Kontinuierliches Security-Monitoring

Endlich Durchblick im IT-Security-Management

CSO

IN KOOPERATION MIT AMPEG

IT-Infrastrukturen sind in den vergangenen Jahren immer heterogener, komplexer und unübersichtlicher geworden. Um sie effektiv zu schützen, brauchen CISOs, Security-Verantwortliche und IT-Leiter einen kontinuierlichen Überblick über den Sicherheitsstatus in ihren IT-Umgebungen.

Cyberattacken sind weltweit das Risiko Nummer eins für Unternehmen, so das Allianz Risk Barometer. Auch die deutsche Wirtschaft ist nahezu flächendeckend von Angriffen betroffen. Dem Digitalverband Bitkom zufolge hatten im vergangenen Jahr 84 Prozent der befragten deutschen Unternehmen einen Sicherheitsvorfall, weitere neun Prozent vermuten dies. Mehr als drei Viertel der Umfrageteilnehmer rechnen mit verstärkten Cyberangriffen in den kommenden zwölf Monaten.

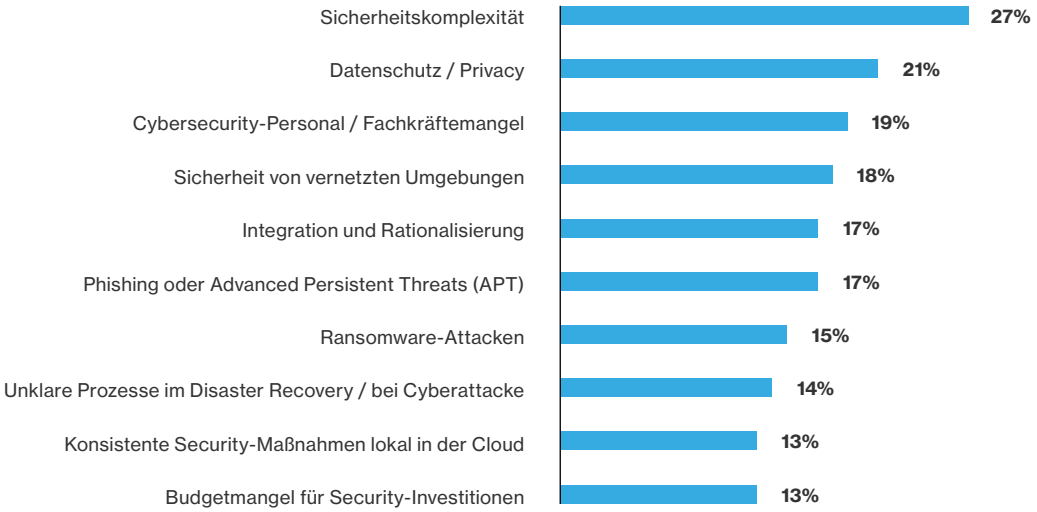
Um ihre heterogenen, gewachsenen Infrastrukturen gegen die zunehmenden Cybergefahren abzusichern, setzen große Organisationen eine Vielzahl von Security- und Management-Lösungen ein. Zum Standardrepertoire gehören Virenscanner, Patch-Management, Mobile-Device-Management (MDM) und Inventory-Management, immer häufiger kommen auch Lösungen und Services wie EDR (Endpoint Detection and Response), Vulnerability-Scanner oder URL-Filter zum Einsatz.

Viele Security Officer verfolgen dabei das Best-of-Breed-Prinzip und wählen die jeweils leistungsfähigsten oder kosteneffizientesten Produkte und Services einer Klasse. So kommt es, dass der Virenscanner von Anbieter A, die Firewall von Hersteller B und das Patch-Management von Firma C bezogen werden. In der Folge entsteht häufig ein Wildwuchs an Verwaltungs-Tools, Mitarbeitende müssen sich in die verschiedensten Bedienlogiken einarbeiten. Oft werden Security Services auch an spezialisierte Provider ausgelagert, die wiederum nur einen Teil der Sicherheitsaufgaben abdecken.

Gefährliche Intransparenz

Die Folge dieser Strategie ist eine heterogene und intransparente Sicherheitsarchitektur. Ein Überblick über alle Security-Applikationen und das im Unternehmen herrschende Sicherheitsniveau fehlt. Wie drängend das Problem ist, zeigt eine Umfrage des Marktforschungsunternehmens IDC: Den Analysten zufolge ist Sicherheitskomplexität aktuell die größte Herausforderung, vor der Cybersecurity-Verantwortliche stehen.

