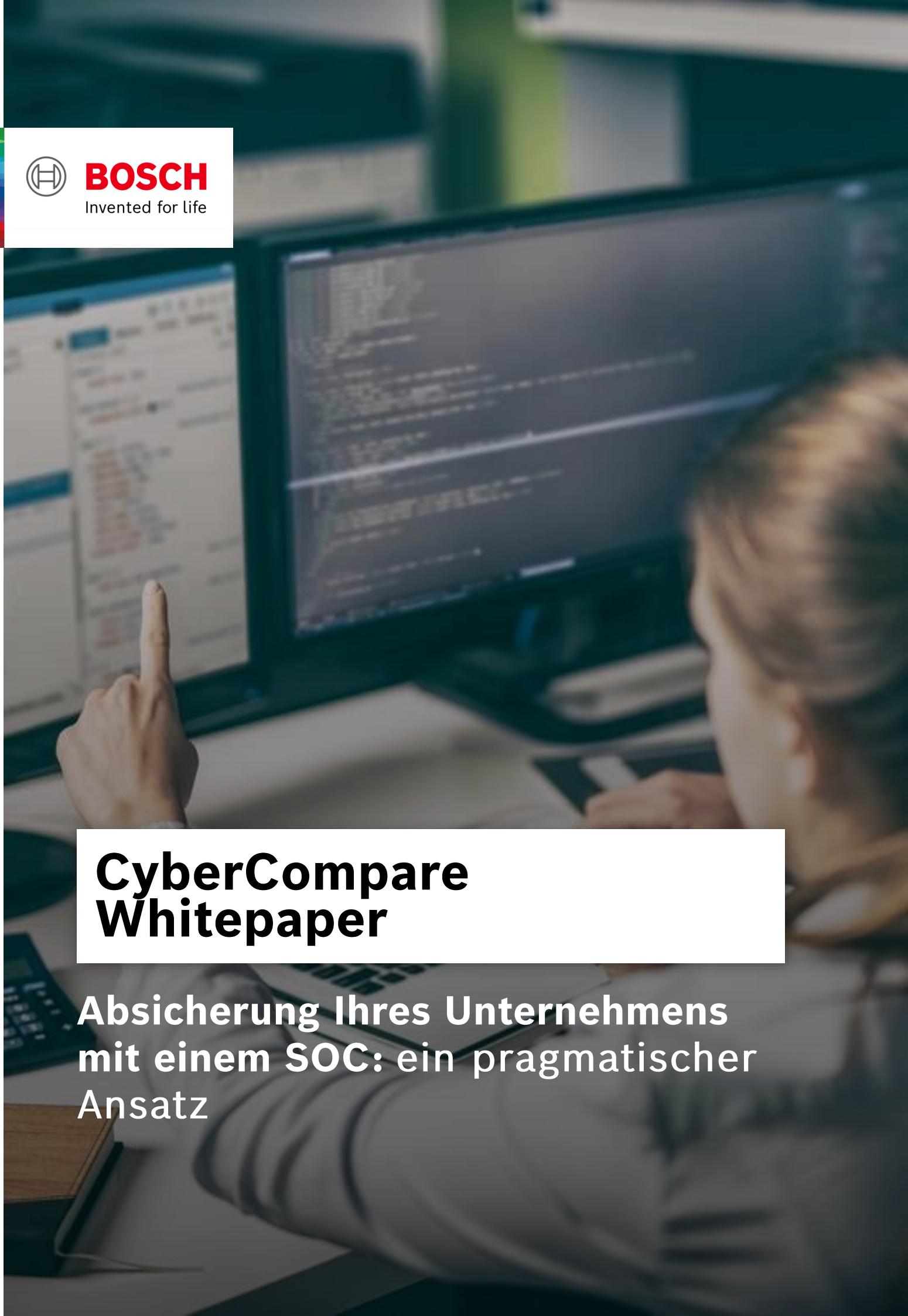


BOSCH
Invented for life

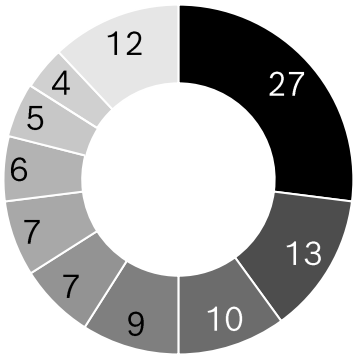
CyberCompare Whitepaper

Absicherung Ihres Unternehmens mit einem SOC: ein pragmatischer Ansatz

Einleitung

Cybersicherheit hat inzwischen auf der Vorstandsagenda oberste Priorität und die Besorgnis über Cyberangriffe nimmt täglich zu (Abbildung 1). Keine Branche ist davor gefeit und die COVID-19-Krise hat die Schwere und das Ausmaß der Angriffe noch verstärkt.

Abbildung 1



Branchen, die Ziel von Cyberangriffen waren, USA, 2016 - 2020
in Prozent

- Finanzinstitute
- Öffentliche Verwaltung
- Gesundheitswesen
- Bildung & Forschung
- Produktion
- Software- und Technologiedienstleistungen
- Unternehmensdienstleistungen
- Einzelhandel
- Versorgungsindustrie
- Sonstige

Organisationen aller Art sind insbesondere in Zeiten der Pandemie mit neuen Schwachstellen konfrontiert. Da viele von ihnen rasch auf ein Remote-Modell umsteigen mussten, hat sich die Angriffsfläche rapide vergrößert. B2C-Unternehmen konzentrieren sich auf die Schaffung neuer digitaler Kundenerlebnisse sowie die Anwendung fortschrittlicher Datenanalysen und investieren in zahlreiche andere technische Innovationen – diese Aktivitäten können aber Einfallstore für Cyberangriffe sein. Auch B2B Unternehmen, insbesondere im industriellen Bereich, setzen zunehmend Maschinen für die Prozessautomatisierung ein. Dies führt in den Bereichen Operational Technology (OT) und Internet of