EWE

Wirksamer Cyberschutz rund um die Uhr mit SOCaaS

Cyberkriminelle kennen keine Bürozeiten –
Ihr Schutz darf das auch nicht

Inhaltsverzeichnis

Die Bedrohungslage für Unternehmen – in Deutschland wie weltweit – ist alarmierend: Laut der Bitkom-Studie „Wirtschaftsschutz“ wurden 9 von 10 Unternehmen allein im vergangenen Jahr Opfer von Cyberangriffen. Zwei Drittel davon sehen sich durch diese Angriffe in ihrer Existenz bedroht. Der jährliche wirtschaftliche Schaden in Deutschland: über 266 Milliarden Euro.

Das Problem

Es gibt keinen 100-prozentigen Schutz vor Cyberangriffen

Keine IT-Sicherheitsmaßnahme kann verhindern, dass Angriffe überhaupt stattfinden. Neue Schwachstellen, menschliche Fehler oder ausgeklügelte Angriffsmethoden durchbrechen selbst modernste Schutzsysteme. Daher ist es nicht nur entscheidend, wie gut ein Angriff abgewehrt wird – sondern wie schnell er erkannt wird.

Die Lösung

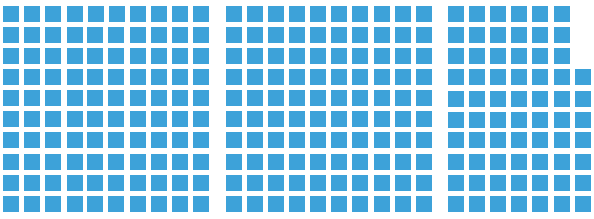
Rund-um-die-Uhr-Überwachung

Cyberangriffe erfolgen rund um die Uhr – automatisiert, KI-gestützt, in hoher Frequenz. Unternehmen müssen deshalb 24/7/365 ihre IT-Infrastruktur im Blick behalten. Ein Security Operations Center (SOC) bietet genau diesen Schutz: **Ein spezialisiertes Expertenteam analysiert kontinuierlich die Sicherheitslage Ihres Unternehmens, erkennt selbst kleinste Anomalien und reagiert sofort – bevor echter Schaden entsteht.**

Cyberbedrohung – Zahlen & Fakten

9 von 10
Unternehmen sind betroffen

2 von 3
sehen ihre Existenz bedroht



266,6 Mrd. €
jährlicher Schaden

Was ist ein Security Operations Center (SOC)?

Ein Security Operations Center – kurz SOC – ist das Herzstück moderner IT-Sicherheit. Es handelt sich um ein spezialisiertes Team von IT-Sicherheitsexpert:innen, das kontinuierlich – rund um die Uhr – alle sicherheitsrelevanten Aktivitäten in einem Unternehmen überwacht, analysiert und bei Bedrohungen sofort reagiert.

Wie funktioniert ein SOC?

Das SOC nutzt Daten aus verschiedensten Sicherheitslösungen – z. B. Firewall, Endpoint Protection – und kombiniert diese in einer zentralen Analyseplattform. Dort werden alle Ereignisse in Echtzeit bewertet. So lassen sich Angriffe frühzeitig erkennen, gezielt abwehren und Schwachstellen kontinuierlich beheben.

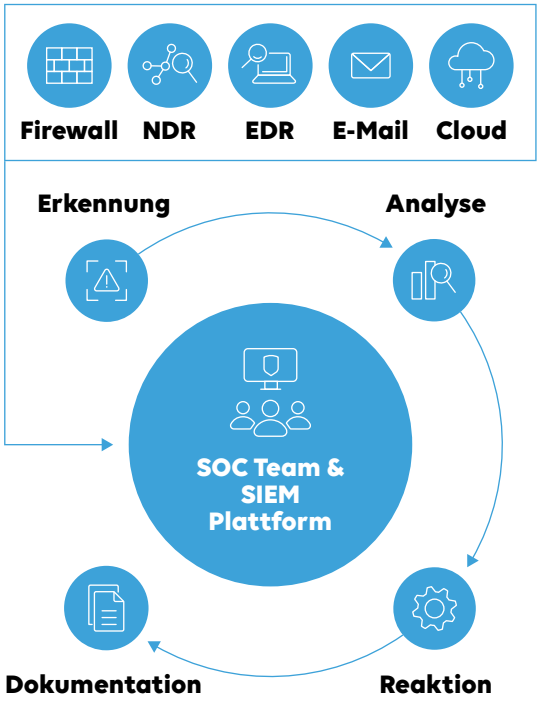
Ein SOC erkennt zum Beispiel:

- ungewöhnlich viele Zugriffsversuche aus dem Ausland in der Nacht
- plötzlichen Anstieg des Datenverkehrs
- verdächtige Aktivitäten auf Endgeräten
- unerlaubte Datenbankzugriffe durch interne Benutzer:innen

Der Schlüssel zum Erfolg:

Echtzeitüberwachung mit menschlicher Expertise und intelligenter Software. Denn im Ernstfall zählt jede Minute.

