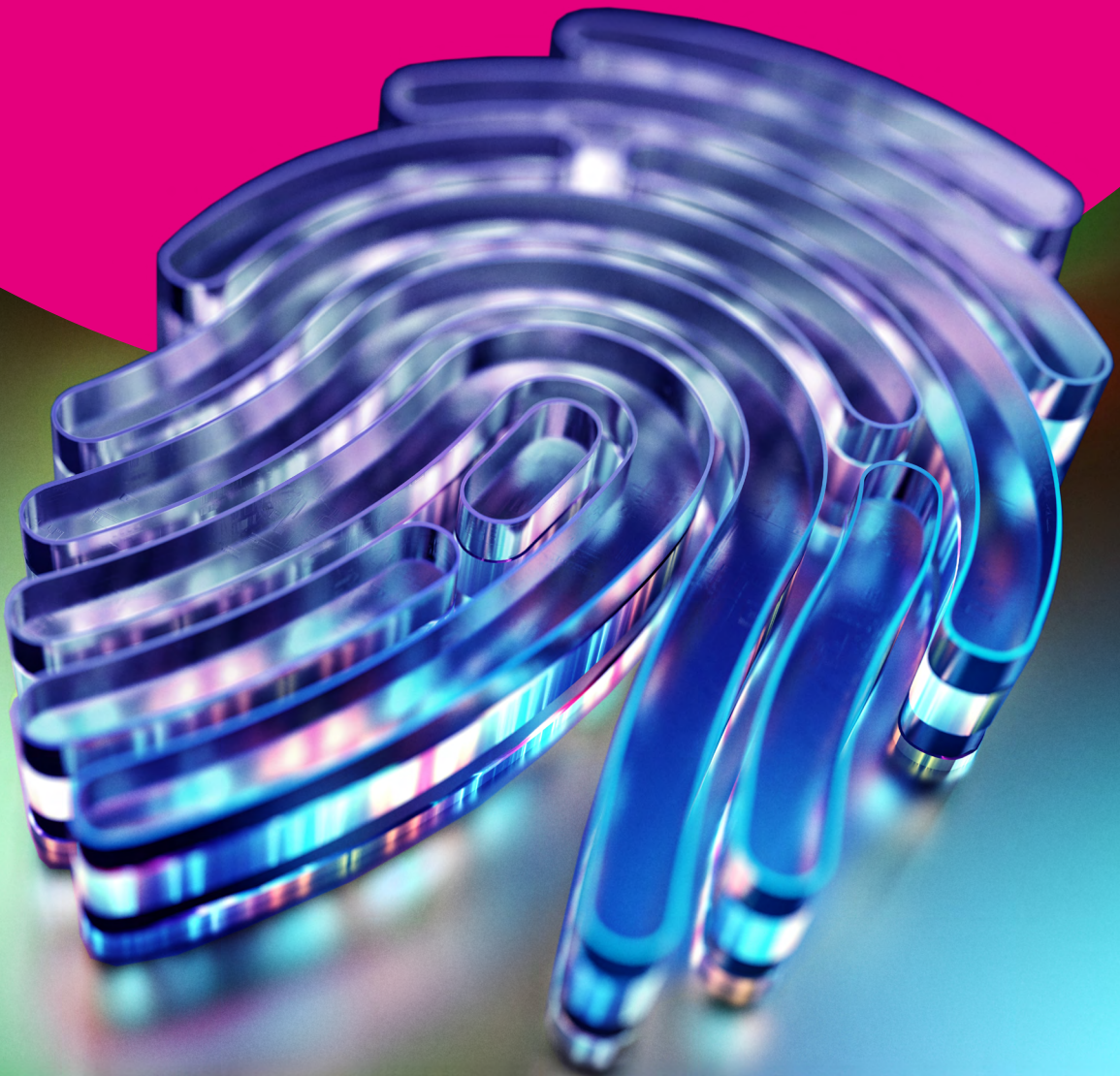




SECURITY

CYBER-RESILIENZ ALS STABILISATOR
FÜR DEN BUSINESS-ERFOLG



Innovation ermöglichen

Die digitale Transformation fördert das Unternehmenswachstum:

Aus digitalen Innovationen entstehen neue Geschäftsmodelle und Geschäftsfelder. Dieses Marktpotenzial gilt es jedoch nicht nur zu erschließen, sondern vor allem daten- und transaktionssicher zu realisieren.