Top 10 der Security-Herausforderungen



N = 206; maximal drei Antworten pro Studienteilnehmer; Abbildung gekürzt
Quelle: IDC Studie „Cybersecurity Deutschland 2022"; November 2022

Sicherheitskomplexität ist die größte Herausforderung für die Cybersecurity deutscher Unternehmen.
Quelle: IDC-Studie „Cybersecurity in Deutschland", November 2022

Dies führt immer häufiger dazu, dass Sicherheitslücken nicht erkannt und damit auch nicht geschlossen werden. Dem Ponemon Institut zufolge gehen 60 Prozent der Datenpannen auf bereits bekannte Schwachstellen zurück, die nicht gepatcht wurden.

Organisationen mit verteilten Standorten und dezentraler IT-Infrastruktur stehen vor einer zusätzlichen Herausforderung. Sie müssen die lokal erhobenen Daten möglichst in Echtzeit zusammenführen und analysieren, um einen Überblick über den Sicherheitsstatus des Gesamtunternehmens zu erhalten.

Wie schwierig das sein kann, zeigt das Beispiel des Saatgutherstellers KWS SAAT SE (KWS), dessen Standorte sich auf 70 Länder verteilen. „Wir haben mit regelmäßig übermittelten, umfangreichen Excel-Listen gearbeitet, um den Überblick über den Bestand an IT-Systemen und die darauf installierte Software sowie über Sicherheitswerkzeuge, ausgerollte Patches, Viren-Patterns und andere wichtige Daten zu behalten“, sagt Andreas Sternberg, IT Security Officer bei KWS, „dieses Verfahren verschaffte uns jedoch nicht den unmittelbaren Zugriff auf die weltweiten Statusinformationen, den wir uns wünschten.“

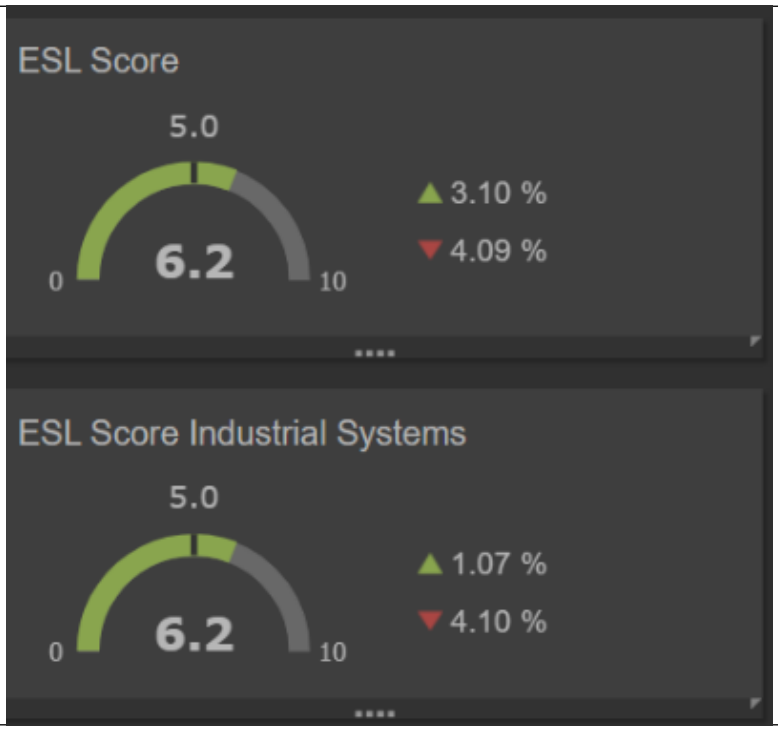
Kontinuierliches Monitoring für eine aktive Sicherheit

Um tatsächlich über die aktuelle Sicherheitslage Bescheid zu wissen, müssen Unternehmen einen kontinuierlichen Überblick über alle Security-Applikationen und deren Wirksamkeit gewinnen. Dazu brauchen sie ein zentrales Monitoringsystem, das Daten aus den verschiedenen Quellen erfassen und verarbeiten kann.

Diese Aufgabe leisten CSM-Systeme (Continuous Security Monitoring) wie Security Lighthouse des deutschen IT-Sicherheitsspezialisten AMPEG. Sie verknüpfen die gesammelten Daten, vergleichen sie mit externen Informationen wie CVE-Datenbanken (Common Vulnerabilities and Exposures) und stellen die Ergebnisse nahezu in Echtzeit in einem übersichtlichen Dashboard dar. CISOs, IT-Sicherheitsverantwortliche und die Fachkräfte im Security Operations Center (SOC) erhalten so auf Knopfdruck einen Überblick über den Security-Status in ihrem Unternehmen.