Wie arbeitet ein SOC?



»Je früher ein Angriff erkannt wird, desto geringer ist der potenzielle Schaden.«

Aufgaben und Datenquellen eines Security Operations Centers

Was genau macht ein SOC?

Ein Security Operations Center verfolgt das Ziel, Sicherheitsvorfälle so früh wie möglich zu erkennen, schnell darauf zu reagieren und den Gesamtschutz kontinuierlich zu verbessern. Dafür übernimmt das SOC vier zentrale Aufgabenbereiche:

1. Überwachung & Erkennung

Das SOC-Team beobachtet alle sicherheitsrelevanten Aktivitäten im Unternehmen in Echtzeit. Verdächtige Muster und Anomalien – etwa ungewöhnlicher Datenverkehr oder verdächtige Login-Versuche – werden sofort registriert.

2. Analyse & Bewertung

Jeder Alarm wird durch geschulte Analyst:innen geprüft, priorisiert und bewertet. Ist der Vorfall echt oder ein Fehlalarm? Welche Systeme sind betroffen? Wie groß ist das Risiko?

3. Reaktion & Koordination

Bei bestätigten Vorfällen leitet das SOC umgehend Gegenmaßnahmen ein – z. B. das Blockieren von IP-Adressen, das Isolieren von Endgeräten oder das Aktivieren von Notfallplänen. Interne IT-Verantwortliche und relevante Abteilungen werden eingebunden.

4. Dokumentation & Verbesserung

Alle Vorfälle werden lückenlos dokumentiert. Das SOC erstellt Reports, analysiert Trends, identifiziert Schwachstellen und hilft, die Sicherheitsstrategie kontinuierlich weiterzuentwickeln.

Welche Informationen analysiert ein SOC?

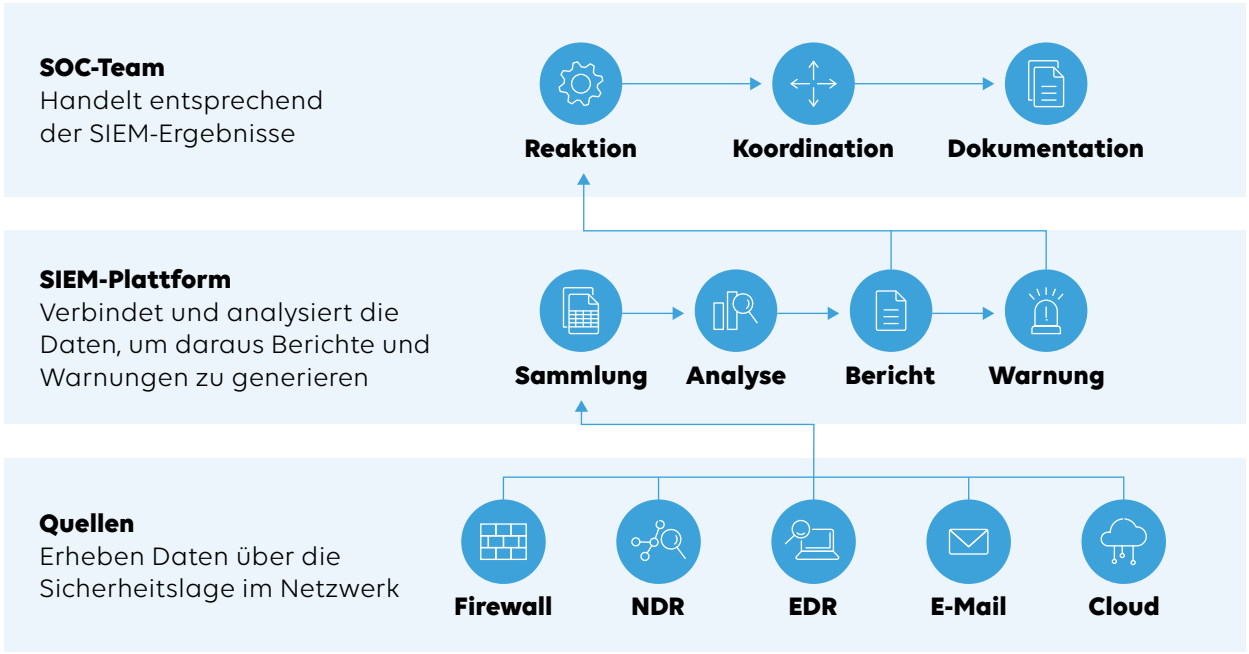
Damit das SOC einen vollständigen Überblick über die Sicherheitslage bekommt, benötigt es Daten aus unterschiedlichen Quellen. Beispiele ihrer Arbeit:

- Firewalls
- Kontrolle des eingehenden und ausgehenden Datenverkehrs
- Endpoint Detection & Response (EDR)
- Identifikation verdächtiger Aktivitäten auf Endgeräten
- Network Detection & Response (NDR)
- Überwachung und Analyse von Datenströmen im Netzwerk
- E-Mail-Security-Lösungen
- Filtern von Phishing, Malware und Spam
- Mobile & Endpoint Protection
- Schutz mobiler Geräte und Arbeitsstationen
- Intrusion Detection/Prevention Systeme (IDS/IPS)
- Diagnose und Abwehr von Angriffen auf Netzwerkebene
- Überwachung von Cloud-Security-Tools, Cloud-Anwendungen und Zugriffsmustern

Was macht ein SIEM-System?

Das SIEM (Security Information and Event Management) ist die zentrale Analyseplattform im SOC. Es sammelt die Rohdaten aus den oben genannten Quellen, normalisiert sie, korreliert zusammenhängende Ereignisse und erstellt auf dieser Basis Warnungen, Berichte und Risikoanalysen. **Ein SIEM ist also keine Quelle – sondern das „Gehirn" des SOC, das aus vielen Einzeldaten ein Gesamtbild erstellt.**

SOC-Quellen & SIEM-Plattform



Wie ist ein Security Operations Center aufgebaut?

Ein wirksames Security Operations Center ist mehr als nur Software und Monitore. Es ist ein ganzheitliches Zusammenspiel aus Menschen, Prozessen und Technologie – rund um die Uhr im Einsatz.

Damit ein SOC wirklich leistungsfähig ist, müssen vier Voraussetzungen erfüllt sein:

1. Das richtige Team – 24/7/365 im Einsatz

Cyberangriffe passieren nicht nur werktags zwischen 9 und 17 Uhr. Ein effektives SOC muss deshalb rund um die Uhr besetzt sein – auch nachts, an Wochenenden und an Feiertagen.

Dazu braucht es:

- Mindestens acht ausgebildete IT-Sicherheitsexpert:innen, um den Schichtbetrieb abdecken zu können.
- Ein stabiles Team mit klaren Rollen: Analyst:innen, Incident Responder, SOC-Leitung.
- Laufende Weiterbildung zu neuen Angriffsmethoden, Technologien und Compliance-Vorgaben.

2. Fachliches Know-how

Die Teammitglieder müssen in der Lage sein, große Datenmengen aus verschiedenen Quellen zu bewerten, Angriffsmuster zu erkennen und Sofortmaßnahmen abzuleiten. Erfahrung, kontinuierliche Schulung und ein tiefes Verständnis von IT-Security sind Pflicht.

3. Die passende Technologie

Ein modernes SOC benötigt eine leistungsstarke, skalierbare Infrastruktur mit:

- Einem zentralen SIEM-System.
- Integrationen zu allen sicherheitsrelevanten Systemen (EDR, Firewall, NDR, etc.).
- Automatisierungsfunktionen für schnelle Reaktionsprozesse (z. B. über SOAR).
- Die Plattform muss übersichtlich, kompatibel und anpassbar an individuelle Unternehmensbedürfnisse sein.

4. Ausreichende Ressourcen & Budget

Der Aufbau eines Inhouse-SOC erfordert erhebliche Investitionen:

Fachpersonal:
~ 1.000.000 € pro Jahr

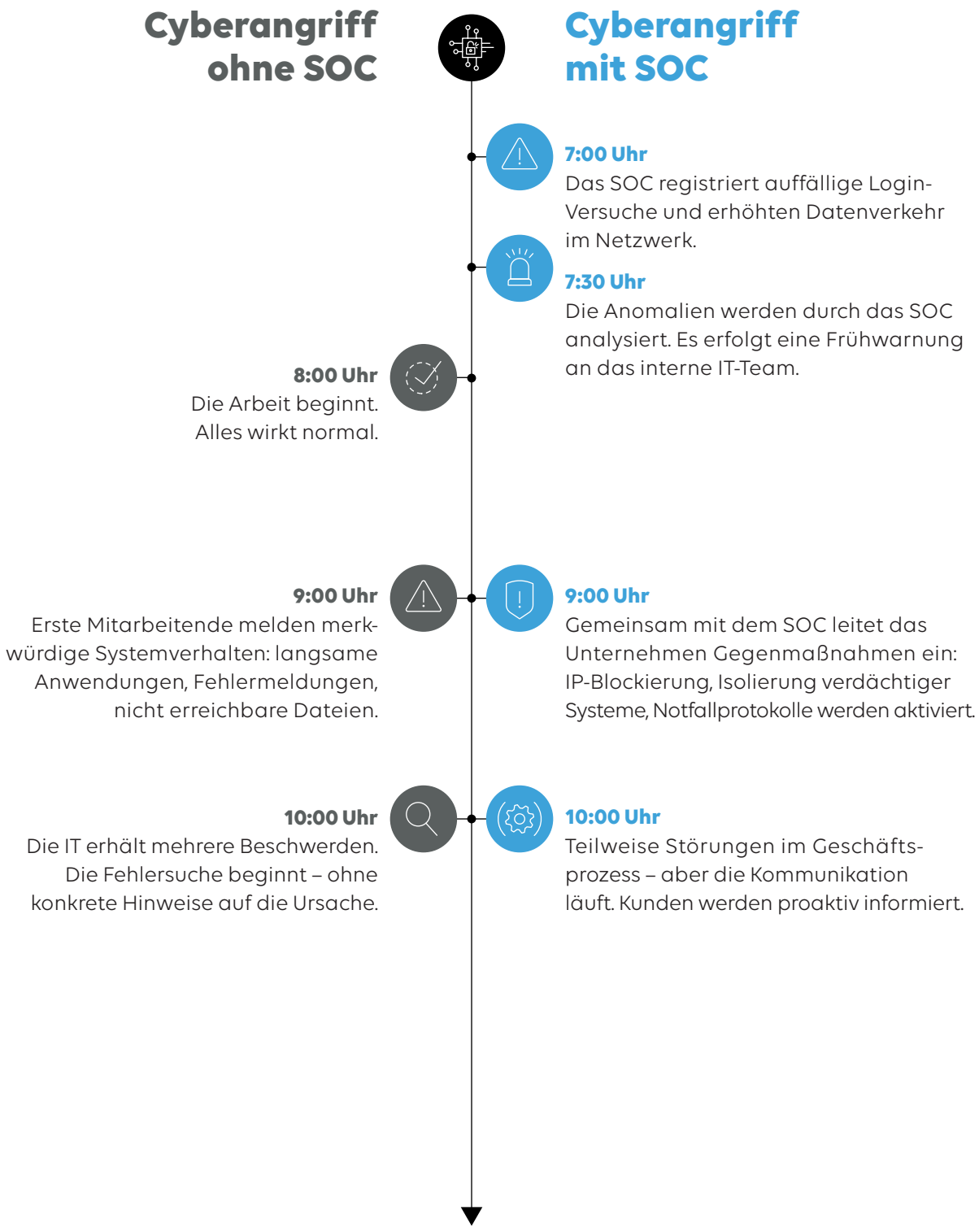
Technologie & Software:
~ 250.000 € pro Jahr

Zeitaufwand:
6–12 Monate Implementierungsphase

In Zeiten von Fachkräftemangel und steigender Bedrohungslage ist das für viele Unternehmen eine große Herausforderung – oft auch ein Argument für SOC-as-a-Service (siehe Seite 11).

Cyberangriff – mit und ohne SOC

Reaktionsgeschwindigkeit ist alles. Cyberangriffe treffen Unternehmen oft ohne Vorwarnung – und sie entfalten ihre Wirkung in wenigen Stunden. Der Unterschied zwischen einem katastrophalen Vorfall und einer kontrollierten Situation liegt in der Früherkennung und schnellen Reaktion. **Hier zeigt sich der wahre Wert eines Security Operations Centers.**



12:00 Uhr
Die Bedrohung ist eingedämmt. Betroffene Systeme werden bereinigt und schrittweise wieder in Betrieb genommen.

13:00 Uhr
Es steht fest: Das Unternehmen wurde kompromittiert. E-Mail, Telefonie, Datenbanken – alles muss abgeschaltet werden. Kunden und Partner sind betroffen.

14:00 Uhr
Die IT versucht, den Schaden zu begrenzen. Externe Dienstleister werden kurzfristig angefragt. Wertvolle Zeit vergeht.

18:00 Uhr
Mit externer Hilfe beginnt die Eindämmung. Systeme werden schrittweise isoliert und untersucht.

Nächster Tag
Erste Erkenntnisse zeigen: Kundendaten wurden entwendet, interne Informationen kompromittiert. Die Medien berichten. Kunden sind verunsichert.

Langfristig
Die Wiederherstellung dauert Wochen. Es entstehen Millionenschäden durch Produktionsausfall, Rechtsstreitigkeiten, Reputationsverluste und Bußgelder.

