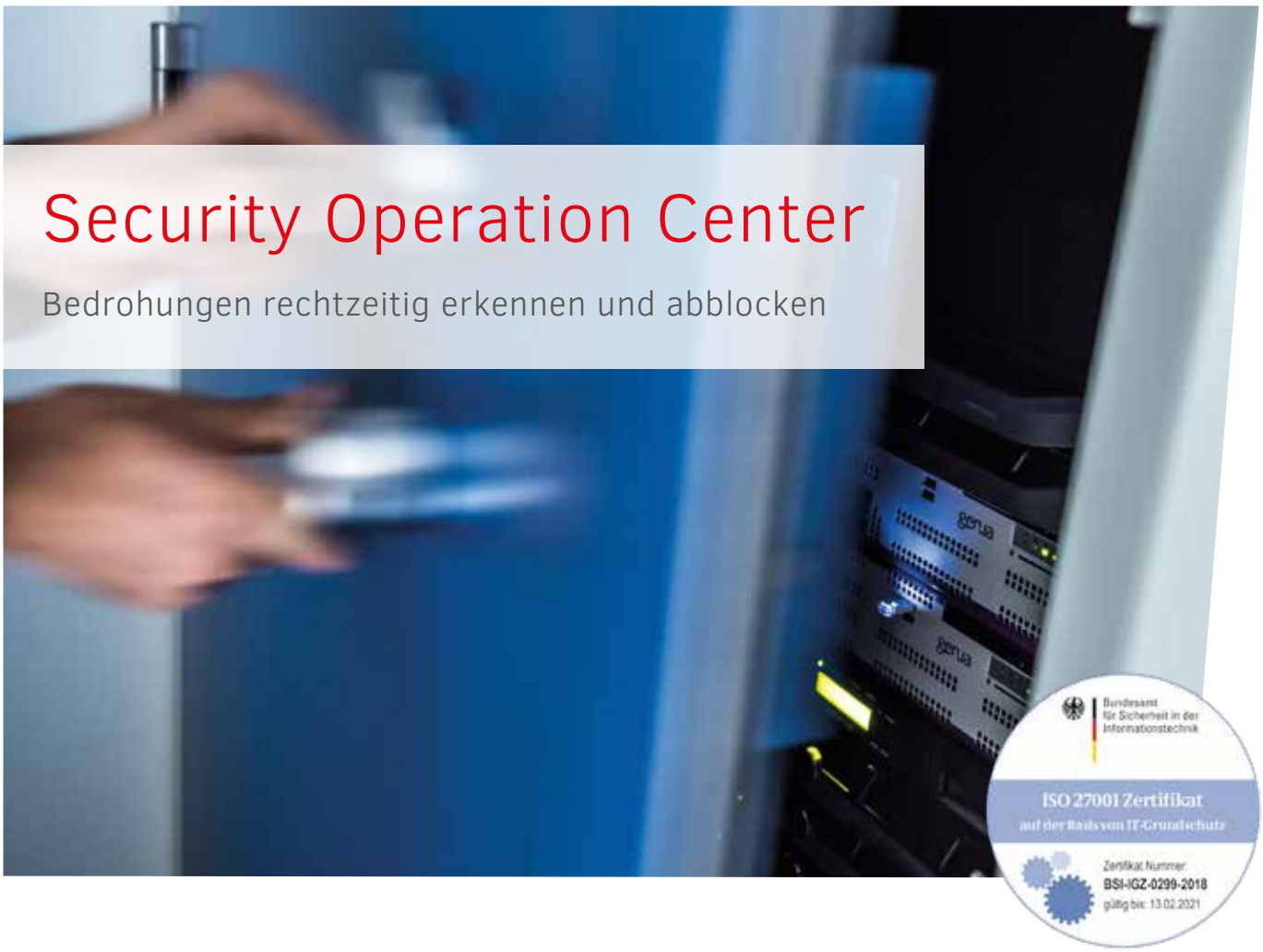
dacoso
data communication solutions



Security Operation Center

Bedrohungen rechtzeitig erkennen und abblocken

Angriffe werden immer raffinierter

Sicherheit ist für viele Unternehmen inzwischen die Achillesferse. Stabilität bleibt und Erfolg gelingt nur, wenn der Schutz der eigenen Daten gewährleistet ist. Das aber wird zunehmend schwieriger, weil Datensaboteure extrem skrupellos agieren. Durch E-Mails, USB-Sticks oder durch den Abruf manipulierter Webseiten gelangen Viren, Trojaner und sonstige Malware in die Unternehmensnetze und richten großen Schaden an. Über externe Zugänge manipulieren Angreifer Netzwerk-Komponenten, um so auch Zugriff auf vernetzte Applikations-Server zu erhalten. Oft reichen schon „Denial-of-Service-Attacken“ aus, um durch die Blockade von Anwendungen ganze Geschäftszweige lahmzulegen.

