Use Case Bund & Länder

TREND MICRO™ | Global Leader in Cybersecurity

NIS2-Herausforderungen trotz Fachkräftemangel meistern

Trend Service One

HILFE, NOCH MEHR REGULATORIK!

Wird Ihnen auch langsam alles zu viel? Mit der NIS2-Richtlinie kommen noch mehr regulatorische Anforderungen auf Sie zu. Die Uhr tickt: Bis zum 17. Oktober 2024 muss der Gesetzgeber die EU-Vorgaben in nationales Recht umsetzen. Als Security-Verantwortlicher stehen Sie vor der Herausforderung, sich auf die neuen Pflichten vorzubereiten. Doch so richtig neu ist das Ganze zum Glück gar nicht.

Im Grunde geht es um drei zentrale Bereiche: Cyber-Risikomanagement, Angriffserkennung und Incident Response. Diese möglichst gut abzudecken, ist in der Security ohnehin unverzichtbar. Im IT-Sicherheitsgesetz 2.0 stand dazu bisher nur schwammig „nach Stand der Technik". Eigentlich also gut, dass es mit NIS2 endlich einmal konkreter wird. Denn die Bedrohungslage spitzt sich zu. Wie der aktuelle BSI-Lagebericht zeigt, stehen Kommunalverwaltungen und kommunale Betriebe verstärkt im Visier von Cyberkriminellen.

SCHAFFEN SIE DAS ALLEINE?

Natürlich überprüfen Sie jetzt Ihre Security-Aufstellung und überlegen, wo Sie nachrüsten müssen. Doch mit moderner Technik ist es nicht getan. Ihr größtes Problem ist der Fachkräftemangel. Die wichtigste Frage lautet daher: Welche Aufgaben können Sie selbst erfüllen und wo brauchen Sie externe Unterstützung?

Sie müssen Cyberrisiken erkennen, bewerten und managen. Dafür müssen Sie Transparenz in der IT-Umgebung gewinnen, interne und externe Daten korrelieren und richtig interpretieren.

Laut NIS2 müssen Sie einen Cybervorfall innerhalb von 24 Stunden beim BSI melden. Das setzt nicht nur eine gute Angriffserkennung voraus. Sie müssen die Warnmeldungen der Security-Systeme auch bewerten und entscheiden, ob es sich um einen meldepflichtigen Vorfall handelt.

Wer kümmert sich um die Konfiguration Ihrer Security-Systeme? Erzielen Sie die bestmögliche Erkennungsrate und Performance? Die Einstellungen regelmäßig zu überprüfen und anzupassen ist wichtig, um optimalen Schutz zu gewährleisten.

Wer übernimmt im Ernstfall die Incident Response? Dafür brauchen Sie garantierten Zugriff auf professionelle Spezialisten, die den Cyberangriff detailliert untersuchen und ihn schnell eindämmen. Doch solche Teams sind stark ausgebucht.

SO ENTLASTEN SIE IHR TEAM

Wäre es nicht schön, Sie hätten einen Partner an der Seite, der Ihnen all diese Sorgen abnimmt? Ihr persönlicher Customer Service Manager prüft dann, ob Ihre Security-Systeme optimal konfiguriert sind, und unterstützt Sie dabei, die Technologie nach Best Practices einzusetzen. Mithilfe von XDR-Technologie untersuchen Experten die Angriffsfläche und machen Risiken transparent.

Außerdem überwachen erfahrene Security-Analysten Ihre IT-Umgebung 24/7, suchen proaktiv nach Angriffen, werten Warnmeldungen aus und verständigen Sie, sobald Handlungsbedarf besteht. Die Spezialisten geben Ihnen auch Empfehlungen zu Gegenmaßnahmen. Und falls es trotzdem zu einem Cybervorfall kommt, steht ein hochprofessionelles Incident Response-Team bereit, sodass Sie Schaden minimieren und schnell wieder betriebsfähig werden.

DIE TECHNISCHE VORAUSSETZUNG: EXTENDED DETECTION & RESPONSE (XDR)

Damit Managed Detection & Response- und IR-Teams effizient arbeiten können, brauchen sie eine fundierte Datengrundlage. Dafür sorgt eine XDR-Plattform, die Telemetriedaten aller angeschlossenen Systeme in einem zentralen Data Lake sammelt, KI gestützt korreliert und analysiert. Dabei fließen auch externe Security-Informationen zu aktuellen Angriffskampagnen und Schwachstellen ein.

DARUM LOHNT ES SICH

- Sie erweitern Ihr Team durch externe Spezialisten.
- Trotz Fachkräftemangel können Sie zentrale NIS2-Anforderungen erfüllen.
- Sie können Bedrohungen schneller erkennen und schneller reagieren.
- Ein 24/7-Service schützt Sie auch außerhalb Ihrer Geschäftszeiten. So erfüllen Sie die Meldefrist innerhalb von 24 Stunden und sind NIS2-konform.
- Sie erhöhen die Effizienz Ihrer Security-Systeme und holen das Beste aus Ihren Investitionen.
- Sie profitieren vom Know-how weltweit führender Sicherheitsforscher
- Im Ernstfall haben Sie garantiert Zugriff auf ein professionelles Incident Response Team.

DER PARTNER AN IHRER SEITE

Trend Micro´s Service One Complete ist ein Rund-um-die-Uhr Service für Managed Detection, Response und Support. Er umfasst Targeted Attack Detection, Managed XDR, einen designierten Service-Manager, Premium Support und Incident Response.

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.“

Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.