dacoso
data communication solutions

Managed SIEM

Security und Compliance unter Kontrolle haben

Es ist immer mehr zu tun

IT-Verantwortliche sind heute stärker denn je damit beschäftigt, die strengen Anforderungen an Daten-Sicherheit und Compliance zu erfüllen – Tendenz nach wie vor steigend. Aggressive Datenspionage und Cyber-Attacken machen nervös, Handlung wird erwartet und die möglichst totale Kontrolle über alles, was innerhalb Ihrer IT-Infrastruktur passiert und gefährlich werden könnte. Zusätzlich gibt es zahlreiche Gesetze und Verordnungen wie zum Beispiel das Bundesdatenschutzgesetz, die DSGVO, SOX, ISO, Basel II oder PCI DSS. Sie verkomplizieren die Berichtsstruktur und das Schwachstellen-Management auch in Ihrem Unternehmen massiv.

Das wache Auge

dacoso Managed SIEM liefert Ihnen eine ganzheitliche Übersicht über den Status Quo Ihrer IT-Landschaft, und zwar mit Blick auf die technische und organisatorische IT-Sicherheit. Das erfolgt in Echtzeit oder rückblickend über einen bestimmten Zeitraum, den Sie definieren. Aus unserem Network & Security Operation Center (NOC/SOC) heraus erkennen wir sicherheitsrelevante Events und informieren Sie nach abgestuften Service-Levels.
So kann schnell und angemessen auf potentielle Gefahren reagiert werden.

Umfassende Kontrolle und Gefahren-Erkennung

Überwachung der gesamten Infrastruktur:

- Betriebssysteme
- Switches, Router, Sicherheitsanwendungen
- Benutzerverwaltung (AD, IDM, CASB)
- Gerätemanagement (MDM, Software-Entwicklungen)
- Unternehmensanwendungen

Exakte Daten-Analyse:

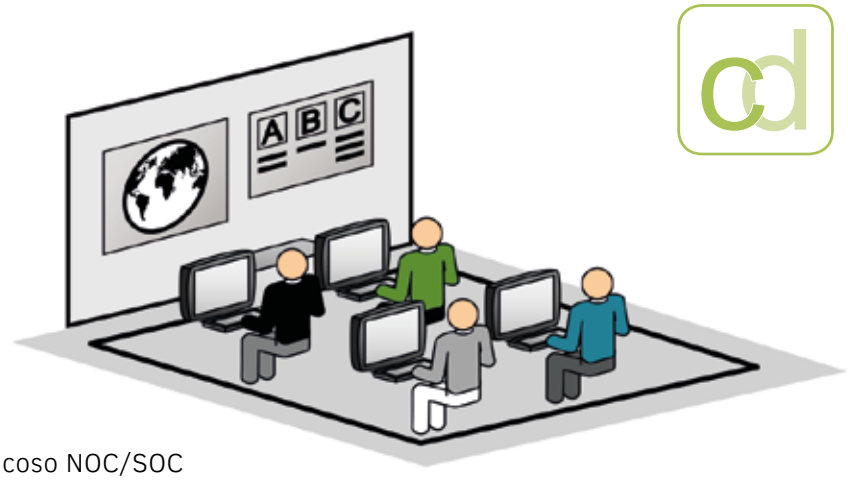
- Änderungen an Konfigurationen
- Änderungen an kritischen Systemdateien
- Zugang und Nutzung von Geschäftssystemen
- Benutzer- und Geräteverwaltung
- jede Aktion, die von privilegierten Benutzern ausgeführt wird
- potenziell „gefährliche“ Aktivitäten, die auf Datenspeichern mit sensiblen Daten durchgeführt werden
- Sitzungsdaten von Netzwerk-Sensoren

Aussagekräftige Reports:

- für Compliance-Anforderungen, Audits, ISO-Zertifizierungen u.a.
- für die Dokumentation vorgenommener Maßnahmen (Nachweispflicht)
- als Grundlage zur forensischen Untersuchung im Fall eines Vorfalls

