Kann IT auf alles gefasst sein?
Der Bauplan für Ihre IT von Morgen

CONSIST

Inhalt

Seite

· Herausforderungen / Ziele 3

· ISMS *– Das Managementsystem für Informationssicherheit* 4

· XDR *– Erweiterte Bedrohungserkennung und -reaktion* 8

· SIEM *– Zentralisierte Sicherheitsinformations- und Ereignisverwaltung* 12

· SOC *– Das Zentrum für Sicherheitsüberwachung und -betrieb* 15

· CSIRT *– Das Reaktionsteam für IT-Sicherheitsvorfälle* 18

· ITSM *– Management von IT-Prozessen* 21

· ITAM *– Die Verwaltung von Assets* 24

· Vulnerability Management 27

· Fazit 30

· CONSIST Software Solutions GmbH 32

Die Herausforderung

Stellen Sie sich vor, Ihre IT Security wäre ein Kartenhaus. Ein Windstoß – ein gezielter Angriff, eine versehentliche Fehlkonfiguration, eine neue Sicherheitslücke – und alles fällt in sich zusammen. Kundendaten, Geschäftsgeheimnisse, Ihr Ruf – alles liegt offen dar.

Was wäre, wenn Ihr Unternehmen stattdessen eine Festung wäre? Uneinnehmbar, widerstandsfähig, ein sicherer Hafen vor Cyberbedrohungen. Das ist keine Utopie, sondern das Ziel einer ganzheitlichen IT-Sicherheitsstrategie, die auch gesetzliche Regelungen wie KRITIS, NIS2, DORA abdecken kann. Und dieses Whitepaper ist Ihr Bauplan.

Wir zeigen Ihnen, wie Sie

... **ein starkes Fundament errichten:** ISMS stellt das Zusammenspiel Ihrer Verteidigung dar, zeigt die schützenswerten Bereiche und klärt, wo welche Sicherheitsmechanismen greifen.

... Wachtürme errichten: SIEM, XDR und Co. sind Ihre Verteidigungsanlagen, das SOC Ihre Wächter, die rund um die Uhr nach Angreifern Ausschau halten und im Ernstfall alarmieren.

... Schwachstellen ausmerzen: Vulnerability Management und Asset Management helfen Ihnen, als wachsames Auge Risse in der Mauer zu erkennen und zu reparieren und gleichzeitig eine Karte der Festung anzulegen.

... die Verteidigung organisieren: Ihr ITSM und BCM sorgen dafür, dass alle Soldaten wissen, was im Ernstfall zu tun ist und sollten doch einmal die Special Forces notwendig sein, erklären wir, wie ein IRT funktionieren kann.

Stellen Sie sich vor, Sie könnten sich entspannt zurücklehnen, weil Sie wissen, dass Ihre IT-Sicherheit nicht nur gut, sondern exzellent ist. Stellen Sie sich vor, Sie könnten sich voll und ganz auf Ihr Geschäft konzentrieren, anstatt sich ständig Sorgen um Cyberangriffe zu machen.

Sind Sie bereit, Ihre IT-Sicherheit auf ein neues Level zu heben?

ISMS

Ein **Information Security Management System (ISMS)** ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen, um deren Sicherheit zu gewährleisten. Es umfasst die Implementierung von Richtlinien, Prozessen, Verfahren und Kontrollen, um die ***Vertraulichkeit, Integrität und Verfügbarkeit*** von Informationen zu schützen. Ein ISMS basiert auf bewährten Standards, wie ISO/IEC 27001, und bietet Unternehmen einen strukturierten Rahmen, um Informationssicherheitsrisiken zu identifizieren, zu bewerten und zu steuern.

»Risiken besser einschätzen, Vertrauen von Kunden und Gesetzgebern stärken«

Funktionsweise eines ISMS

1. Risikomanagement: Das Herzstück eines ISMS ist das Risikomanagement. Es beginnt mit der Identifikation aller informationsbezogenen Risiken innerhalb eines Unternehmens. Diese Risiken werden anschließend bewertet, um ihre potenziellen Auswirkungen und Eintrittswahrscheinlichkeiten zu bestimmen. Daraus ergibt sich eine Priorisierung der Risiken, auf deren Basis geeignete Maßnahmen zur Risikominderung oder -vermeidung implementiert werden können.

2. Definition von Sicherheitsrichtlinien: Basierend auf der Risikoanalyse entwickelt das Unternehmen Sicherheitsrichtlinien, die klare Vorgaben für den Schutz von Informationen enthalten. Diese Richtlinien decken alle Aspekte der Informationssicherheit ab, einschließlich Zugangskontrolle, Datensicherung, Netzwerksicherheit und Reaktion auf Sicherheitsvorfälle.

» **Business Continuity und Disaster Recovery:** Ein ISMS unterstützt auch die Entwicklung und Umsetzung von Notfallplänen und Business Continuity Management (BCM). Durch die Identifikation kritischer Geschäftsprozesse und die Implementierung von Maßnahmen zur Minimierung von Ausfallzeiten trägt das ISMS zur Aufrechterhaltung des Geschäftsbetriebs bei.

3. Implementierung von Sicherheitsmaßnahmen: Ein ISMS bietet den strukturellen Rahmen für die Integration verschiedener Sicherheitsmaßnahmen und sorgt dafür, dass diese aufeinander abgestimmt sind. Auf Grundlage der festgelegten Richtlinien werden technische und organisatorische Maßnahmen eingeführt, um die identifizierten Risiken zu mindern.