Things (IoT) zu einer immer größeren Zahl von Endpoints, die gesichert werden müssen. Große Produktionsstandorte – die in den letzten Monaten ein massives Wachstum erfahren haben – stehen vor der besonderen Herausforderung, Altsysteme von unterschiedlichen Anbietern zu verwalten, die mehrere hochspezialisierte Protokolle verwenden.

Wie die jüngsten schwerwiegenden Ransomware-Angriffe gezeigt haben, ist keine Branche und kein Unternehmen völlig sicher vor Cyberangriffen. Colonial Pipeline (der Betreiber der größten Pipeline an der US Ostküste), JBS (das größte fleischverarbeitende Unternehmen in Nordamerika) und Irlands Gesundheitssystem sind nur einige Beispiele von Organisationen, die Opfer von Ransomware-Angriffen wurden.

Weltweit belaufen sich die Kosten der Cyberkriminalität auf 1 Bio. USD pro Jahr – etwa 1,2 Prozent des weltweiten BIP. Diese Cyberangriffe sind in dreifacher Hinsicht mit Kosten verbunden:

Kosten für die Zahlung von Lösegeldern, wie die 4,3 Mio. USD, die von der Colonial Pipeline Company gefordert wurden

Kosten für Geschäftsunterbrechungen, die sich für große, multinationale Unternehmen häufig auf mehrere Millionen Dollar pro Tag belaufen

Langfristige Reputationskosten

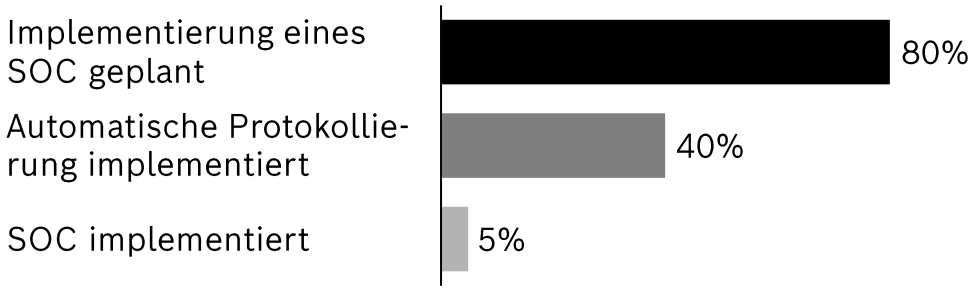
So besteht Schätzungen zufolge z.B. im Falle eines durchschnittlichen Cyberangriffs auf eine Bank bei 27 Prozent der Kunden ein hohes Risiko einer Kontoauflösung; gleichzeitig sinkt der Aktienkurs um 5 bis 7 Prozent