Nur europäische Anbieter

Zum Einsatz kommt ausschließlich Software von Herstellern, die ihren Sitz in Europa haben und Erfahrung mit Kunden auch aus sicherheitskritischen Segmenten nachweisen können. Damit Kundendaten auf keinen Fall weitergegeben werden, ist uns der Verzicht auf „call-home“ wichtig.



d dacoso NOC/SOC

Managed SIEM im dacoso NOC/SOC

Die SIEM-Lösung ist Bestandteil unseres Network & Security Operation Centers. Die Sicherheits-Experten dort nehmen die Kontroll-Verantwortung von Ihren Schultern: Sie sparen Ressourcen in Ihrem IT-Team und können sich auf das Know-how unserer erfahrenen Security-Spezialisten verlassen. Vorfälle werden schnell und richtig beurteilt, auffällige Wiederholungen gehen als Expertenregeln in die Kontrollmechanismen ein, neue Compliance-Anforderungen werden in Absprache mit Ihnen umgehend berücksichtigt. Das Reporting der Überwachung und der einzelnen Aktionen richtet sich selbstverständlich exakt nach dem Bedarf in Ihrem Unternehmen. Wir haben dafür vier Service-Levels entwickelt, die vom Basis-Monitoring bis hin zur aktiven Hilfe bei Sicherheits-Problemen reichen.

Nach BSI-Vorgaben

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) haben wir für unser NOC/SOC das „ISO 27001-Zertifikat auf Basis von IT-Grundschutz“ erhalten. Damit sind wir als Dienstleister definiert, der für „Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen“ sorgt. Für unsere Kunden mit aufwändigen Sicherheits- oder auch speziellen KRITIS-Anforderungen ist dieses Siegel das Zeichen für eine technisch ausgereifte und verlässliche Überwachungslösung.

Vorteile NOC/SOC

- 24/7 bedienter Betrieb
- alle Services bei Bedarf gemäß den hohen Anforderungen des BSI
- modulares Konzept: NOC/SOC-Dienste sind frei wählbar
- Hochsicherheitscontainer für alle Überwachungs-Server und Netzwerk-Komponenten
- optionaler NOC-Support im Fehlerfall: von der Beratung bis hin zur Ersatzteil-Lieferung
- NOC/SOC-Management von Deutschland aus, mit hier ausgebildeten Technikern
- durchgängig deutschsprachiger Support, bei Bedarf auch in Englisch

- transparente und nach BSI IT-Grundschutz definierte Prozesse
- nach BSI IT-Grundschutz ausgewählte Tool-Landschaft
- EU-DSGVO, GDPR – sichergestellt durch Tools und Zertifikat
- Sicherstellung, dass empfohlene präventive Maßnahmen dem BSI IT-Grundschutz entsprechen

dacoso Cyber Defence

Wir begleiten Sie gerne auf Ihrem Weg zu einer ganzheitlichen Sicherheits-Strategie und beraten Sie auf allen relevanten Ebenen. Zusammen mit Ihnen suchen wir die besten und auch wirtschaftlich effizienten Lösungen für einen umfassenden Schutz Ihrer Unternehmensdaten. Wir werfen von außen einen Blick auf Ihr bisheriges Gerüst und unterstützen Sie bei der Auswahl neuer Maßnahmen, die wir als Managed Security Service Provider auf Wunsch auch umsetzen. Zu unserem Ansatz gehören außerdem Schulungen und Workshops, in denen wir Ihrem Team unser Wissen rund um IT Security weitergeben.

dacoso
data communication solutions

dacoso GmbH
Deutschland | Robert-Bosch-Str. 25a | D-63225 Langen | T +49 6103 404 569 0
Schweiz | Riedstr. 1 | CH-8953 Dietikon | T +41 44 371 78 77
Österreich | Am Europlatz 2 | A-1120 Wien | T +43 1 717 28 324
info@dacoso.com | www.dacoso.com

LBR-SIEM-1905 | Fotos: Axel Boesten