4. Kontinuierliche Verbesserung: Ein ISMS ist kein statisches System sondern fördert eine Kultur der kontinuierlichen Verbesserung. Regelmäßige Audits und Penetrationstests sind essenziell, um Schwachstellen zu identifizieren und das ISMS kontinuierlich zu verbessern. Dies führt zu einer stetigen Optimierung des Sicherheitsprozesses und den daraus resultierenden Sicherheitsmaßnahmen und hilft dem Unternehmen, auf neue Bedrohungen flexibel und effektiv zu reagieren.

5. Dokumentation und Berichterstattung: Alle Prozesse, Richtlinien und Maßnahmen innerhalb eines ISMS müssen umfassend dokumentiert werden. Diese Dokumentation dient nicht nur als Nachweis für die Einhaltung der gesetzlichen Vorschriften, sondern unterstützt auch die Verantwortlichen dabei, fundierte Entscheidungen über notwendige Anpassungen und Verbesserungen zu treffen.

» **Compliance und Risikomanagement:** Durch die Einführung eines ISMS können Unternehmen sicherstellen, dass sie den gesetzlichen und regulatorischen Anforderungen entsprechen, was nicht nur das Vertrauen der Kunden stärkt, sondern auch finanzielle Sanktionen vermeidet. Es erleichtert nicht nur die Einhaltung von Datenschutzgesetzen wie der DSGVO, indem es einen klaren Rahmen für den Umgang mit personenbezogenen Daten bietet, sondern auch darüber hinausgehender Regulatorien wie NIS2, DORA und KRITIS.

Das ISMS im Kontext einer ganzheitlichen Security-Strategie

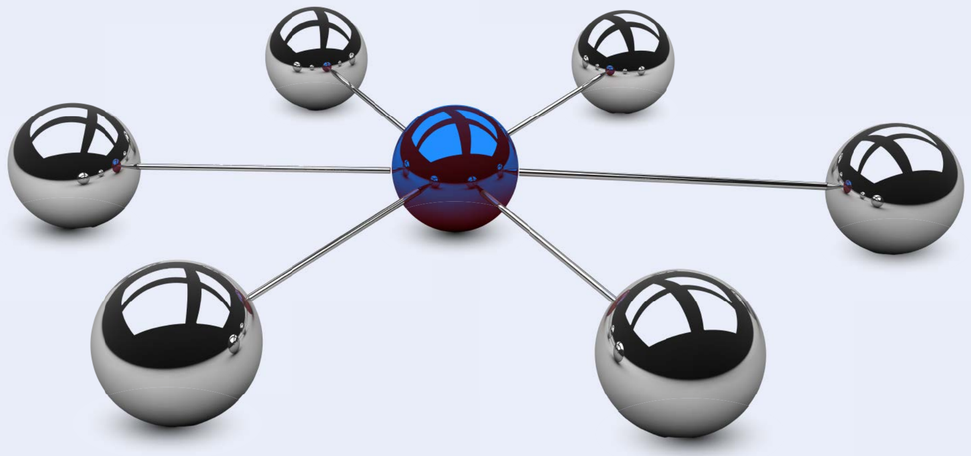
Ein **Information Security Management System (ISMS)** ist das Fundament einer ganzheitlichen IT-Sicherheitsstrategie. Es bildet den Rahmen, innerhalb dessen alle sicherheitsrelevanten Prozesse, Richtlinien und Maßnahmen strukturiert und koordiniert werden. Während Sicherheitslösungen wie SIEM oder XDR auf spezifische Bedrohungen reagieren, legt das ISMS die strategischen Leitlinien fest, nach denen diese Lösungen agieren. Es sorgt für eine konsistente und systematische Umsetzung von Sicherheitsvorgaben, unterstützt die Erfüllung regulatorischer Anforderungen und schafft Transparenz über Risiken und Schutzmaßnahmen. Durch die enge Verzahnung mit operativen Sicherheitslösungen ermöglicht das ISMS eine proaktive und widerstandsfähige Sicherheitsarchitektur, die flexibel auf neue Herausforderungen reagieren kann.

»den strategischen Überblick behalten«

XDR

Mit zunehmender Digitalisierung, mobilem Arbeiten und der Möglichkeit aus allen Ecken der Welt sensible Unternehmensdaten abzurufen, steigt die potenzielle Angriffsfläche.

Viele Technologien, die dagegen Schutz bieten sollen, werden als Einzellösungen angeboten und treiben die Kosten in die Höhe. Mit **XDR (Extended Detection and Response)** wird ein Großteil dieser Technologien in einer Lösung integriert und der Projektaufwand maßgeblich reduziert.



»Projektaufwand reduzieren, Kosten sparen«

Funktionsweise eines XDR

XDR besteht im Kern aus einer modernen EDR (Endpoint Detection and Response) Lösung, welche um weitere Features erweitert wird. 90 % aller erfolgreichen Angriffe beginnen auf dem Endpunkt. Veraltete signaturbasierte Sicherheitslösungen bilden dagegen keine ausreichende Verteidigungslinie mehr. Eine ganzheitliche Abdeckung der Endpunkte und Anreicherung der Datengrundlage durch weitere sicherheitsrelevante Datenquellen ist daher geboten. Durch XDR wird dies ermöglicht. XDR schützt nicht nur den Endpunkt, sondern auch Identitäten und Cloud-Workloads. Zudem werden alle Daten mit einer Threat Intelligence angereicht, um schneller und präziser aussagekräftige Ergebnisse zu liefern.