Vor diesem Hintergrund hat in den Unternehmen ein Wettrennen um die Entwicklung von Cyberkompetenzen und den Schutz vor Cyberrisiken eingesetzt. Banken geben schon jetzt 2.691 USD pro Beschäftigten für Cybersicherheit aus. Das Geld wird für den Aufbau von Schutzmechanismen zur Abwehr von Cyberangriffen, die Erkennung von Eindringlingen und das Management von Cyberangriffen verwendet. Zwar ist der Schutz des Unternehmens vor Cyberangriffen enorm wichtig, doch lehrt uns die Geschichte, dass hundertprozentige Sicherheit nicht möglich ist. Deshalb kommt der Erkennung und Bewältigung von Cyberangriffen eine ebenso große Bedeutung zu.

Bei der Beratung von Unternehmen im B2B- und B2C-Segment haben wir bei Bosch CyberCompare beobachtet, dass Best-Practice-Organisationen das Security Operations Center (SOC) zum Kernstück für die Erkennung und das Management von Cyberangriffen machen. Dennoch stellen wir fest, dass insbesondere im KMU-Segment weniger als 5 Prozent unserer Kunden ein SOC flächendeckend implementiert haben (Schaubild 2).

Abbildung 2

Bereitschaft unserer Kunden für die Implementierung eines SOC



Im SOC kommen alle relevanten Personen, Prozesse und Technologien zusammen. Es vereint dabei relevante Funktionsgruppen (z.B. Analysten, Sicherheitsingenieure und SOC-Manager), die benötigt werden, um die Bedrohungslage einer Systemlandschaft einschätzen zu können. Der Vorteil eines SOC liegt darin, dass sich seine Beschäftigten auf eine effektive Cyber Abwehr konzentrieren können, da sie häufig vom regulären IT-Betrieb getrennt sind.

Auch wenn alle SOCs einem sicheren Betrieb der Systeme dienen, unterscheidet sich oft der jeweilige Fokus. Der fachliche Scope eines SOC lässt sich in drei Rollen unterteilen:

Kontrolle und Überwachung
Das SOC stellt einen sicheren Zustand der Systeme sicher, indem es den ordnungsgemäßen Betriebsablauf kontrolliert.

Behandlung
Das SOC konzentriert sich darauf, Schadensereignisse zu identifizieren und zu analysieren, um ggf. darauf zu reagieren.

Operativer Betrieb
Das SOC kann auch eine sichere Administration der Systeme sicherstellen (z.B. Durch Identitäts- und Zugangsmanagement).

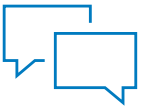
Da das SOC häufig an ein CERT (Computer Emergency Response Team) angebunden ist, insbesondere wenn es durch einen Dienstleister betrieben wird, liegt der Fokus in der Regel auf Kontrolle und Behandlung sicherheitsrelevanter Ereignisse, also der Bewältigung von Cyberangriffen. Dagegen erfolgt die Systemadministration meist intern.

Der technische Scope umfasst den Schutz von Netzwerken, Websites, Datenbanken, Endpunkten (Clients und Server) und Applikationen. Die Log-Daten aller Systeme fließen zusammen und werden idealerweise in Echtzeit auf Anomalien überprüft. Dabei werden sowohl statistische Verfahren als auch vordefinierte Use Cases (Was ist „normal“? Was deutet auf einen Angriff hin?) angewandt, um im Schadensfall eine kurze Reaktionszeit zu gewährleisten. Diese Aufgabe übernimmt in der Regel eine SIEM-Lösung (Security Information and Event Management), wie z.B. Splunk, QRadar oder LogRhythm, und bildet damit ein Kernelement des SOC.