Folgetage
Das SOC erstellt eine forensische Analyse, empfiehlt Optimierungen und dokumentiert den Vorfall für interne und gesetzliche Zwecke.

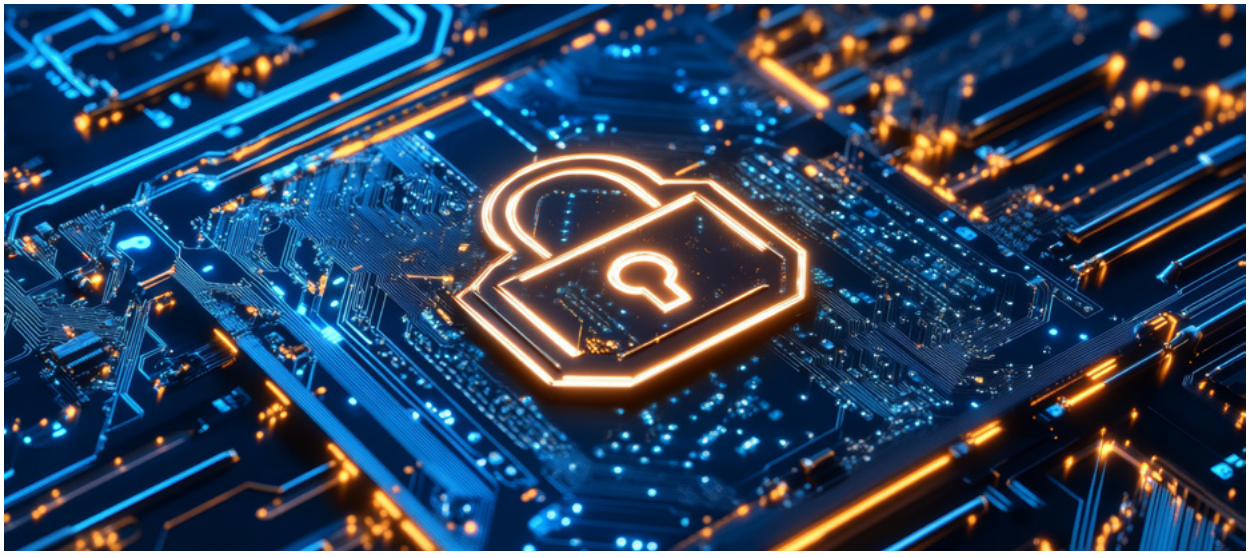
Langfristig
Keine gravierenden Schäden, keine Datenverluste. Kundenvertrauen bleibt bestehen. Der Betrieb läuft stabil weiter.

Vorteile eines Security Operations Centers auf einen Blick

Ein SOC ist nicht nur eine technische Sicherheitsmaßnahme – es ist ein strategisches Sicherheitskonzept, das Unternehmen in ihrer gesamten digitalen Resilienz stärkt. Hier die wichtigsten Vorteile auf einen Blick:

Checkliste: Warum ein SOC unverzichtbar ist

- ☑ Rund-um-die-Uhr-Schutz
- ☑ 24/7/365-Überwachung aller sicherheitsrelevanten Systeme durch erfahrene Expert:innen
- ☑ Frühzeitige Erkennung von Angriffen
- ☑ Anomalien werden sofort erkannt – bevor sie Schaden anrichten
- ☑ Minimale Reaktionszeiten
- ☑ Schnelle, koordinierte Gegenmaßnahmen verhindern Eskalationen
- ☑ Ganzheitlicher Überblick
- ☑ Zentrale Auswertung sämtlicher Sicherheitsdaten aus IT- und OT-Systemen
- ☑ Identifikation von Schwachstellen
- ☑ Erkennung von wiederkehrenden Mustern und potenziellen Sicherheitslücken
- ☑ Kontinuierliche Bedrohungsanalysen
- ☑ Frühzeitiges Erkennen und Berücksichtigen von Trends und neuen Angriffsmethoden
- ☑ Dokumentation & Reporting
- ☑ Lückenlose Nachverfolgung und Nachweisbarkeit für Audits, Prüfungen und Gesetzesvorgaben.
- ☑ Rechtssicherheit & Compliance
- ☑ Unterstützung bei der Einhaltung von Vorgaben wie DSGVO, NIS2 und branchenspezifischen Regularien.
- ☑ Stärkung von Vertrauen & Reputation
- ☑ Transparenz gegenüber Kund:innen, Partner:innen und Mitarbeitenden erhöht die Glaubwürdigkeit.