Sicherheitslösungen bündeln - Projektaufwand reduzieren. Im Gegensatz zu einer reinen EDR-Lösung bezieht XDR nicht nur Endgeräte wie Laptops, Desktops oder Server in die Überwachung ein, sondern integriert Daten aus verschiedenen Sicherheitslösungen, einschließlich Endpoint Protection, Netzwerk-Security und Cloud Security. XDR korreliert diese Informationen, um ein vollständiges Bild eines Angriffs zu erstellen. Ein XDR ist eine hochmoderne Verteidigungslinie, die mit einem intelligenten Netzwerk aus Sensoren, Wachtürmen und automatisierter Abwehr wertvolle Daten und Systeme vor Angreifern schützt.

Erkennung und Analyse. Moderne XDR-Systeme nutzen fortschrittliche Technologien wie künstliche Intelligenz und maschinelles Lernen, um große Mengen an Daten in Echtzeit zu analysieren. Sie sind in der Lage, nicht nur bekannte Angriffsmethoden zu erkennen, sondern auch neue, bisher unbekannte Taktiken aufzudecken. Durch diesen Einsatz von fortschrittlicher Analytik und maschinellem Lernen kann XDR auch komplexe Angriffsmuster erkennen und verhindern.

Reaktion. XDR ist nicht nur auf die Erkennung von Bedrohungen beschränkt. Es verfügt auch über die Fähigkeit zur automatisierten Reaktion. Sobald ein Angriff erkannt wird, setzt XDR Gegenmaßnahmen in Gang, um den Angriff zu stoppen und weitere Schäden zu verhindern. Diese Fähigkeit zur automatisierten Reaktion ist ein entscheidender Vorteil von XDR. Eine schnelle und effektive Reaktion auf Sicherheitsvorfälle wird dadurch möglich, insbesondere bei komplexen Angriffen, die sich über mehrere Bereiche der IT-Infrastruktur erstrecken. Moderne XDR-Lösungen ermöglichen dies mit einem einzigen Agenten. Dadurch ist kein aufwändiges Infrastruktur-Setup mit einer großen Anzahl an Servern nötig, ebenso kein monatelanges Onboarden und Konfigurieren.

Zentrale Steuerung. Darüber hinaus bietet XDR eine Kommandozentrale für die Verwaltung und Überwachung der IT-Sicherheit. Auf Basis einer einzigen zentralen Konsole haben Sicherheitsteams einen vollständigen Überblick über die gesamte Bedrohungslandschaft und können Sicherheitsvorfälle effizient untersuchen und darauf reagieren.

Integration in die Gesamt-Security und Zusammenspiel mit anderen Lösungen

Im Rahmen einer ganzheitlichen Sicherheitsarchitektur versteht sich das XDR als Plattform, die beispielsweise folgende Systeme integriert:

- **Vulnerability Management:** XDR nutzt Informationen über bekannte Schwachstellen, um Bedrohungen frühzeitig zu erkennen und gezielt Gegenmaßnahmen einzuleiten.
- **SIEM (Security Information and Event Management):** Die Kombination aus XDR und SIEM ermöglicht einen noch umfassenderen Blick, indem durch ein SIEM die Menge an Quellen erhöht wird, während das XDR die Abwehr und Detection auf dem Endpunkt integriert.
- **ITSM (IT Service Management):** XDR kann Sicherheitsvorfälle direkt in ITSM-Prozesse einspeisen, um eine schnelle und effiziente Reaktion zu gewährleisten.
- **Firewall:** Die Firewall kann dem XDR Informationen über den Netzwerkverkehr zukommen lassen und neben einer Isolation auf dem Client auch Teile des oder das gesamte Netzwerk entkoppeln.
- **Netzwerk-Management:** Informationen aus dem Netzwerk können integriert werden, um so Bewegungen im Netz schnell zu erkennen.

Welche daraus gewählt werden und welche noch hinzukommen müssten, orientiert sich an den spezifischen Unternehmensanforderungen und sollte im Rahmen von Workshops erarbeitet werden.

SIEM

Die Fähigkeit, Sicherheitsvorfälle schnell und effektiv zu erkennen und darauf zu reagieren ist von entscheidender Bedeutung. Unternehmen stehen vor der Herausforderung, riesige Mengen an sicherheitsrelevanten Daten zu verwalten, die täglich in ihren IT-Infrastrukturen generiert werden. Genau hier setzt das SIEM (Security Information and Event Management) an – als zentrales Werkzeug zur Überwachung, Erkennung und Analyse von Sicherheitsvorfällen.

Was ist ein SIEM? SIEM-Systeme sind spezialisierte Lösungen, die sicherheitsrelevante Daten aus unterschiedlichsten Quellen wie Firewalls, spezialisierten Sicherheitslösungen wie XDR oder Vulnerability Management, Servern, Anwendungen und Netzwerken zentral sammeln und analysieren. Die Hauptaufgabe eines SIEM-Systems besteht darin, diese Daten zu korrelieren und in Echtzeit auf verdächtige Muster zu überwachen. Dabei geht es nicht nur um die Erfassung von Logdaten. Durch deren intelligente Verarbeitung und Auswertung werden potenzielle Bedrohungen frühzeitig identifiziert um darauf zu reagieren. Während XDR-Lösungen gezielte Angriffe auf Endpunkte und Netzwerke erkennen und abwehren, bietet das SIEM eine übergeordnete Sicht auf alle sicherheitsrelevanten Aktivitäten im Unternehmen.