Abbildung 3

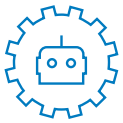
Technische Merkmale eines SOC

Security Information and Event Management (SIEM) – hier gehen die Daten ein, werden normalisiert und analysiert



Endpoint Detection and Response (EDR), um Endpoints zu überwachen

Sandboxes, um verdächtige Anwendungen sicher analysieren zu können



Security Orchestration, Automation and Response (SOAR), um automatisiert reagieren zu können

Unternehmen kennen zwar die Bedeutung eines SOC, sind aber häufig mit dessen Implementierung und Betrieb überfordert, denn es gilt, die Anforderungen und Use Cases zu ermitteln, die richtige Lösung zu finden und eine Reaktionsfähigkeit rund um die Uhr sicherzustellen. Bei diesem Prozess haben wir Unternehmen aus unterschiedlichsten Branchen unterstützt und drei zentrale Faktoren für die erfolgreiche Implementierung eines SOC ermittelt (Abbildung 4).

Abbildung 4

Entscheidung über internes bzw. externes Management des SOC

Unternehmen müssen zuerst die notwendigen Kompetenzen aufbauen, bevor sie sich für ein Insourcing des SOC-Managements entscheiden

Anforderungen ermitteln, klein anfangen und schnell iterieren

Anforderungen und Use Cases im Vorfeld genau definieren

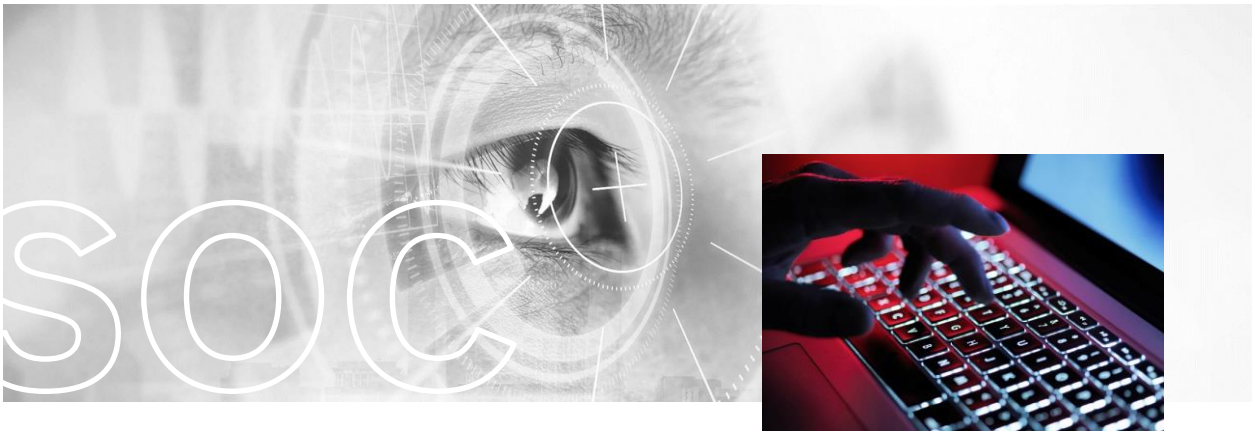
Unterstützung anfordern

Mit professioneller Unterstützung das richtige SOC auswählen, denn schließlich stehen Millionensummen und die Sicherheit des Unternehmens auf dem Spiel

1 Die richtige Entscheidung treffen:

Internes oder externes Management des SOC?

Ein SOC ist nur so gut wie das Team, das es überwacht. Da Cyberrisiken ständig zunehmen und sich deutlich beschleunigt haben, betrachten Unternehmen Cybersicherheit allmählich als strategische Kompetenz und könnten geneigt sein, sich für ein internes SOC-Management zu entscheiden. Unserer Erfahrung nach kann für den Anfang auch ein externes SOC die richtige Wahl sein, um Zeit für den Aufbau interner Fähigkeiten zu gewinnen und zu analysieren, ob das Unternehmen in der Lage ist, die notwendigen Kompetenzen für das SOC-Management zu entwickeln und rund um die Uhr auf Angriffe zu reagieren. Hierfür kann ein zusätzlicher Personalbedarf von mindestens fünf Fachleuten für Cybersicherheit entstehen. Nach Schätzungen einiger Anbieter können sich die Kosten für ein in Eigenverantwortung betriebenes SOC in den ersten drei Jahren auf 1,4 Mio. EUR belaufen.