Denn die Furcht vor möglichen Schwachstellen in der Cybersicherheit ist unter Führungskräften nicht umsonst eine der Hauptsorgen, wenn es um die Einführung vernetzter Angebote, wie beispielsweise IoT- oder KI-basierter Services, geht. Das führt leider oft dazu, dass diese neuen Möglichkeiten verzögert angegangen werden, um potenzielle Cyberrisiken mit Auswirkungen auf das Geschäft und den Unternehmensruf zu vermeiden. Doch so eine Vermeidungsstrategie hat fatale Folgen – denn verpasste Wachstumschancen lassen sich oft nicht mehr aufholen.

Nur mit dem passenden Cybersicherheits-Ansatz ist Innovation möglich. Dieses Cybersecurity Whitepaper thematisiert unseren Ansatz für Cybersicherheit als Stabilisator für den Business-Erfolg.



Cybersicherheit ist ein rasanter Wettlauf

„Das Tempo des Wandels war noch nie so schnell. Und dennoch wird es nie mehr so langsam sein.“

– Justin Trudeau, Präsident Kanadas,
auf dem World Economic Forum in Davos 2018

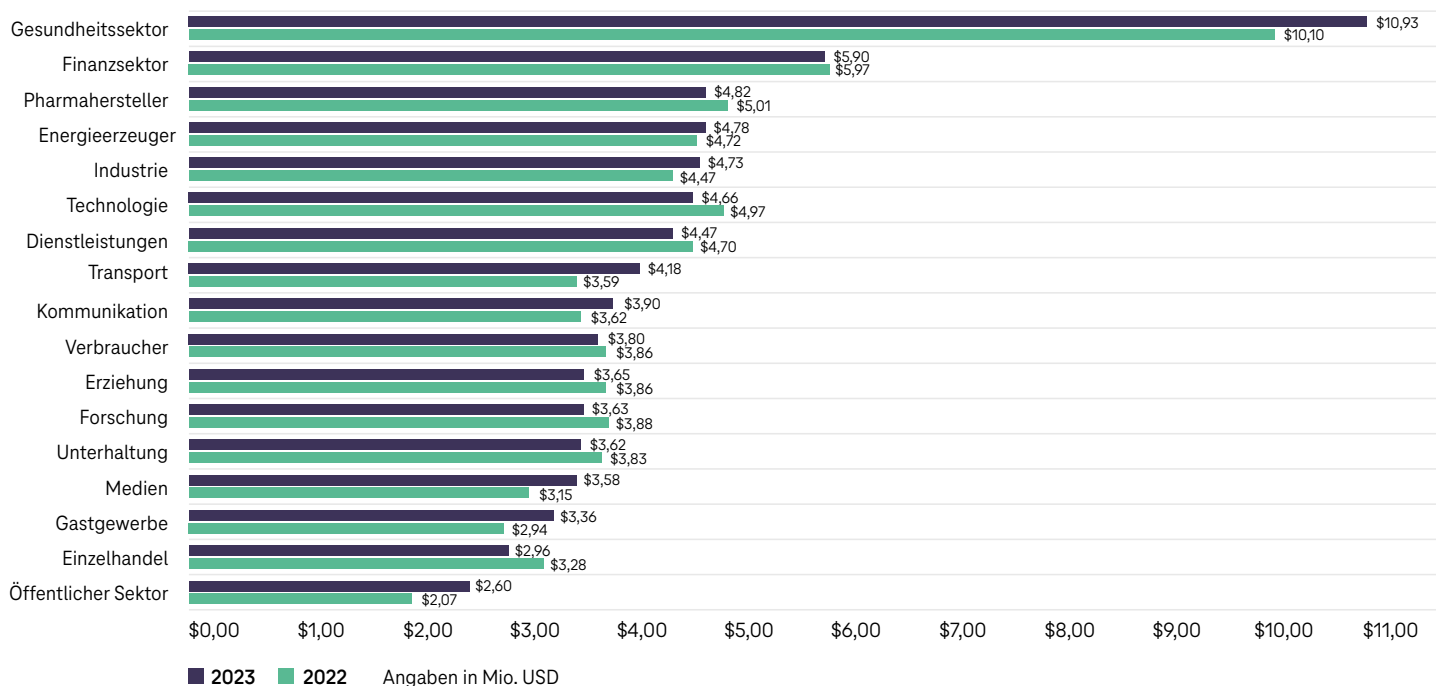
Cyberkriminalität nimmt weiter Fahrt auf