Die Kernfunktionen eines SIEM

1. Datenaggregation und -korrelation: Ein SIEM-System sammelt riesige Mengen an Daten, die in der IT-Infrastruktur generiert werden, und bringt sie in einen gemeinsamen Kontext. Durch die Korrelation dieser Daten erkennt das System komplexe Angriffsmuster, die auf den ersten Blick unzusammenhängend erscheinen könnten. Diese Fähigkeit zur Mustererkennung ist essenziell, um gezielte Angriffe und schädliche Aktivitäten aufzudecken, die traditionelle Sicherheitslösungen möglicherweise übersehen.

2. Echtzeit-Überwachung und Alarmierung: SIEM-Systeme überwachen kontinuierlich die gesammelten Datenströme auf Anomalien. Sobald eine potenzielle Bedrohung erkannt wird, wird sofort ein Alarm ausgelöst. Diese Echtzeitüberwachung ermöglicht es den IT-Sicherheitsteams, schnell zu reagieren und Maßnahmen einzuleiten, um den Schaden zu begrenzen. Dies ist besonders wichtig in einer Bedrohungslandschaft, in der jede Sekunde zählt.

3. Compliance und Reporting: Neben der Bedrohungserkennung unterstützt das SIEM auch die Einhaltung gesetzlicher Vorgaben und regulatorischer Anforderungen. Es automatisiert die Berichterstellung, liefert detaillierte Reports und KPIs zur Sicherheitslage, die für Audits und zur Einhaltung von Standards wie NIS2 oder DORA unerlässlich sind. Dies hilft Unternehmen, die regulatorischen Anforderungen zu erfüllen, ohne dass manuelle Prozesse die IT-Ressourcen belasten.

4. Forensische Analyse: Nach einem Sicherheitsvorfall bietet ein SIEM die Möglichkeit, detaillierte forensische Analysen durchzuführen. Durch die Untersuchung der gesammelten und korrelierten Daten können Unternehmen die genaue Ursache eines Vorfalls ermitteln, um daraus Schlüsse zu ziehen, wie zukünftige Angriffe verhindert werden können. Dies ist ein zentraler Aspekt für die kontinuierliche Verbesserung der Sicherheitsstrategie.

Die Rolle des SIEM im umfassenden Sicherheitskonzept

Das SIEM fungiert als das zentrale Nervensystem einer ganzheitlichen Sicherheitsstrategie und bietet dem Security Operations Center (SOC) einen entscheidenden Mehrwert, indem es nahtlos mit anderen Sicherheitslösungen wie Vulnerability Management oder XDR interagiert. Es liefert die notwendigen Daten und Erkenntnisse, die in einem SOC genutzt werden, um fundierte Entscheidungen zu treffen und effektive Gegenmaßnahmen einzuleiten.

»Mehr Schnelligkeit und Effizienz fürs SOC«

SOC

Durch die proaktive Überwachung, Erkennung und Reaktion auf Bedrohungen trägt ein **SOC (Security Operations Center)** dazu bei, dass Unternehmen ihre Daten und Systeme vor Cyberangriffen schützen können. Auch wenn die Technologien und Prozesse komplex sein mögen, ist das Ziel eines SOC einfach: die Sicherheit und Integrität der IT-Infrastruktur zu gewährleisten.

Was ist ein SOC?

Ein SOC ist im Wesentlichen eine Art „Kontrollturm“, von dem aus Experten rund um die Uhr die IT-Infrastruktur überwachen, potenzielle Bedrohungen erkennen und im Falle eines Angriffs schnell reagieren.

»Der Tower für Ihre IT-Sicherheitsexperten«

Welche Funktionen hat ein SOC?

Überwachung: Das SOC überwacht kontinuierlich die IT-Systeme und Netzwerke des Unternehmens, um verdächtige Aktivitäten zu identifizieren.

Erkennung: Mithilfe fortschrittlicher Technologien wie SIEM-Systemen und XDR-Plattformen werden potenzielle Bedrohungen erkannt und analysiert.

Reaktion: Im Falle eines Sicherheitsvorfalls reagiert das SOC schnell und entschlossen, um den Schaden zu begrenzen und die Systeme wiederherzustellen.

Prävention: Das SOC arbeitet eng mit anderen IT-Sicherheitsteams zusammen, um Schwachstellen zu identifizieren und Maßnahmen zur Verbesserung der Sicherheitslage zu ergreifen.

Welche Rollen arbeiten in einem SOC?

Ein SOC besteht in der Regel aus einem Team von Sicherheitsexperten mit unterschiedlichen Spezialisierungen. Einige der wichtigsten Rollen sind:

- **Security Analyst:** Analysiert Sicherheitswarnungen und -ereignisse, um potenzielle Bedrohungen zu identifizieren.
- **Incident Responder:** Reagiert auf Sicherheitsvorfälle und leitet Maßnahmen zur Eindämmung und Beseitigung ein.
- **Threat Hunter:** Sucht proaktiv nach Anzeichen für Angriffe, die von herkömmlichen Sicherheitsmaßnahmen möglicherweise nicht erkannt werden.
- **SOC Manager:** Leitet das SOC Team und stellt sicher, dass es effektiv arbeitet.

Wie positioniert sich ein SOC im gesamtheitlichen IT-Security-Kontext?

Ein SOC ist ein zentraler Bestandteil einer umfassenden IT-Sicherheitsstrategie. Es bindet die Funktionalitäten eines SIEM oder XDR ein und arbeitet eng mit anderen Sicherheitsfunktionen wie Vulnerability Management, Penetration Testing und Security Awareness Training zusammen, um ein mehrschichtiges Sicherheitskonzept zu schaffen.