Daher muss sich ein Unternehmen fragen, ob das interne Management eines SOC wirtschaftlich tragbar ist und ob kurzfristig die hierfür erforderlichen Kompetenzen im Bereich Cybersicherheit aufgebaut werden können. Angesichts von weltweit derzeit 3,5 Millionen offenen Stellen in diesem Bereich könnte dies zu einer enormen Herausforderung werden.

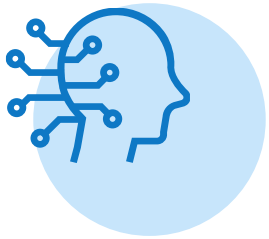
Mit Ausnahme der großen börsennotierten Unternehmen (über 10.000 Mitarbeiter) dürften die meisten Unternehmen mit einem externen SOC besser beraten sein, da Managed Security Service Provider (MSSP) von Skaleneffekten profitieren, was zu günstigeren Preisen für Kundenunternehmen führt.

Doch selbst wenn sich Unternehmen für ein extern verwaltetes SOC entscheiden, müssen sie bedenken, dass sie trotzdem interne Kapazitäten benöti-gen, um das SOC zu koordinieren und täglich mit SOC-Experten zu interagie-ren, wenn Warnungen bzw. falsch-positive Warnungen entdeckt werden.

2 Anforderungen ermitteln, klein anfangen und schnell iterieren

Ein SOC ist dann am erfolgreichsten, wenn Use Cases von Anfang an klar definiert sind und der Implementierungsprozess detailliert und iterativ ist, damit das Unternehmen Tests durchführen und Erkenntnisse gewinnen kann. Nachfolgend einige Tipps, um dies zu ermöglichen.