Inhouse-SOC vs. SOC-as-a-Service

Ein Security Operations Center ist ein wesentlicher Baustein moderner Cybersicherheit. Doch wie sollte es betrieben werden? Eigenständig im Unternehmen (Inhouse-SOC) oder ausgelagert an einen spezialisierten Dienstleister (SOC-as-a-Service / SOCaaS)?

Beide Modelle haben ihre Berechtigung – aber ihre Anforderungen und Vorteile unterscheiden sich deutlich.

Inhouse-SOC – maximale Kontrolle, hoher Aufwand

Vorteile:

- Volle Kontrolle über Datenflüsse & Prozesse
- Integration in bestehende Strukturen und IT-Teams
- Möglichkeit zur Individualisierung der Workflows

Aber:

Der Aufbau ist komplex, teuer und ressourcenintensiv.

Notwendig sind unter anderem:

- Mind. 8 FTE an IT-Sicherheitsexpert:innen
- Umfangreiche Investitionen in Infrastruktur, Software, Monitoring
- Laufende Schulung & Weiterentwicklung der Mitarbeitenden

Geeignet für:

Sehr große Unternehmen mit eigener IT-Security-Abteilung, hoher Sensibilität für Datenhoheit und ausreichend Budget + Personal.

SOC-as-a-Service – Sicherheit mit Skalierbarkeit

SOC-as-a-Service (SOCaaS) bedeutet, den Betrieb eines SOC an einen spezialisierten Anbieter auszulagern. Dieser übernimmt 24/7-Überwachung, Analyse, Reaktion und Reporting – professionell, skalierbar und effizient.

Vorteile:

- Sofort verfügbar, ohne Aufbauphase
- Zugang zu aktueller Technologie und Expertenwissen
- Planbare Kosten durch monatliche Pauschalmodelle
- Kontinuierliche Weiterentwicklung durch den Anbieter
- Kein Risiko durch Personalfluktuation oder Fachkräftemangel

Geeignet für:

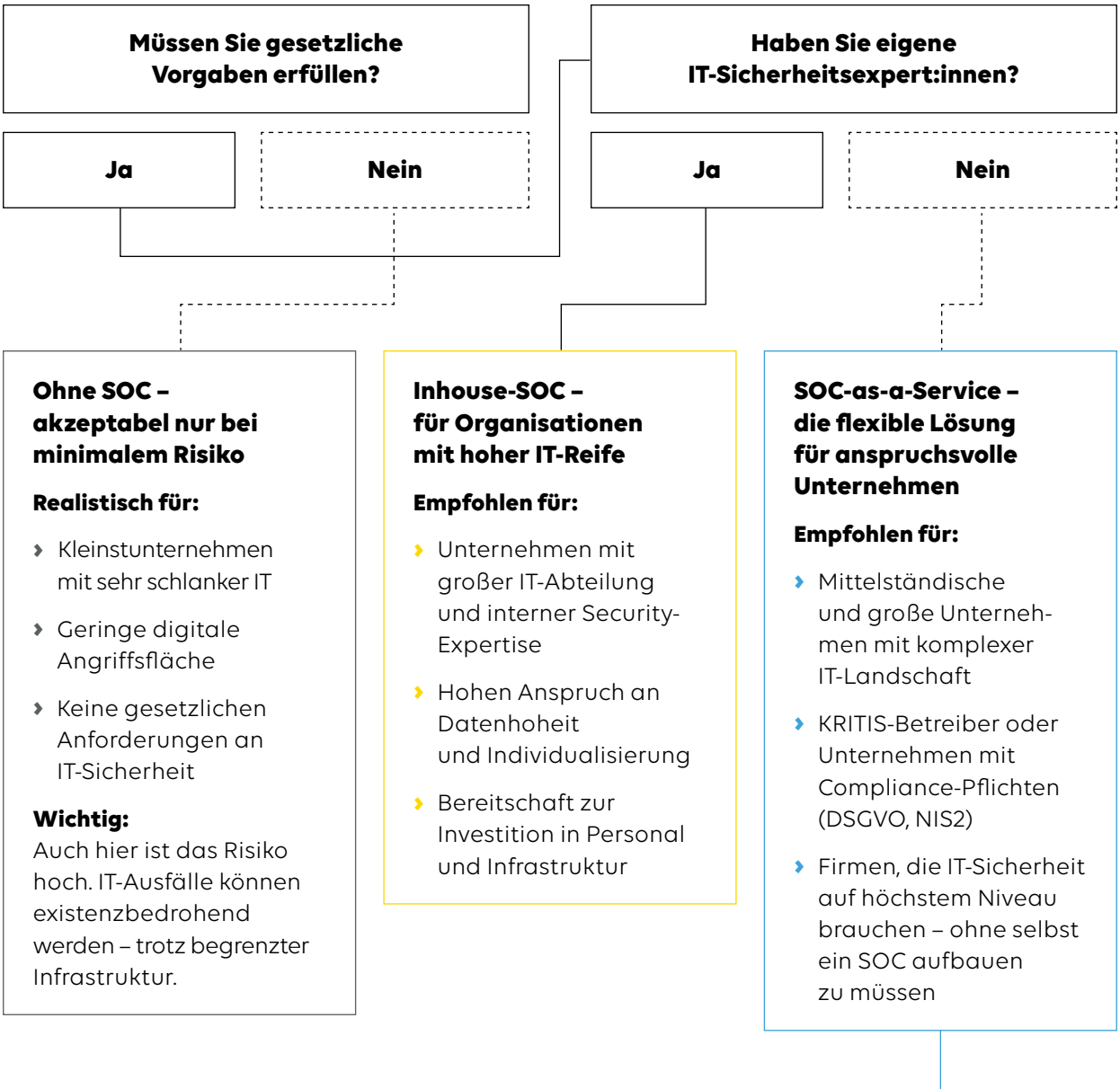
Mittelständische und große Unternehmen sowie KRITIS-Betreiber, die keine internen Ressourcen für ein eigenes SOC aufbauen können oder wollen.