Kontrolle und schnelle Reaktion

Es führt kein Weg daran vorbei: Wenn Sie Ihr Unternehmen umfassend schützen wollen, müssen Sie Ihre sicherheitsrelevanten Systeme und Anwendungen kontinuierlich im Blick haben. Und parallel sollten Sie in der Lage sein, im Angriffsfall sofort aktiv zu werden. Dafür braucht es die richtigen Tools und geschulte Experten mit dem Arbeitsfokus IT-Sicherheit. Unser BSI-zertifiziertes Security Operation Center ist so modular konzeptioniert, dass es genau zu Ihren Anforderungen passt.

Abwehr + Prävention

In unserem SOC überwachen wir alle Aktivitäten in Netzwerken mit dem Ziel, Anomalien sofort zu erkennen. Dabei arbeiten wir nicht nur über unsere eigene Security-Plattform, sondern integrieren bei Bedarf auch Ihre bestehenden Lösungen. Unternehmen, die nicht selbst in aufwändige Tools und eine Experten-Mannschaft investieren wollen, haben also mit uns eine Alternative zum eigenen Betrieb eines Security Operation Centers. Als MSSP (Managed Security Service Provider) bringen wir dafür die richtige Expertise und die nötige Erfahrung mit.

Unser SOC-Team behält Ihre wichtigen Applikationen im Blick und ist darin geschult, auch neue, unbekannte Sabotage-Methoden schnell zu enttarnen. Sollte sich ein Problem nicht direkt abwenden lassen, alarmieren wir sofort und unterstützen ggf. bei der Wiederherstellung.

Unsere SOC-Aufgaben richten sich nach Ihrem Bedarf.

Hier einige Beispiele:

- Alarmierung bei bedenklichen oder vordefinierten Auffälligkeiten
- Orchestrierung, Automatisierung und Reaktion auf Vorfälle in Echtzeit mit unserer Security-Information- und Event-Management-(SIEM)-Plattform
- Next Generation End Point Security mit Machine Learning
- Asset & Device Management für Network Access Control
- Zwei-Faktor-Authentifizierung
- komponentenbezogene Schwachstellenanalyse, von innen und außen
- Unterstützung bei der Isolation und dem Restore der betroffenen Systeme und Netze

Zertifiziert durch das BSI

Das dacoso Security Operation Center hat vom BSI (Bundesamt für Sicherheit in der Informationstechnik) das „ISO 27001-Zertifikat auf Basis von IT-Grundschutz“ erhalten. Damit ist amtlich bestätigt, dass wir „für Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen“ (BSI) sorgen. Nicht nur für sicherheitsbetreute Unternehmen, sondern für alle Firmen, die ihre Daten zuverlässig schützen wollen, ist das BSI-Siegel der überzeugende Nachweis für Sicherheit auf höchstem Niveau.