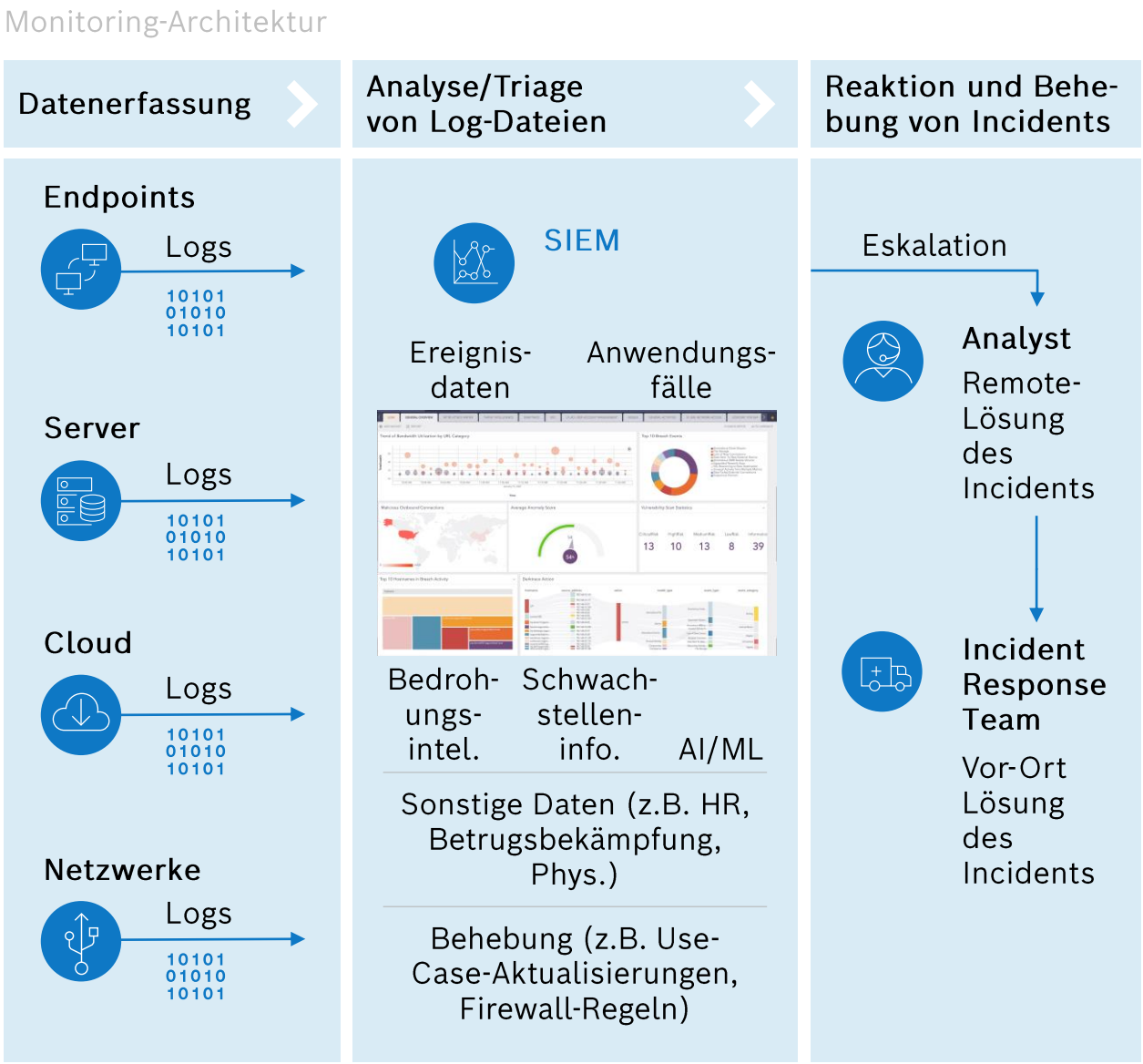
- SIEM-Meldungen (z.B. Korrelation in Netzwerkverkehr, Endpoints, Firewalls, Serverprotokollen)
- Verdächtige Active-Directory-Aktivitäten (z.B. Anmeldungen von mehreren Standorten aus, Lateral Movement)
- Meldungen von OT-Monitoring-Systemen (z.B. Korrelation, Ausfall)
- Meldungen von „Endpoint Detection and Response“-Systemen (EDR/XDR) (z.B. verdächtiges Nutzerverhalten, Malware-Erkennung)
- Angriffe auf Webserver (z.B. DDoS-Angriffe (Distributed Denial of Service), verdächtige Aktivitäten an kritischen Ports)
- Fernzugriffswarnungen (z.B. verdächtiges Verhalten von VPN-Nutzern, Brute-Force-Angriffe)
- Physischer Zugang (z.B. mehrfach fehlgeschlagene Authentifizierungen an physischen Barrieren)
- Meldungen zur Cloud-Performance (z.B. Verstoß gegen SLAs)
- E-Mail-Sicherheit (z.B. Datenverlust, schädliche Anhänge)
- Meldungen von Datenbanksystemen (z.B. verdächtige Änderungen oder Datenverluste)



Mit einem SIEM beginnen

Ein SIEM kann eine solide Grundlage für ein SOC bilden (Abbildung 5).

Abbildung 5 Typische Implementierung eines SIEM



Quelle: Bosch Expertenanalyse (vereinfachte Illustration); LogPoint Screenshot

Das SOC schrittweise im gesamten Unternehmen aufbauen

In einem Industrieunternehmen wird es z.B. drei wesentliche Bereiche geben: IT, OT und IoT. Die Implementierung funktioniert in der Regel am besten in Unternehmen, die sich zunächst nur einen Bereich vornehmen und nicht alle drei gleichzeitig angehen, also z.B. ein SOC zunächst nur im IT-Bereich implementieren. Ausgehend von den dabei gewonnenen Erkenntnissen erfolgt anschließend in zwei weiteren Wellen die Implementierung in den Bereichen OT und IoT.

