit in Unternehmen

Notebooks, Desktops und Smartphones stehen im Fokus von Cyberkriminellen. Präventive Massnahmen alleine reichen nicht aus, um sie zu stoppen. Um raffinierte Cyberattacken zu kontern, braucht es zusätzliche Schutzmassnahmen, wie ein System für Endpoint Detection & Response (EDR). Swisscom lanciert einen neuen managed Service für Unternehmen.

Am Anfang steht oft das Endgerät: Rund 70 Prozent der Cyberattacken nutzen als ersten Angriffspunkt Endpoints. Damit sind Notebooks, PCs, Smartphones sowie lokale Server im Firmennetz gemeint. Zu diesem Schluss kommt eine Studie des US-Sicherheitsanbieters "Absolute Software". Die Attacken werden immer ausgeklügelter, insbesondere dateilose Angriffe nehmen zu. Sie können etwa aus einem Programmiercode bestehen und laufen ausschliesslich im Arbeitsspeicher des Rechners – ohne Spuren im Dateisystem zu hinterlassen. "Für viele Antivirenprogramme ist ein solcher Angriff unsichtbar und selbst Firewalls schöpfen oft keinen Verdacht", erklärt Cyrill Peter, Leiter Enterprise Security Services bei Swisscom. "Deshalb ist es wichtig, Endgeräte zusätzlich zu schützen, Angriffe zu erkennen und rechtzeitig zu verhindern."

Puzzleteil einer umfassenden Security-Lösung

Endpoint Detection & Response (EDR) ist dazu in der Lage. Im Gegensatz zu signaturbasierter Antivirensoftware analysieren sie das Verhalten des Endgerätes und suchen nach Anomalien. "Unsere Kunden können alles in Echtzeit auf einem Dashboard verfolgen", sagt Peter. "So sind potentielle Sicherheitslücken über alle Endgeräte hinweg sichtbar. Sicherheitsmeldungen werden automatisch untersucht und wenn möglich behoben, dadurch wird das Security Betriebsteam entlastet."

EDR bedeutet aber nicht, dass alle Angriffe automatisch erkannt und abgewehrt werden. EDR benötigt die Integration in weitere Security-Lösungen, die Einbindung in ein Security Operation Center (SOC) und oftmals die abschliessende Bewertung von verdächtigem Endpoint-Verhalten durch erfahrene Security-Analysten. Diese können sich dank EDR auf wenige, mögliche Angriffe

(aufbereitete Alerts) konzentrieren und müssen nicht Tausende von Events und Logs auswerten. Dadurch werden sie massiv entlastet. Kommt es zu einem Vorfall, kann das Security Team über EDR einen schnellen Überblick über die überwachte IT-Infrastruktur erlangen und umgehend über alle Endpoints hinweg reagieren - zum Beispiel mit der Isolation eines von Malware befallenen Endpoints oder dem Verschieben verdächtiger Dateien in ein Quarantäne-Verzeichnis.

EDR ist somit keine Standalone-Lösung, sondern sollte in bestehende Security-Lösungen und Prozesse der Security eingebunden werden. Bei Swisscom lässt sich EDR zum Beispiel mit SOC as a Service oder CSIRT as a Service kombinieren. Dadurch können sich Swisscom Kunden effizient gegen dateilose Angriffe wie Malware, bösartige Software und Zero-Day-Exploits zur Wehr setzen.

So funktioniert Endpoint Detection & Response

Mit Netzwerken verbundene Geräte liefern potentielle Angriffsflächen für komplexe Cyberattacken und stellen sogenannte Endpoints dar. Endpoint Detection & Response (EDR) überwacht alle Aktivitäten auf dem Endpoint inklusive im Übergang zum Netzwerk in Echtzeit und untersucht und behebt automatisch Sicherheitsmeldungen. So werden alle Zugangspunkte zum Netzwerk vor komplexen Cyberangriffen geschützt.

Whitepaper:
https://www.swisscom.ch/de/business/enterprise/downloads/security/endpoint-detection-response.html

Produktewebseite EDR:
https://www.swisscom.ch/de/business/enterprise/angebot/security/edr.html

Produktewebseite SOC Services:
https://www.swisscom.ch/de/business/enterprise/angebot/security/threat-detection-and-response.html

Bern, 14. Oktober 2020