

Aufwand reduzieren und die Sicherheit erhöhen

Managed XDR



KENNEN SIE DAS AUCH?

Als Security-Verantwortlicher eines Einzelhandelsunternehmens müssen Sie eine weit verteilte IT-Landschaft absichern, darunter Kassensysteme in den verschiedenen Filialen, Cloud-Services und Netzwerke. Hier steht viel auf dem Spiel. Was, wenn eine Ransomware-Attacke die IT lahmlegen würde und die Kassen ausfallen? Oder wenn Hacker sensible Zahlungs- und Kundendaten abgreifen?

Das können Sie auf keinen Fall riskieren. Deshalb tun Sie alles dafür, um Cyberangriffe so früh wie möglich zu erkennen und einzudämmen. Zudem müssen Sie sich mit einem umfangreichen Katalog an Regularien auseinandersetzen, darunter die DSGVO und die PCI DSS.

Wenn Ihr Unternehmen zu den großen Lebensmittelversorgern gehört, zählt es außerdem zu den KRITIS-Organisationen und muss die Security-Anforderungen des branchenspezifischen Sicherheitsstandards (B3S) erfüllen. Ein wichtiges Kriterium, das darin genannt wird, ist eine leistungsfähige Detection and Response.

LEICHTER GESAGT, ALS GETAN

Sie geben Ihr Bestes, um den Geschäftsbetrieb aufrechtzuerhalten, Daten zu schützen und für Compliance zu sorgen. Vielleicht haben Sie bereits ein SIEM, das Sicherheitsmeldungen verschiedener Systeme sammelt, oder Sie betreiben sogar ein Security Operations Center (SOC). Aber trotzdem gibt es noch vieles, was Ihnen Bauchschmerzen bereitet:



Ihre Mitarbeiter sind täglich mit Tausenden von Security Alerts konfrontiert. Wie sollen sie da schnell genug die wirklich wichtigen erkennen?



Da das SIEM nach Events pro Sekunde lizenziert wird, fallen durch die vielen angeschlossenen Security-Systeme hohe Kosten an.



Auch Use Cases für SIEM- und SOC-Projekte zu erstellen und die entsprechende Logik aufzubauen, ist aufwändig und teuer.



Sie brauchen hochqualifizierte Analysten, um Sicherheitsmeldungen zu bewerten und Zusammenhänge herzustellen. Doch solche Spezialisten sind in Zeiten des Fachkräftemangels schwer zu finden.



Die Analysten müssen sich kontinuierlich weiterbilden, denn Cyberangriffe werden immer komplexer. Auch das kostet Zeit, die Ihnen fehlt.

SO KLAPPT'S

Sie brauchen einen Managed Service, der eine zuverlässige Lösung für Extended Detection and Response (XDR) mit hochqualifiziertem Analysten-Know-how kombiniert. XDR sammelt nicht nur Security-Informationen aus der gesamten IT-Umgebung, sondern korreliert sie auch automatisch und bereitet sie so auf, dass verwertbare Warnungen entstehen. Dabei nutzt die Lösung Künstliche Intelligenz (KI) und bezieht globale Threat Intelligence mit ein, um Risiken besser zu erkennen. Lesen Sie dazu auch die Einschätzung von Gartner in den [Top Security and Risk Management Trends](#).

Im Managed Service übernehmen spezialisierte SOC-Analysten die Auswertung und Einschätzung der Ergebnisse, die die XDR-Lösung ausgibt. Da sie auch Indikatoren kennen, die bei anderen Kunden entdeckt wurden, können sie sogar neue Angriffsmuster schnell identifizieren. Die Analysten bewerten die Kritikalität der Funde und empfehlen geeignete Gegenmaßnahmen mit einem Schritt-für-Schritt-Aktionsplan.

Im eigenen Team sparen Sie also erheblichen Analyse-Aufwand und müssen sich nur noch um die Umsetzung der Maßnahmen kümmern. Auch dabei kann der Managed Service Provider unterstützen. Er liefert zudem regelmäßige Berichte zur Sicherheitssituation Ihres Unternehmens, die Sie der Geschäftsleitung vorlegen können.



WIE FINDE ICH DEN PASSENDEN ANBIETER?

Achten Sie darauf, dass der Managed XDR-Provider über einen führenden Security Stack, ein großes Team an SOC-Spezialisten, nachweisbare Expertise und möglichst viele Kunden verfügt. So können Sie sicher sein, dass er ein hohes Qualitätsniveau bietet. Je größer die Datenbasis, auf die der Anbieter zugreifen kann, umso treffsicherer sind seine Analysen.

DARUM LOHNT SICH MANAGED XDR



- Sie profitieren von spezialisiertem Know-how erfahrener SOC-Analysten. Da diese über globale Bedrohungsinformationen verfügen und neueste Analyseverfahren einsetzen, können sie Gefahren und Angriffsmuster noch besser erkennen.
- Sie erhöhen Ihre Analyse-, Korrelations- und Reaktionsgeschwindigkeit.
- Ihr Team wird entlastet. Allein die Automatismen der XDR-Lösung leisten so viel wie durchschnittlich acht Vollzeit Security-Mitarbeiter, so der [ESG Research Insights Report](#).
- Sie sparen SIEM- und SOC-Kosten. Denn mit Managed XDR reduziert sich die Zahl der zu bearbeitenden Events auf ein Minimum.
- Sie sparen Planungskosten, da die XDR-Lösung bereits vorgefertigte Use Cases für Endpunkt- und E-Mail-Security mitbringt.
- Ihr eigenes Team kann von den SOC-Spezialisten lernen und sich weiterentwickeln. So können Sie den Managed Service-Anteil nach und nach reduzieren.

DER PARTNER AN IHRER SEITE



Mit XDR von Trend Micro erhalten Sie Best of Breed-Lösungen vereint aus einer Hand von einem Marktführer. Trend Micro wurde im Forrester Wave™: Enterprise Detection and Response als Leader genannt (1. Quartal 2020) und ist laut MITRE ATT&CK Evaluations - APT29 führend bei der Ersterkennung.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist.

Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss.“



©2021 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. For details about what personal information we collect and why, please see our Privacy Notice on our website at: <https://www.trendmicro.com/privacy>