Fazit: Entscheidung nach Kapazität und Risiko

Die Entscheidung für ein Inhouse-SOC oder SOCaaS hängt von **Budget, internen Kompetenzen, Sicherheitsbedarf** und **Compliance-Anforderungen** ab. Für viele Unternehmen bietet ein professioneller SOCaaS-Anbieter den besten Schutz bei maximaler Flexibilität und planbaren Kosten – ohne eigene Sicherheitsinfrastruktur aufbauen zu müssen.

Fazit: Welches SOC-Modell passt zu Ihrem Unternehmen?

Nicht jedes Unternehmen hat die gleichen Anforderungen, Ressourcen oder Sicherheitsrisiken. Die Wahl des passenden SOC-Modells sollte sich daher nach Größe, IT-Komplexität und Sicherheitsbedarf richten. Hier eine praxisnahe Einordnung:



Ohne SOC – akzeptabel nur bei minimalem Risiko

Realistisch für:

- Kleinstunternehmen mit sehr schlanker IT
- Geringe digitale Angriffsfläche
- Keine gesetzlichen Anforderungen an IT-Sicherheit

Wichtig:
Auch hier ist das Risiko hoch. IT-Ausfälle können existenzbedrohend werden – trotz begrenzter Infrastruktur.

Inhouse-SOC – für Organisationen mit hoher IT-Reife

Empfohlen für:

- Unternehmen mit großer IT-Abteilung und interner Security-Expertise
- Hohen Anspruch an Datenhoheit und Individualisierung
- Bereitschaft zur Investition in Personal und Infrastruktur

SOC-as-a-Service – die flexible Lösung für anspruchsvolle Unternehmen

Empfohlen für:

- Mittelständische und große Unternehmen mit komplexer IT-Landschaft
- KRITIS-Betreiber oder Unternehmen mit Compliance-Pflichten (DSGVO, NIS2)
- Firmen, die IT-Sicherheit auf höchstem Niveau brauchen – ohne selbst ein SOC aufbauen zu müssen

Wer keine eigenen IT-Sicherheitsressourcen aufbauen kann oder will, trifft mit einem SOC-as-a-Service eine zukunftssichere, wirtschaftlich planbare Entscheidung – bei maximaler Sicherheit.

Übersicht der SOC-Modelle

	Kein SOC	Inhouse-SOC	SOCaaS
Überwachung rund um die Uhr	Nicht vorhanden	Möglich bei ausreichendem Personal	Vollständig gewährleistet durch externes Expertenteam
Reaktionsgeschwindigkeit	Langsam, reaktiv	Geplant und intern koordiniert	Sehr schnell, professionell abgestimmt
Sicherheitsniveau	Gering	Hoch, bei guter Ressourcenausstattung	Sehr hoch, 24/7 und mit Erfahrung & Technologien
Initiale Kosten	Gering	Sehr hoch (Personal, Infrastruktur, Tools)	Planbar, meist monatliche Pauschalen
Laufende Betriebskosten	Unkalkulierbar (Folgekosten durch Schäden)	Hoch (Schulungen, Wartung, Personalbindung)	Gut planbar, geringer interner Aufwand
Skalierbarkeit	Nicht gegeben	Begrenzt durch internes Team	Hoch, flexibel anpassbar
Zugang zu aktueller Technologie	Kaum vorhanden	Träge durch lange Upgradezyklen	Immer auf dem neuesten Stand
Personalbedarf	Kein eigenes Security-Team	Min. 8 FTE erforderlich	Keine internen Ressourcen notwendig
Compliance (z. B. NIS2, DSGVO)	Kaum erfüllbar	Aufwändig, aber machbar	Vollumfängliche Unterstützung
Reputationsschutz und Vertrauen	Hohe Risiken	Stark bei stabiler Besetzung	Nachhaltig durch professionelle Kommunikation