3 Mit professioneller Unterstützung das richtige SOC auswählen

Eine bedarfsgerechte Lösung erhöht nicht nur die Sicherheit, sondern reduziert auch die Kosten. Ein Unternehmen im Bereich erneuerbare Energien machte selbst diese Erfahrung und konnte mit der Beauftragung eines spezialisierten Anbieters, der den Anforderungen des Unternehmens optimal gerecht wurde, ca. 1,9 Mio. EUR pro Jahr sparen.

Das Energieunternehmen hatte ein SOC in seiner IT bereits erfolgreich implementiert und war auf der Suche nach Unterstützung bei der Implementierung eines SOC für seine heterogene OT-Landschaft. Ohne den eigenen Bedarf konkret ermittelt zu haben, sichtete das Unternehmen die Angebote von Full-Service-Anbietern für SOC, die allerdings sehr kostspielig waren. In Zusammenarbeit mit dem Energieunternehmen ermittelten wir die benötigten Funktionalitäten, Servicelevel und Zielarchitekturen, so dass wir eine gezielte Suche in unserem Netzwerk mit qualifizierten Anbietern starten konnten. So fand das Unternehmen nicht nur ein SOC, das die unternehmenseigenen OT-Systeme optimal absicherte, sondern konnte außerdem allein in den ersten fünf Jahren ca. 10 Mio. USD einsparen.

Interview

Wie ein Industrieunternehmen im KMU-Segment erfolgreich ein SOC implementierte

Ein führendes Industrieunternehmen musste dringend seine Strategie und Kompetenzen im Bereich Cybersicherheit verbessern, nachdem das Unternehmen Opfer eines Ransomware-Angriffs geworden war und die Kerninfrastruktur – samt E-Mail-Systemen, Internetverbindungen, Dateidiensten und ERP-Systemen – vier Monate lang nicht funktionierte.

Nachdem das Unternehmen also schmerzlich zu spüren bekommen hatte, dass es keinen hundertprozentigen Schutz vor Cyberangriffen gibt, entwickelte es eine neue Strategie für Cybersicherheit: Hierbei fungiert das SOC als Kontrollinstanz, die Cyberangriffe in Echtzeit erkennt und das Unternehmen in die Lage versetzt, unmittelbar zu reagieren.

Und tatsächlich konnten weitere Cyberangriffe zwar nicht gänzlich verhindert, mit Hilfe des SOC aber frühzeitig erkannt werden. Nachfolgend beschreibt der CIO, wie das Unternehmen dabei vorgegangen war:

1 Warum haben Sie sich für ein SOC entschieden?

Unser SOC erfüllt inzwischen vielfältige Aufgaben und bei unserer Entscheidung dafür kamen zahlreiche Aspekte zum Tragen. Im Mittelpunkt unserer Überlegungen stand die Gewährleistung eines Betriebs rund um die Uhr. Darüber hinaus unterstützt uns das SOC bei der Schulung unserer Beschäftigten, die sich ständig neues Fachwissen aneignen und lernen, wie man mit sicherheitsrelevanten Zwischenfällen umgeht. Im Fokus des SOC steht die Sicherheit unserer Systeme, denn das Thema Sicherheit hat für uns einen höheren Stellenwert bekommen, und das SOC stellt sicher, dass unsere Systeme kontinuierlich gewartet werden. Abgesehen von den Sicherheits-aspekten versetzt uns das SOC auch in die Lage, die Funktionsfähigkeit unserer Anlagen zu überwachen.

2 Wie haben Sie die SOC-Aufgaben intern/extern aufgeteilt und was sind die Gründe dafür? Wie sind die Rollen im Falle eines Angriffs verteilt?

Der Betrieb wird gemeinsam gesteuert: Die operative Verantwortung obliegt dem SOC – wir haben immer noch Schreibrechte, müssen uns aber beim Änderungsmanagement an die Vorgaben des SOC halten.