»Entlastung Ihrer IT, Threat-Know-how nutzen«

CSIRT

Erweiterung der SOC Services um ein **Cyber Security Incident Response Team.** Neben bestehenden SOC Services, die sich auf die Überwachung und Erkennung von Bedrohungen konzentrieren, ist die Reaktion auf ernsthafte IT-Security-Vorfälle wichtig. Eine Eskalation zu einem spezialisierten IRT (Incident Response Teams) ist dann eine angemessene Reaktion. Das IRT ergreift sofortige Reaktionsmaßnahmen für tatsächliche Sicherheitsvorfälle.

»Threat-Know-how auf höchstem Niveau«

Leistungen des Incident Response Teams

Das IRT bietet eine Reihe von Dienstleistungen, die speziell darauf ausgerichtet sind, die Reaktionsfähigkeit auf Cybervorfälle zu verbessern:

- **24/7 Verfügbarkeit:** Das Team ist rund um die Uhr einsatzbereit, um auf Sicherheitsvorfälle schnell zu reagieren.
- **Schnelle Vorfallserkennung und Gegenmaßnahmen:** Durch die enge Zusammenarbeit mit dem SOC kann das IRT verdächtige Aktivitäten schnell analysieren und geeignete Gegenmaßnahmen einleiten.
- **Eindämmung und Wiederherstellung:** Nach der Eindämmung eines Vorfalls unterstützt das IRT bei der schnellen Wiederherstellung der betroffenen Systeme.
- **Forensische Untersuchung:** Zur Ermittlung der Ursachen von Sicherheitsvorfällen führt das Team forensische Analysen durch, die auch zur Verbesserung der Sicherheitsvorkehrungen genutzt werden können.
- **Nachbereitung und Dokumentation:** Nach Abschluss der Maßnahmen wird der Vorfall detailliert dokumentiert und analysiert, um daraus Lehren für zukünftige Sicherheitsstrategien zu ziehen.

Das IRT im Kontext einer ganzheitlichen IT Security

- **Reduktion von Ausfallzeiten:** Die schnelle Reaktionsfähigkeit des Incident Response Teams hilft, Betriebsunterbrechungen zu minimieren.
- **Zugriff auf Expertenwissen:** Ein erweiterter Pool an IT-Security-Spezialisten steht zur Verfügung, um auch anspruchsvolle Sicherheitsvorfälle effektiv zu bewältigen.
- **Flexible Anpassung:** Der Incident Response Service kann an die spezifischen Bedürfnisse von Unternehmen angepasst werden, unabhängig von deren Größe oder Branche.
- **Sprachlicher Vorteil:** Die Möglichkeit, den Service in deutscher Sprache zu nutzen, erleichtert die Kommunikation und Abstimmung in kritischen Situationen.

Die Kombination aus kontinuierlicher Überwachung und sofortiger Reaktion ermöglicht es Unternehmen, Sicherheitsvorfälle effizienter zu bewältigen und die Auswirkungen auf den Geschäftsbetrieb zu minimieren. Unternehmen profitieren von einem ganzheitlichen Ansatz, der sowohl Prävention als auch Reaktion auf Sicherheitsvorfälle umfasst.

ITSM

In der heutigen digitalen Landschaft ist eine zuverlässige und effiziente IT-Infrastruktur für Unternehmen jeder Größe unerlässlich. Sie bildet das Rückgrat des Geschäftsbetriebs, unterstützt kritische Prozesse und ermöglicht die Bereitstellung hochwertiger Dienstleistungen. Doch die Komplexität der IT-Umgebungen nimmt stetig zu, und die Anforderungen an die IT-Abteilungen steigen – hier kommt **ITSM (IT Service Management)** ins Spiel.

Was ist ITSM?

ITSM ist ein strategischer Ansatz zur Gestaltung, Bereitstellung, Verwaltung und Verbesserung von IT-Services, die den Geschäftsanforderungen entsprechen. Es umfasst eine Reihe von Prozessen, Tools und Best Practices, die darauf abzielen, die Qualität und damit die Sicherheit der IT zu erhöhen, die Kosten zu senken und die Kundenzufriedenheit zu stärken.

Im Bereich IT Security bedeutet das, dass die IT-Abteilung nicht nur auf Bedrohungen reagiert, sondern durch etablierte Services proaktiv Sicherheitsrisiken identifiziert und minimiert. So kann ein Vulnerability Management durch regelmäßige Pentests noch effizienter ausgestaltet werden.

Ein entscheidender Faktor ist dabei, die IT-Sicherheit effektiv, effizienter und kostengünstiger zu gestalten - indem. Das heißt, Prozesse oder Services zu schaffen, zu optimieren, Routineaufgaben zu automatisieren und ständig nach Verbesserungsmöglichkeiten zu suchen.

Die Kernprozesse des ITSM

ITSM umfasst eine Vielzahl von Prozessen, die in verschiedene Kategorien unterteilt werden können:

» **Service Desk:** Der zentrale Anlaufpunkt für alle IT-bezogenen Anfragen und Probleme.

» **Incident Management:** Schnelle Wiederherstellung des normalen Betriebs nach einem IT-Ausfall oder Sicherheitsvorfällen. Durch ein strukturiertes Vorgehen und klare Verantwortlichkeiten wird sichergestellt, dass Vorfälle effizient bearbeitet werden und die Auswirkungen auf das Unternehmen möglichst gering gehalten werden.

» **Problem Management:** Identifizierung und Behebung der Ursachen von wiederkehrenden Incidents oder auch einmaligen Sicherheitsvorfällen. Durch eine gründliche Ursachenanalyse können Schwachstellen in Systemen und Prozessen aufgedeckt und behoben werden, was die IT-Sicherheit nachhaltig stärkt.

