GEFAHR ERKANNT, GEFAHR GEBANNT: WIE GEHT GUTES THREAT HUNTING?

SOPHOS Threat Detection and Response (kurz TDR) ist eine Methode, die es Krankenhäusern ermöglicht, Cyberangriffe zu neutralisieren, bevor sie Schaden anrichten können. Denn es ist immer schwieriger, Cyberbedrohungen zu identifizieren und darauf zu reagieren. Und zwar so effektiv und effizient wie ein Großkonzern – ohne ein Heer an IT-Sicherheitsexperten zur Verfügung stehen zu haben.

Oftmals werden Angriffe heutzutage als sogenannte Blended Attacks durchgeführt, die maschinelle und menschliche Angriffstechniken kombinieren. In der Folge kommen verschiedenste und oftmals unter dem Radar laufende Einzelangriffe zum Einsatz, die sich zudem individuell anpassen, wenn sich ihnen ein Hindernis in den Weg stellt. Threat Hunter und Analysten enthüllen diese verborgenen Gegner, indem sie sich an verdächtigen Ereignissen, Anomalien und Aktivitätsmustern orientieren. Das Auffinden der Bedrohung ist dabei nur der erste Schritt, im Anschluss ist die Zusammenarbeit im Teamwork wichtig, um die Situation zu entschärfen. Das Ergebnis ist Threat Detection and Response.

Während sich solche Expertenteams lange Zeit zumeist nur Großkonzerne oder staatliche Einrichtungen leisten konnten, öffnet Sophos diesen individuellen Service mit seinem Manage Threat Response Service (MTR) nun auch stationären Einrichtungen jeder Größenordnung und lässt seine Cybercrime-Experten für Kunden aktiv werden. Denn nur wenige Organisationen haben intern die richtigen Tools, Mitarbeiter und Prozesse, um ihr Sicherheitsprogramm effizient rund um die Uhr zu verwalten und sich gleichzeitig proaktiv vor neuen Bedrohungen zu schützen. Das Sophos MTR-Team informiert nicht nur über Angriffe und verdächtiges Verhalten, sondern ergreift auf Wunsch gezielte Maßnahmen direkt im Netzwerk, um selbst hochkomplexe Bedrohungen unschädlich zu machen. Die Cybercrime-Experten übernehmen dabei sieben Tage die Woche rund um die Uhr folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen

MENSCHLICHE EXPERTISE UND MODERNSTE TECHNOLOGIE

Sophos MTR basiert auf Intercept X Advanced with EDR, einer Technologie zur Erstellung detaillierter Abfragen, um Bedrohungen aufzuspüren und IT Security Operations zu optimieren. Auf diese Weise werden leistungsstarkes Machine Learning mit Expertenanalysen zu einem effektiven Teamwork vereint. So erhalten Unternehmen und andere Einrichtungen eine optimale Bedrohungssuche und -erkennung, eine fundierte Analyse der Warnmeldungen sowie gezielte Maßnahmen zur schnellen und vollständigen Beseitigung von Bedrohungen. Diese leistungsstarke Kombination aus Endpoint Protection, intelligenter Endpoint Detection & Response und hochqualifizierten Sicherheitsexperten ermöglicht dank maschinengestützter Technologie eine besonders schnelle und zielführende Reaktion.

SOPHOS
Die Evolution der Cybersecurity.

Sophos Technology GmbH
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Tel.: +49-(0)800 2782761
(gebührenfrei aus Deutschland)
Tel.: +49-(0)611 5858-0 (Ausland)