> Um tatsächlich über die **aktuelle Sicherheitslage Bescheid** zu wissen, müssen Unternehmen **einen kontinuierlichen Überblick** über alle Security-Applikationen und deren Wirksamkeit gewinnen.

Organisationen, die ein CSM-System implementieren, erleben oft eine Überraschung, wie Dirk Ossenbrueggen, Head of Information Governance and Security beim Glashersteller SCHOTT berichtet: „Das Kontrollsystem hat uns klipp und klar aufgezeigt, wo wir stehen. In gewisser Weise waren die Daten ernüchternd, denn wir hatten gedacht, mit unserer IT-Sicherheit schon weiter zu sein."



Der Enterprise Security Level (ESL) Score zeigt auf einen Blick, wie sich das Sicherheitsniveau im Unternehmen entwickelt. Quelle: AMPEG

Der richtige Einstieg ins Kontinuierliche Security-Monitoring

Den größten Nutzen bietet eine CSM-Lösung natürlich, wenn sämtliche IT-Management- und Security-Systeme daran angeschlossen werden. Security Lighthouse stellt dafür Kollektoren und mehr als 400 Auswertungen zur Verfügung. Kundenspezifische Anforderungen lassen sich im Regelwerk schnell und einfach konfigurieren.

Dennoch empfiehlt es sich in vielen Fällen, klein anzufangen und erst einmal die wichtigsten Quellen über Kollektoren anzubinden. Dazu gehören zum Beispiel Patch-Management, Inventarverwaltung, Virenscanner und Active Directory. Das hat weniger technische als kulturelle Gründe. Häufig sind Fachbereichsleiter nämlich skeptisch und gewähren nur ungern Einblick in ihre operativen Prozesse. Die klaren Vorteile eines CSM überzeugen die Verantwortlichen aber schnell, wenn sie es im praktischen Einsatz erleben.

Ein rollenbasiertes Zugriffskonzept, wie es Security Lighthouse bietet, fördert die Akzeptanz zusätzlich. Im Rechtemanagement kann festgelegt werden, dass Mitarbeitende zum Beispiel nur die Auswertung über ihren Standort, ihre Abteilung oder sogar nur eine einzelne Applikation zu sehen bekommen. So können Verantwortliche auf allen Ebenen und in allen Bereichen in das gemeinsame Projekt IT-Sicherheit einbezogen werden. Auch Provider lassen sich durch das rollenbasierte Konzept einfach in das Security-Monitoring einbinden.

> **Ein rollenbasiertes Zugriffskonzept,** wie es Security Lighthouse bietet, fördert **die Akzeptanz** zusätzlich.

Fazit: Security-Level-Management schafft den Überblick

Es genügt heute nicht mehr, auf erkannte Sicherheitsvorfälle zu reagieren. In einer immer komplexer und hybrider werdenden Infrastruktur ist die Gefahr zu groß, dass Angreifer unerkannte Schwachstellen ausnutzen, sich in der IT-Infrastruktur ausbreiten und Schäden anrichten, bevor SIEM und andere Lösungen Alarm schlagen.

Organisationen benötigen deshalb ein kontinuierliches Security-Monitoring sämtlicher Systeme und Vorgänge in der IT-Infrastruktur, das alle Informationen übersichtlich aufbereitet und nahezu in Echtzeit zur Verfügung stellt. Diese Daten bieten nicht nur einen Gesamtüberblick über den aktuellen Sicherheitsstatus und zeigen Verbesserungsmöglichkeiten auf, sie können auch als Argumentationsgrundlage für Budgetverhandlungen mit dem obersten Management dienen. Mit den Kennzahlen, die ein System wie Security Lighthouse liefert, lassen sich notwendige Verbesserungsmaßnahmen deutlich überzeugender begründen und der erreichte Fortschritt besser dokumentieren.

KWS konnte mit AMPEG Lighthouse sein drängendstes Problem lösen: „Wir sehen, wo wir stehen, können eventuellen Detailfragen unmittelbar auf den Grund gehen und schnell Abhilfe schaffen“, sagt IT Security Officer Sternberg.

Erfahren Sie mehr über Kontinuierliches Security-Monitoring und Security-Level-Management. Informieren Sie sich jetzt!