» **Change Management:** Kontrollierte Umsetzung von Änderungen an der IT-Infrastruktur. Jede Änderung, sei es eine Softwareaktualisierung, eine Konfigurationsänderung oder die Einführung neuer Technologien, birgt potenzielle Risiken für die IT-Sicherheit. Change Management stellt sicher, dass diese Risiken bewertet und minimiert werden, bevor Änderungen umgesetzt werden, um die Stabilität und Sicherheit der IT-Umgebung zu gewährleisten.

» **Knowledge Management:** Erfassung, Speicherung und Bereitstellung von Wissen über IT-Services und -Prozesse. Informationen und Erfahrungen aus Sicherheitsvorfällen, Problemanalysen sowie Risikobewertungen werden gesammelt, dokumentiert und allen relevanten Mitarbeitenden zugänglich gemacht. Durch den Aufbau einer Wissensdatenbank können Lösungen für bekannte Probleme schneller gefunden, bewährte Verfahren (Best Practices) etabliert und das Sicherheitsbewusstsein im Unternehmen gestärkt werden.

» **Risk Management:** Identifizierung, Bewertung und Behandlung von Sicherheitsrisiken, um Verständnis der Risiken zu entwickeln und angemessene Maßnahmen zu ergreifen.

» **Security Management:** Entwicklung und Umsetzung einer umfassenden Sicherheitsstrategie auf Basis der genannten Prozesse, die sicherstellt, dass die IT-Sicherheit kontinuierlich an die sich wandelnde Bedrohungslandschaft angepasst wird.

ITSM ist ein wichtiger Bestandteil einer modernen IT-Infrastruktur. Es hilft Unternehmen, ihre IT-Services zu optimieren, die Kundenzufriedenheit zu steigern und die IT-Sicherheit zu gewährleisten. ITSM entwickelt sich ständig weiter, um den sich ändernden Anforderungen der Unternehmen gerecht zu werden. Neue Technologien wie künstliche Intelligenz (KI) und maschinelles Lernen (ML) werden zunehmend in ITSM-Lösungen integriert, um Prozesse zu automatisieren, Vorhersagen zu treffen und die Entscheidungsfindung zu verbessern.

»Transparenz wahren, Sicherheitsprozesse kontinuierlich optimieren«

ITAM

ITAM (IT Asset Management) ist ein systematischer Ansatz zur Verwaltung und Optimierung von IT-Ressourcen innerhalb eines Unternehmens. ITAM umfasst den gesamten Lebenszyklus von IT Assets, darunter Hardware, Software, Netzwerkinfrastrukturen und digitale Ressourcen. Ziel ist es, Transparenz, Kontrolle und Effizienz über diese Assets zu gewährleisten, was sowohl finanzielle als auch operationelle Vorteile mit sich bringt.

»nur was man sieht, kann man schützen«

Funktionsweise des ITAM im Rahmen einer ganzheitlichen IT-Security-Strategie

Ein effektives IT Asset Management ist ein wesentlicher Bestandteil einer ganzheitlichen IT-Security-Strategie:

» **Sichtbarkeit und Kontrolle:** Ohne eine vollständige Inventarisierung und Kontrolle über die Assets ist es schwierig, Sicherheitslücken zu identifizieren und zu schließen. Durch die genaue Kenntnis von Geräten und Softwareversionen können Schwachstellen proaktiv adressiert werden.

» **Schwachstellen-Management:** Regelmäßige Inventarisierung und Überwachung der IT Assets stellen sicher, dass alle Geräte und Software auf dem neuesten Stand sind. ITAM ermöglicht es, potenziell gefährdete Systeme zu identifizieren und rechtzeitig Patches oder Upgrades durchzuführen.

» **Compliance und Audits:** ITAM unterstützt bei der Einhaltung gesetzlicher Vorschriften und interner Richtlinien, einem zentralen Bestandteil jeder Sicherheitsstrategie. Das Management von Softwarelizenzen und die Einhaltung von End-of-Life-Zyklen gewährleistet, dass sie nicht nur rechtlich, sondern auch sicherheitskonform sind. Eine aktuelle und genaue Asset-Datenbank vereinfacht regelmäßige Audits erheblich.

» **Reaktionsfähigkeit bei Vorfällen:** Da alle Assets und deren Konfigurationen bekannt sind, kann das IT-Sicherheitsteam schnell die betroffenen Geräte identifizieren und Maßnahmen zur Schadensbegrenzung einleiten. Dies ist insbesondere bei Zero-Day-Exploits oder Ransomware-Angriffen von Bedeutung, bei denen eine schnelle Reaktion entscheidend ist.

» **Optimierung der Sicherheitsinvestitionen:** Durch ITAM können IT-Sicherheitsinvestitionen optimiert werden, weil genau bekannt ist, welche Assets besonders schützenswert sind und wo die größten Risiken bestehen. Dies ermöglicht eine gezielte Allokation von Ressourcen und Investitionen in Sicherheitsmaßnahmen dort hinein, wo sie am dringendsten benötigt werden.

Zusammenspiel mit Vulnerability Management und XDR:

» **Vulnerability Management:** Das Asset Management liefert die Grundlage für ein effektives Vulnerability Management, indem es eine genaue Übersicht über alle Assets und deren Konfigurationen bereitstellt. So können Schwachstellen gezielt identifiziert und behoben werden, bevor sie von Angreifern ausgenutzt werden.

» **XDR:** Durch die Kenntnis der Assets und ihrer Beziehungen können XDR-Systeme verdächtige Aktivitäten besser erkennen und darauf reagieren.

