| Finanzdienstleister & Versicherungen

Assume Breach

Immer mit dem Ernstfall rechnen

DETECTION & RESPONSE STEHT GANZ OBEN AUF IHRER AGENDA

Als Security-Verantwortlicher in einem Finanz- oder Versicherungsunternehmen sind Sie an Herausforderungen gewöhnt. Sie haben es mit hochsensiblen Daten zu tun, die nahezu in Echtzeit verarbeitet werden müssen. Gleichzeitig steht Ihre Branche im Visier von Cyberkriminellen, die professionell agieren und neueste Techniken anwenden. Daher ist für Sie klar: Prävention allein reicht nicht aus, um für Schutz zu sorgen.

„Assume Breach" heißt die Devise – immer davon ausgehend, dass irgendwann einmal ein Angreifer durchkommt. Mit diesem Mindset folgen Sie aktuellen Security Best Practices. Was im Ernstfall zählt, ist die Bedrohung so schnell wie möglich zu erkennen und zu mitigieren. Deshalb steht das Thema Detection & Response ganz oben auf Ihrer Agenda.

Auch das neue IT-Sicherheitsgesetz 2.0, dem Sie als KRITIS-Organisation unterstehen, fordert in §8a explizit Systeme zur Angriffserkennung. Die BaFIN hat das in den BAIT und VAIT für die Finanz- und Versicherungsbranche spezifiziert. Noch bis Ende April 2023 haben Sie Zeit, die Anforderungen umzusetzen.

SIND SIE BEREIT, WENN'S PASSIERT?

Bestimmt sammeln Sie bereits Security-Informationen in einem SIEM und betreiben ein SOC. Aber reichen die Maßnahmen aus, um Compliance-konform zu sein? Und sind sie effizient genug?

Zu den Anforderungen an die operative Informationssicherheit (Kapitel 5 BAIT und VAIT) zählt: Sie müssen in der Lage sein, Vorfälle technisch zu identifizieren, zu analysieren und umfassend zu dokumentieren.

Sie müssen Risiken nicht nur erkennen, sondern auch bewerten und schnell die richtigen Gegenmaßnahmen einleiten.

Um das zu erreichen, müssen Security-Analysten unzählige False Positives aussortieren und in mühevoller Kleinarbeit Indicators of Compromise (IoC) aus verschiedenen Systemen zusammensetzen und analysieren.

All das verursacht großen Aufwand, macht den SOC-Betrieb teuer und dauert im Ernstfall zu lange.

SO GELINGT IHNEN COMPLIANCE-KONFORME ANGRIFFSERKENNUNG

Sie brauchen eine umfassende Plattform für erweiterte Detection & Response (XDR), die von einer zentralen Konsole aus einen Überblick über die Risiken in der gesamten IT-Umgebung gibt. Hier fließen sicherheitsrelevante Informationen verschiedener Sensoren zusammen – von den Endpunkten über Server, Netzwerke und E-Mail bis hin zu Cloud Workloads. Die Daten werden KI-gestützt und unter Berücksichtigung neuester, globaler Threat Intelligence analysiert, korreliert und bewertet. So sehen SOC-Mitarbeiter auf einen Blick, welche Risiken kritisch sind, und können detailliert nachvollziehen, wie ein Angriff bisher verlaufen ist.

Zusätzliche Entlastung bringt ein Service für Managed XDR: Trend Micro-Experten überwachen dann die Alarme aus der XDR-Lösung, priorisieren sie und suchen aktiv nach IoCs. Ein Incident Reponse Team unterstützt im Ernstfall bei der Schadensbehebung. Möchten Sie Ihre Detection & Response darüber hinaus noch weiter ausbauen und bei der Geschwindigkeit Ihrer Datenverarbeitung keinerlei Kompromisse eingehen, so empfehlen wir Ihnen unsere Best Practice „Präventiv Gefahren abwehren – ohne auszubremsen“. Darin erfahren Sie, wie ein Intrusion Prevention System (IPS) Bedrohungen in Echtzeit blockiert.

IDENTIFIZIEREN SIE SCHWACHSTELLEN MIT RED TEAMING

Eine XDR-Plattform ermöglicht es, Risiken kontinuierlich zu monitoren. Eine ideale Ergänzung dazu ist ein Red Teaming: Sicherheitsspezialisten von Trend Micro stellen dann die Reaktionsfähigkeit Ihres Unternehmens in realistischen Angriffsszenarien auf die Probe. Dabei agieren sie aus der Perspektive der Angreifer und folgen dem EU-TIBER-Framework (Threat Intelligence Based Ethical Red Teaming). So decken die Experten Schwachstellen auf, ermitteln organisationsspezifische Angriffsrisiken und schlagen gezielte Präventivmaßnahmen vor. Mehr zu Red Teaming hier ››

DIESE VERBESSERUNGEN ERZIELEN SIE

- Sie schaffen Transparenz über Risiken in der gesamten IT-Umgebung.
- Die XDR-Plattform vereinfacht die Risikobewertung der IT-Systeme enorm.
- Sie reduzieren Aufwand im SOC. Laut einer ESG Studie können Sie 63 Prozent bei den jährlichen Sicherheitskosten einsparen.
- Sie können Bedrohungen schneller mitigieren. Laut einer ESG-Studie kann XDR die Reaktionsgeschwindigkeit um 70 Prozent verkürzen.
- Sie können Angriffe lückenlos nachverfolgen und so Ihrer Dokumentations- und Meldepflicht laut BAIT und VAIT leichter nachkommen.

DER PARTNER AN IHRER SEITE

Mit Trend Micro Vision One erhalten Sie eine branchenführende Plattform für erweiterte Detection & Response in der gesamten IT-Umgebung. Trend Micro ist der erfahrene Sicherheitspartner für KRITIS-Betreiber im Finanz- und Versicherungswesen. Laut MITRE ATT&CK Evaluations sind wir 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."

TREND MICRO™
Securing Your Connected World