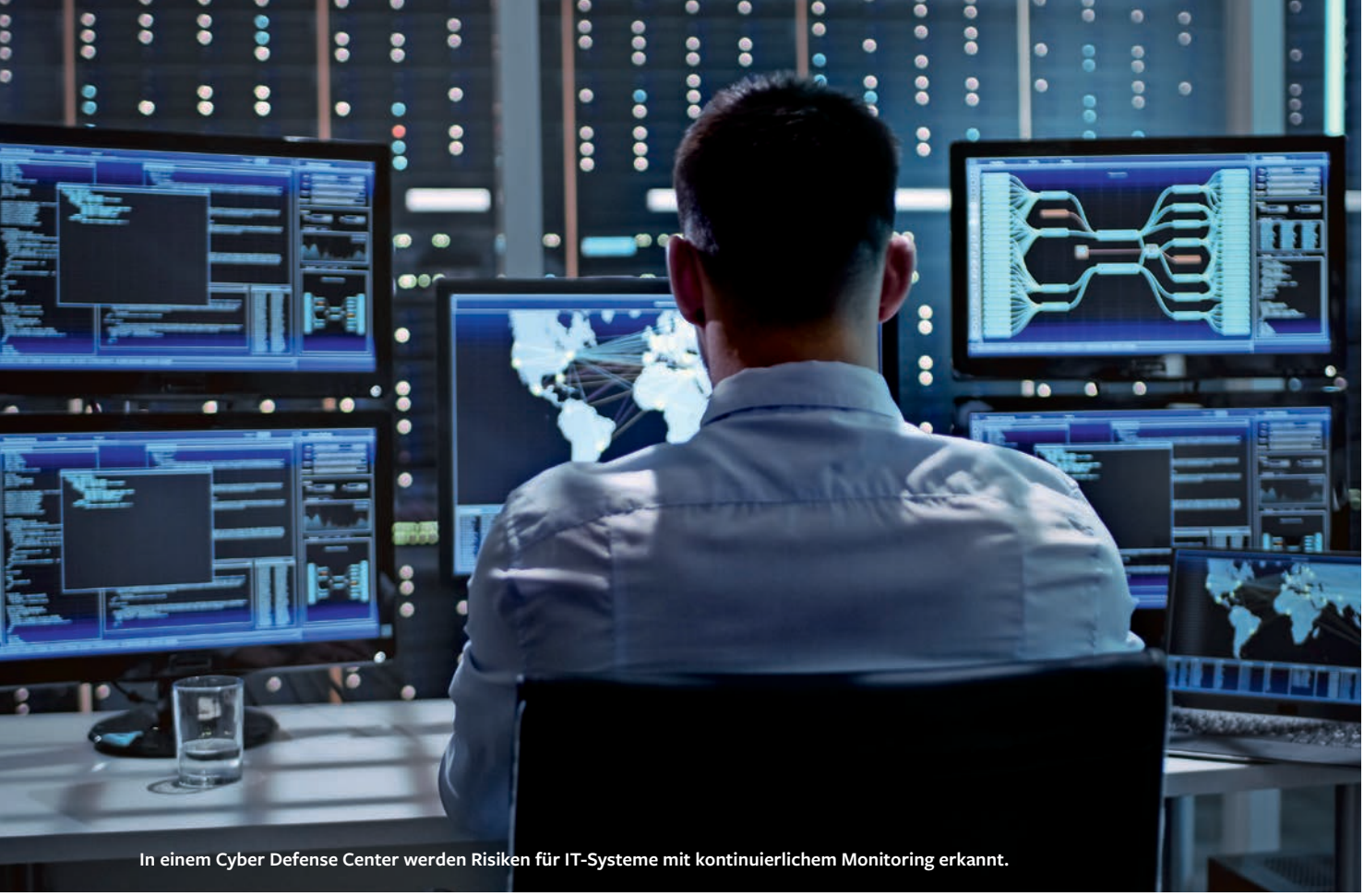

In einem Cyber Defense Center werden Risiken für IT-Systeme mit kontinuierlichem Monitoring erkannt.

Foto: Adobe Stock/ Gorodenkoff Productions OU

Kontinuierliches Monitoring dank Cyber Defense Center

Aufgrund der steigenden Bedrohungslage müssen IT-Infrastrukturen rund um die Uhr überwacht werden. Ein Cyber Defense Center, betrieben von IT-Spezialisten, kann hier Abhilfe schaffen.