Wie EWE Sie unterstützen kann

Die Einführung eines Security Operations Centers – ob als Inhouse-Lösung oder als Service – ist eine strategische Entscheidung. Sie soll Ihr Unternehmen nicht nur vor aktuellen Bedrohungen schützen, sondern auch langfristig sicher und handlungsfähig halten. EWE unterstützt Sie dabei – mit Expertise, Erfahrung und konkreten Lösungen.

Unsere Leistungen für Sie:

Beratung & Bedarfsanalyse

Wir analysieren Ihre aktuelle Sicherheitsarchitektur und identifizieren gemeinsam mit Ihnen den passenden Weg zu mehr Resilienz.

Konzept & Architekturplanung

Ob punktuelle Absicherung oder ganzheitliches SOC-Modell – wir entwickeln mit Ihnen ein Konzept, das zu Ihrer Organisation passt.

Betrieb & Weiterentwicklung

Unser Expertenteam übernimmt auf Wunsch Betrieb, Wartung und kontinuierliche Weiterentwicklung Ihrer Sicherheitslösung – vollständig oder in Teilbereichen.

Compliance & Auditfähigkeit

Wir helfen Ihnen dabei, regulatorische Anforderungen (z. B. DSGVO, NIS2) zuverlässig zu erfüllen – mit vollständiger Dokumentation und regelmäßigen Reports.

»

Unser Ziel: ein Sicherheitsniveau, das mit Ihrem Unternehmen mitwächst – nicht ausbremst.

«

Über EWE – Ihr Partner für digitale Sicherheit mit Substanz

Als regional verwurzelter IT- und Telekommunikationsanbieter mit jahrzehntelanger Erfahrung kennen wir die Anforderungen von Unternehmen im digitalen Wandel genau – vom Mittelstand bis zur kritischen Infrastruktur. Mit unserer Expertise und Infrastruktur sorgen wir nicht nur für verlässliche Konnektivität, sondern auch für ganzheitliche Sicherheitslösungen, die mit Ihren Anforderungen wachsen.

Warum EWE?

KRITIS-erprobt & sicherheitszertifiziert

Als Teil des EWE Konzerns – einem der größten KRITIS-Unternehmen in Deutschland – erfüllen wir höchste Anforderungen an Verfügbarkeit, Ausfallsicherheit und Datenschutz. Dieses Know-how geben wir direkt an unsere Kund:innen weiter.

100 % in Deutschland – 100 % vertrauenswürdig

Unsere Rechenzentren, Service-Teams und Datenströme befinden sich ausschließlich in Deutschland – keine Cloud-Umwege, keine Datenabflüsse ins Ausland. Das sorgt für Transparenz, Datenschutzkonformität und Vertrauen.

Ein Ansprechpartner, viele Lösungen

Von der Glasfaserleitung über SD-WAN bis zum SOCaaS – wir bieten alles aus einer Hand. Damit vermeiden Sie Schnittstellenprobleme, Beschaffungsstress und Sicherheitslücken durch fragmentierte Systeme.

Ihr persönlicher Ansprechpartner:

David Brieskorn
IT-Security Experte

@ david.brieskorn@ewe.de
0162 1385546

Schneller Service – mit echtem Menschenkontakt

Wir betreuen unsere Geschäftskund:innen persönlich, lösungsorientiert und mit kurzen Reaktionszeiten. Unser Service ist kein anonymes Callcenter – sondern ein echter Partner mit Verantwortungsbewusstsein.

Unser Leistungsspektrum im Überblick

- Managed Security Services: Firewall, DDoS-Schutz, Endpoint Protection, Awareness-Schulungen, SOC as a Service
- Sichere Standortvernetzung: MPLS, SD-WAN, VPN
- Rechenzentrumsservices: Housing, Hosting, Plattformlösungen
- Individuelle Sicherheitsarchitekturen: Beratung, Konzeption, Betrieb
- Direktanbindung an das EWE-IP-Backbone: Mehrfach redundant, hochverfügbar
- Ob Sie Ihre IT-Sicherheit neu aufstellen oder auf das nächste Level bringen wollen – wir begleiten Sie dabei verlässlich, pragmatisch und zukunftssicher.

Sichern Sie sich jetzt Ihre persönliche Sicherheitsberatung – unverbindlich und individuell auf Ihre IT-Landschaft abgestimmt.