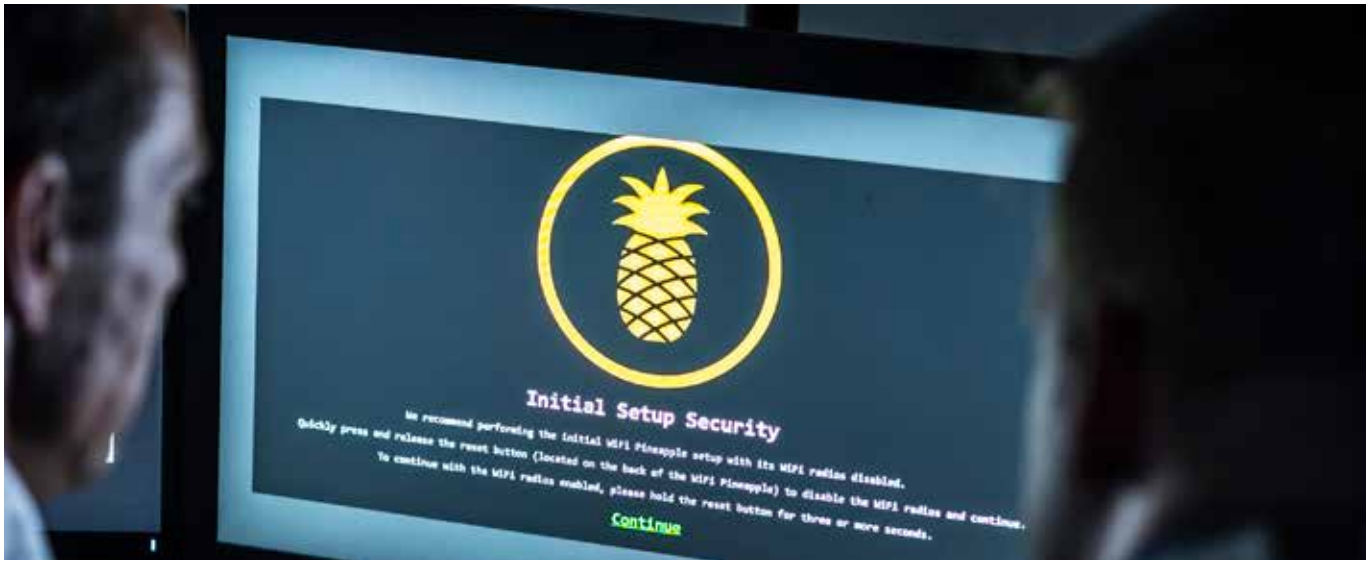
Vorteile SOC

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

Flexible Preismodelle

Wenn Sie unser SOC nutzen, profitieren Sie von OPEX-Vorteilen, da Sie nicht selbst investieren. Die Kosten werden über eine monatliche Nutzungsmiete in Rechnung gestellt. Der Preis reguliert sich natürlich auch noch nach unterschiedlichen Gesichtspunkten, beispielsweise:

- gewünschte Aufgaben und Verantwortlichkeiten
- Anzahl der zu überwachenden Standorte
- SLA-Vorgaben (Reaktionszeiten, Eskalationszeiten)
- Mindestvertragslaufzeit

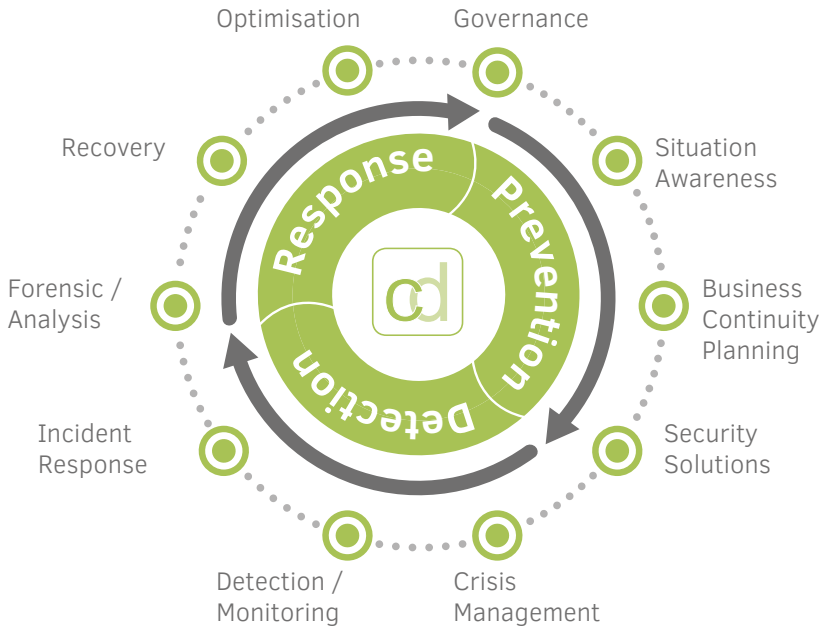


Die Ergänzung: Network Operation Center (NOC)

In unserem NOC stehen insbesondere Ihre Netzverbindungen und die eingesetzte Hardware unter professioneller Kontrolle. Unsere NOC-Mitarbeiter werden sofort aktiv, wenn sich Probleme abzeichnen und sorgen für die Wiederherstellung der Systeme. Die Aufgaben im Wesentlichen:

- Hardware und Verbindungen überwachen
- Netzwerke provisionieren und konfigurieren
- Netzwerke betreiben und auf aktuellem Stand halten
- Fehler proaktiv vorhersehen
- bei Sicherheitsproblemen sofort alarmieren
- die Instandsetzung frühzeitig einleiten

In das NOC können wir unterschiedliche Plattformen integrieren und Netzwerke unter ganz bestimmten Gesichtspunkten in den Blick nehmen. Dazu zählen beispielsweise die Netztechnologie von ADVA Optical Networking, das Carrier-Grade-Equipment von NOKIA oder der WAN-Optimizer von InfoVista (Ipanema). Außerdem die Verschlüsselungs-Lösungen von atmedia, deren reibungsloses Funktionieren durch die Überwachung sichergestellt wird. Auch für virtualisierte Netzwerke kommt das NOC zum Einsatz. Gerade bei diesen relativ neuen Netzwerk-Lösungen sind die richtigen Leute und die richtige Ausstattung für die Kontrolle der SD WANs gefragt.
Das dacoso-NOC wurde vom BSI mit ISO-27001 auf der Basis von IT-Grundschutz zertifiziert.



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-SOC-D-1904 | Fotos: Axel Boesten