Ein effektives Asset Management geht weit über eine bloße Inventarliste hinaus und bietet eine vollständige und aktuelle Übersicht über sämtliche IT-Ressourcen. Damit ist es Teil des Fundaments einer erfolgreichen IT-Security-Strategie. Denn wie können Sie Ihre Festung effektiv verteidigen, wenn Sie nicht wissen, welche Schwachstellen sie hat, wo sich die wertvollsten Schätze befinden und wer Zutritt zu welchen Bereichen hat? Eine ganzheitliche IT-Sicherheitsstrategie, die ITAM integriert, ermöglicht es Unternehmen, Sicherheitsrisiken zu minimieren, Compliance zu gewährleisten und gleichzeitig die Transparenz und Kontrolle über ihre IT Assets zu maximieren.

Vulnerability Management

Angesichts der Tatsache, dass moderne IT-Systeme immer komplexer und die Bedrohungen immer raffinierter werden, ist es schlichtweg unmöglich, alle Schwachstellen manuell zu erkennen und zu schließen. Ein **Vulnerability-Scanner** bietet eine automatisierte Lösung, die kontinuierlich und systematisch nach Sicherheitslücken sucht, diese bewertet und somit eine wertvolle Grundlage für gezielte Gegenmaßnahmen liefert.

»Sicherheitslücken schließen«

Die Rolle des Vulnerability-Scanners in einer ganzheitlichen IT-Security-Strategie

» **Automatisierte Scans.** Der Einsatz eines Vulnerability-Scanners in einem Unternehmen ist aus einer Vielzahl von Gründen geradezu unerlässlich, um die Cybersicherheit auf einem angemessenen Niveau zu halten. Wie eine Art digitaler Wachhund durchforstet der Scanner ununterbrochen die IT-Infrastruktur und hält nach Schwachstellen Ausschau, noch bevor diese von potenziellen Angreifern ausgenutzt werden können. Regelmäßige, automatisierte Scans ermöglichen es Unternehmen, schnell auf neu entdeckte Sicherheitslücken zu reagieren. Dies minimiert das Risiko von Datenverlusten und Betriebsunterbrechungen und erheblichen finanziellen Schäden, die durch einen erfolgreichen Angriff entstehen können.

» **Compliance und Audits vereinfachen.** Ebenso unterstützt ein Vulnerability-Scanner Unternehmen darin, Sicherheitsrichtlinien und Compliance-Anforderungen effizienter zu erfüllen, indem er Abweichungen von definierten Sicherheitsstandards aufdeckt. Der Scanner fügt sich nahtlos in ein ISMS ein und hilft bei der Erfüllung diverser Regulatoriken. Schwachstellen, die proaktiv identifiziert und behoben werden, demonstrieren Bemühungen um eine angemessene IT-Sicherheit, was insbesondere bei Audits und Zertifizierungen von Bedeutung ist. Der Scanner liefert zudem wertvolle Daten und Berichte für die Dokumentation von Sicherheitsmaßnahmen und die Nachweisführung gegenüber Aufsichtsbehörden.

» **Gefahrenpunkte aufdecken.** Ein weiterer, nicht zu unterschätzender Vorteil besteht darin, dass der Einsatz eines solchen Scanners die Transparenz über den aktuellen Sicherheitsstatus eines Unternehmens erhöht. Die von diesen Tools generierten Schwachstellenberichte bieten eine klare Grundlage für die Priorisierung von Sicherheitsmaßnahmen und unterstützen die IT-Abteilung darin, gezielte und effektive Maßnahmen zur Behebung von Sicherheitslücken einzuleiten. Sie erhalten sozusagen eine aktuelle „Landkarte" Ihrer IT-Infrastruktur, auf der potenzielle Gefahrenpunkte markiert sind.

Integration in die Gesamt-Security und Zusammenspiel mit anderen Lösungen

Der Vulnerability-Scanner ist kein isoliertes Werkzeug, sondern ein integraler Bestandteil der gesamten Sicherheitsarchitektur. Er arbeitet Hand in Hand mit anderen Sicherheitslösungen, um einen mehrschichtigen Schutz zu gewährleisten.

- **XDR:** Die vom Scanner identifizierten Schwachstellen dienen als wertvolle Informationen für XDR-Lösungen. Diese können dann gezielt nach Anzeichen für Angriffe suchen, die diese Schwachstellen ausnutzen, und automatisierte Reaktionen einleiten, um Bedrohungen frühzeitig zu erkennen und abzuwehren.
- **SIEM:** SIEM-Systeme sammeln und analysieren die Scan-Ergebnisse zusammen mit anderen Sicherheitsdaten, um ein umfassendes Bild der Sicherheitslage zu erstellen. Anomalien und verdächtige Aktivitäten können so schneller erkannt und potenzielle Angriffe frühzeitig identifiziert werden.
- **ITSM:** Die vom Scanner gefundenen Schwachstellen werden in ITSM-Prozesse integriert, um sicherzustellen, dass diese effizient und nachvollziehbar behoben werden. Durch die Verbindung von Sicherheitsinformationen mit IT-Service-Management-Prozessen wird die Behebung von Schwachstellen zu einem strukturierten und nachverfolgbaren Prozess.
- **Asset Management:** Ein effektives Asset Management ist entscheidend für den Erfolg von Vulnerability-Scans. Nur wenn Sie wissen, welche Geräte und Systeme Sie haben, können Sie diese auch umfassend scannen und schützen. Ein Vulnerability-Scanner kann dabei helfen, unbekannte oder nicht verwaltete Assets zu identifizieren, die ein Sicherheitsrisiko darstellen könnten.