Im Notfall greift ein Eskalationsprotokoll und die Entscheidungen werden von einem Gremium getroffen. Es handelt sich um ein globales Team, das Entscheidungen nach dem Sechs-Augen-Prinzip trifft. Konkret heißt das, dass ein Beschäftigter aus dem SOC und zwei Beschäftigte von uns zügig Entscheidungen treffen können, wobei die Führung jedoch dem SOC obliegt.

3 Welche Erkenntnisse haben Sie aus der Implementierung gewonnen, die Sie mit anderen mittelständischen Unternehmen teilen können?

Die Implementierung eines SOC ist ein umfassender Prozess. Es müssen Verfahren und Regeln entwickelt werden. Ein SOC lässt sich daher nicht in ein paar Tagen implementieren. Je besser der Übergang gelingt, desto schneller werden die Prozesse etabliert. Darüber hinaus erfordert ein Outsourcing der eigenen Sicherheit auch großes Vertrauen.

Interview

Ein Hersteller von einbaufertigen Präzisionsteilen entschied sich aus ähnlichen Gründen für ein SOC, wie sein IT-Manager berichtet:

1 Warum haben Sie sich für ein SOC entschieden?

Im Rahmen unserer IT-Strategie wollten wir unsere Position stärken. Die Rund-um-die-Uhr-Überwachung unserer Systeme in einem SOC ist dabei zentraler Bestandteil unserer Maßnahmen. Darüber hinaus will unser Management sicherstellen, dass wir bei der Bekämpfung potenzieller Cyberangriffe unser Bestes geben. Die zunehmende Zahl von Angriffen auf Lieferketten führte auch zu höheren Anforderungen seitens unserer Kunden. Für die Zusammenarbeit mit Drittunternehmen sind häufig Zertifizierungen wie ISO2700x oder TISAX erforderlich. Ein SOC hilft uns dabei, diese und andere Richtlinien einzuhalten.

2 Wie haben Sie die SOC-Aufgaben intern/extern aufgeteilt und was sind die Gründe dafür? Wie sind die Rollen im Falle eines Angriffs verteilt?

Wir haben uns aus zwei Gründen für ein externes SOC entschieden: Erstens ist es für uns schwierig, die dafür erforderlichen internen Kompetenzen aufzubauen. Und zweitens wollten wir nicht in Eigenregie zusätzliche Software und Hardware aufbauen und warten.

Die Aufgaben sind klar zwischen internen Beschäftigten und dem Personal im SOC aufgeteilt. Bei einem Zwischenfall erhalten wir von den Experten im SOC weitere Informationen und Empfehlungen für die Lösung des Problems. Besteht das Problem weiterhin, erhalten wir Unterstützung von Incident-Response-Analysten im SOC-Team.

3 Welche Erkenntnisse haben Sie aus der Implementierung gewonnen, die Sie mit anderen mittelständischen Unternehmen teilen können?

Bei der Anbieterauswahl hat es sich für uns bewährt, befreundete Unternehmen nach ihren Erfahrungen zu fragen. Wir haben festgestellt, dass sich die Angebote im Hinblick auf Preis und Leistungsumfang stark unterscheiden. Daher war es wichtig, die unterschiedlichen Angebote auszuwerten. Maßgeblich für uns ist Flexibilität. Daher empfehlen wir kurze Vertragslaufzeiten und die Nutzung gängiger Soft- und Hardware, um Lock-in-Effekte zu vermeiden.

Kontaktieren Sie uns!

Zusammen stärken wir Ihre Cybersicherheit – vom transparenten Überblick über Ihr Risiko bis hin zur Auswahl passender Anbieter.

Individuell. Pragmatisch. Unabhängig.

Kontaktieren Sie das CyberCompare Management

Dr Jannis Stemmann (CEO)

Jannis.Stemmann@
de.bosch.com
Tel.: +49 711 811-44954

Philipp Pelkmann (CTO)

Philipp.Pelkmann@
de.bosch.com
Tel.: +49 711 811-15519

Simeon Mussler (COO)

Simeon.Mussler@
de.bosch.com
Tel: +49 711 811-19893

Verbände/Industriekooperationen von **Bosch CyberCompare**

Besuchen Sie unsere Website:
www.CyberCompare.com

BOSCH