Bedrohungen durch Hacker und Cyberkriminelle nehmen immer mehr zu. Herkömmliche Methoden, wie Firewalls oder Passwortschutz, sind schon lange nicht mehr ausreichend. Ein SIEM (Security Information Event Management) ist ein wichtiger Bestandteil eines IT-Sicherheitskonzeptes. Potenzielle IT-Sicherheitsrisiken können rechtzeitig erkannt und analysiert werden. In einem SIEM laufen alle Informationen zu möglichen Angriffsszenarien zusammen.

Die Aufgaben eines SIEM werden durch das Cyber Defense Center (CDC) übernommen. In einem Cyber Defense Center werden Risiken für IT-Systeme mit kontinuierlichem Monitoring erkannt. Security-Analysten identifizieren und bewerten Sicherheitsvorfälle in Echtzeit und leiten Gegenmaßnahmen ein. Unternehmen und Organisationen erhalten so ein konstantes Sicherheitsniveau. Dieses wird von Spezialisten beständig automatisiert und weiterentwickelt. Im Zusammenspiel mit der bestehenden Sicherheitsarchitektur bietet das Cyber Defense Center ein Früherkennungssystem für Cyberattacken für die Informationsverarbeitung.

Managed SIEM Services

MANAGED Services sind modular aus unterschiedlichen Bausteinen aufgebaut und reichen von der Analyse bis zum SIEM-Tool. Security-Analysten der Consecur GmbH erkennen Risiken für IT-Systeme mit kontinuierlichem Monitoring, bewerten Sicherheitsvorfälle in Echtzeit und leiten Gegenmaßnehmen ein.

In Koexistenz mit der IT-Abteilung vor Ort gewährleisten Managed Security Services (MSS) den sicheren Betrieb von IT-Systemen.

„Der digitale Wandel verändert die Anforderungen an die IT-Infrastruktur fundamental."

Um die vielfältigen Herausforderungen zu meistern, sind mehr Ressourcen und Personal notwendig.

Ziel eines Cyber Defense Centers ist die kontinuierliche Überwachung und Analyse zur Vermeidung von Sicherheitsvorfällen.

Welche Vorteile bietet ein CDC?

- schnelles Erreichen eines hohen IT-Sicherheitsniveaus
- Rund-um-die-Uhr-Überwachung der IT-Infrastruktur
- regelmäßige Reportings und Handlungsempfehlungen
- aktive Abwehr von Sicherheitsbedrohungen (Incident Response)
- Log- und Eventanalyse
- Compliance-Nachweise durch Dokumentation von Maßnahmen und Ereignisse
- kalkulierbare Kosten

Personal, Prozesse und Technologie

Um ein Cyber Defense Center erfolgreich zu etablieren ist das richtige Zusammenspiel von Personen, Prozesse und Technologien entscheidend.

Erfahrenes Personal: Qualifizierte Mitarbeiter sind die wichtigste Grundlage, um ein CDC erfolgreich zu betreiben. Diese qualifizierten Mitarbeiter müssen sowohl über technische Fähigkeiten verfügen als auch über soziale Kompetenzen. Die eingesetzten Security-Analysten müssen in der Lage sein erste Einschätzung und Priorisierung von Sicherheitsvorfällen abgeben zu können. Weiterhin müssen die Security-Analysten über das toolgestützte Standard Monitoring hinaus unterschwellige Sicherheitsvorfälle erkennen. Da es keine Berufsausbildung für die obengenannten Aufgaben gibt, wird ein auf den Kunden maßgeschneidertes Schulungsprogramm entwickelt.

Etablierte Prozesse: Die Prozesse müssen gut aufeinander abgestimmt sein, damit ein hoher Grad an Effektivität und Effizienz gewährleisten werden kann. Gut definierte Prozesse ermöglichen konsistente Vorgänge und reproduzierbare Ergebnisse.

Geeignete Technologie: Die richtige Auswahl der Tools ist unerlässlich für den Schutz vor Bedrohungen. Die Einführung eines gut konzipierten CDC ist der Schritt, den Unternehmen ergreifen müssen, um den größtmöglichen Nutzen aus einer SIEM-Tool-Implementierung zu ziehen. Die Herausforderung besteht somit darin eine kundengerechte Bedarfsanalyse zur Funktionalität zu erstellen. Entscheidend ist somit nicht das SIEM-Tool, sondern, ob dieses zum Kunden passt.

70

PROZENT der Unternehmen und Institutionen in Deutschland sind in den Jahren 2016 und 2017 Opfer von Cyberangriffen geworden.

Welche Vorteile bietet Managed SIEM?

- einfacher Zugang zu Technikern und Ressourcen
- modulares Konzept zur Auswahl der benötigten Services
- kurze Implementierungsdauer
- kosteneffiziente und effektive Lösung

ConSecur GmbH:
www.consecur.de