Spezifische Einsatzfelder: Vulnerability-Scanner können in verschiedenen Bereichen eingesetzt werden, um die Sicherheit Ihrer IT-Infrastruktur zu erhöhen, darunter Netzwerke, Webanwendungen, Datenbanken, Cloud-Infrastrukturen und Container.

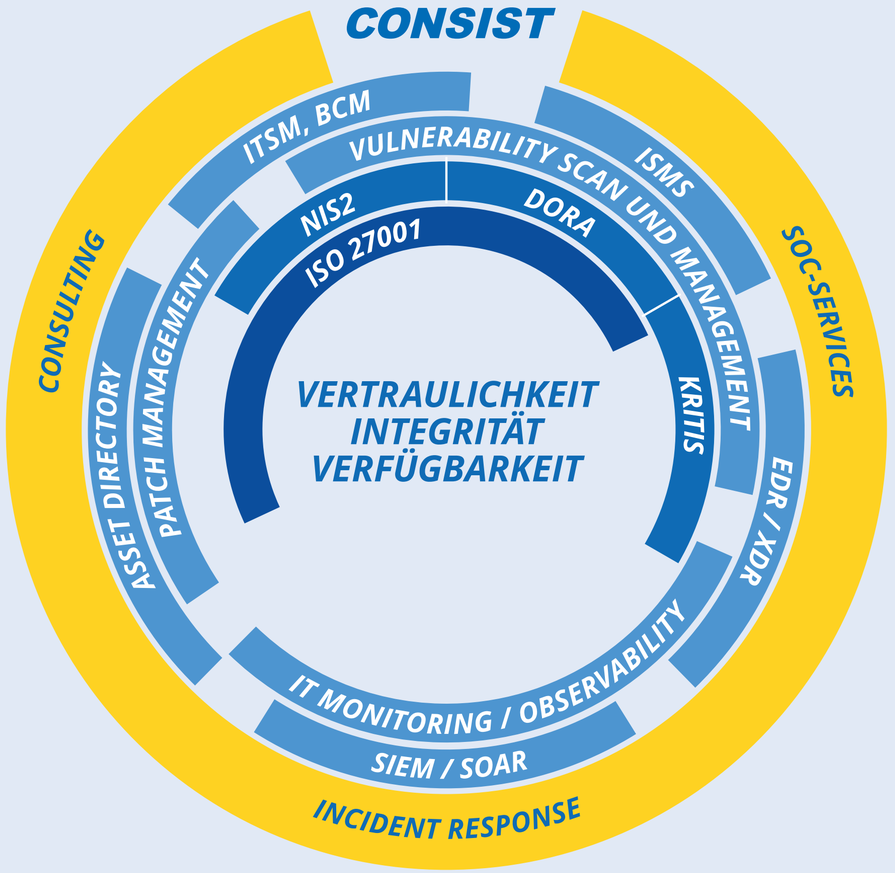
Fazit

Im Kern Ihrer IT-Sicherheits-Festung liegen die wichtigsten Werte für Ihren Unternehmenserfolg:

Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Unternehmensdaten

Eine übergeordnete Guideline für deren Schutz findet sich zum Beispiel in der ISO 27001 als Basis für Ihren Ansatz in der Informationssicherheit. Feinere Konzepte werden branchenspezifisch in **KRITIS, DORA, NIS2** eingebracht, um die Gesamt-IT-Sicherheit in Deutschland und Europa zu erhöhen. Schon hier werden ganzheitliche Security-Konzepte gefordert, die ihre Unterschiede im jeweiligen Schutzbedarf finden.

Wir sind davon überzeugt, dass es einer ganzheitlichen Security-Strategie bedarf, deren wichtigste Bauteile dieses Whitepaper beschreibt. **Consist ist Ihr Baupartner** für die notwendigen Elemente und unterstützt Sie in der erfolgreichen Verteidigung mit den Consist SOC Services.



Fazit

» *Am IT-Security-Markt gibt es viele Lösungen und viele Versprechungen. Im Grunde genommen braucht es jedoch nicht eine Masse an Speziallösungen, die mitunter nicht effizient zu integrieren und synchronisieren sind. Vielmehr ist es der* ***geeignete Mix aus automatisierter, proaktiver IT-Technik und IT-Fachkräften****, die diese nicht nur bedienen können, sondern* ***IT-Security als eine taktische und lösungsorientierte Kommunikationsbeziehung*** *zu ihrem internen oder externen Auftraggebenden begreifen.* «

CONSIST

Die **CONSIST Software Solutions GmbH** ist Spezialist für Digitale Transformation, IT Security und Managed Services. Das ganzheitliche Dienstleistungs- und Lösungsangebot des Unternehmens ermöglicht IT-Sicherheit für alle Bereiche eines Unternehmens. Mehr als 200 Mitarbeiterinnen und Mitarbeiter kümmern sich nicht nur um Konzeption und Integration der notwendigen IT-Architekturen, sondern auch um die nachfolgende Betreuung von Anwendungen und Systemen in den Managed Services. CONSIST verfügt über mehr als 35 Jahre Erfahrung am Markt und ist an den Standorten Kiel und Frankfurt präsent.

Weitere Informationen erhalten Sie auf **www.consist.de**

Der schnellste Weg?

Sprechen Sie mit unseren Fachberatern:

Joscha Sternadel
Portfoliomanagement
+49 431 3993-775
sternadel@consist.de

Christian Staab
Presales Security
+49 431 3993-596
staab@consist.de

CONSIST Software Solutions GmbH
Christianspries 4, 24159 Kiel
+49 431 3993-500
info@consist.de

www.consist.de