Noch nie zuvor war unsere digitale Welt so schnelllebig wie heute und die Risiken einer Cyberbedrohung so hoch. Aber die Änderungsgeschwindigkeit wird nie wieder so langsam wie heute sein, denn auch die Bedrohungen entwickeln sich mit ähnlicher Geschwindigkeit durch Ausnutzung neuester Angriffstechniken. Dieses ist kein Paradoxon, sondern zeigt die aktuelle Herausforderung. Die digitale Transformation ist unaufhaltsam und wir müssen die notwendigen Anpassungen unserer Arbeitsweise laufend vornehmen. Speziell die Cyberabwehr muss mit dieser

Geschwindigkeit Schritt halten, um Unternehmen effizient vor einem Betriebsausfall zu schützen und Cyberattacken rechtzeitig abzuwehren. Denn leider lohnt sich das Geschäftsmodell der Cyberkriminalität heute mehr denn je. Das sieht man etwa an den ermittelten Kosten, die durch Datendiebstahl entstehen. Immer noch gibt es Firmen, die keine geeigneten Cyber-Security-Maßnahmen ergriffen haben und somit entweder auf die Forderung der Erpresser eingehen und direkt oder durch den Abfluss und Weiterverkauf der Daten indirekt bezahlen. Das aus Ransomware generierte Lösegeldvolumen wird für 2023 mit rund US\$ 900 Mio. prognostiziert¹, Tendenz weiter steigend.

In der Cybersicherheit kann man sich nie auf einem Status quo ausruhen, der langfristig das nötige Sicherheitsniveau garantiert. Insbesondere das Erkennen von Cyberangriffen – die Detektion – muss ihr Tempo kontinuierlich erhöhen, um mit den sich immer weiter und schneller entwickelnden Angriffsmethoden Schritt halten zu können. Die Zahl der veröffentlichten Sicherheitslücken steigt ebenso wie das finanzielle Risiko. **Im Kontext komplexer hybrider Infrastrukturen und der zunehmenden Nutzung von Software-as-a-service (SaaS) sollte die Angriffserkennung deshalb am besten automatisiert und unverzüglich erfolgen, denn Zeit für Entscheidungen bleibt häufig keine.**

Datendiebstahl – Kosten nach Branchen



Quelle: IBM Cost of a Data Breach, Report 2023

¹ <https://therecord.media/ransomware-gangs-extorted-record-amounts>

Das Ziel: Cyberresilienz

Management verantwortlich für Compliance

Digitale Resilienz durch Prävention zu stärken, ist der Weg, den das Bundesamt für Sicherheit in der Informationstechnik aufzeigt². Auch die Novelle der EU-Netzwerk- und Informationssicherheitsrichtlinie (NIS2) setzt auf Prävention und verschärft die Anforderungsbasis für den Umgang mit Cyberrisiken. Gleichzeitig wird die Rolle der C-Level-Ebene durch die neue Richtlinie komplexer. Denn Führungskräfte sollen künftig für Verstöße gegen die erweiterten Pflichten zum Einhalten der Cybersicherheit haften³. Der Druck, die Anforderungen zu erfüllen, ist also hoch.

Dabei stellt sich die Frage: Reicht Compliance-Konformität aus, um gegen Cyberrisiken geschützt zu sein? Die Antwort ist ein klares Nein. Compliance-Erfüllung sollte nicht mit echter Security-Implementierung gleichgesetzt werden.

Die Compliance bildet nur die Basis für eine darauf aufbauende Security, die speziell vor Cyberrisiken schützt. Dieses in Einklang zu bringen und sowohl Compliance-Anforderungen als auch reale Sicherheit zu berücksichtigen, ist die Anforderung an die heutige IT-Security und damit an C-Level Exekutives wie CFO, CIO und CISO.

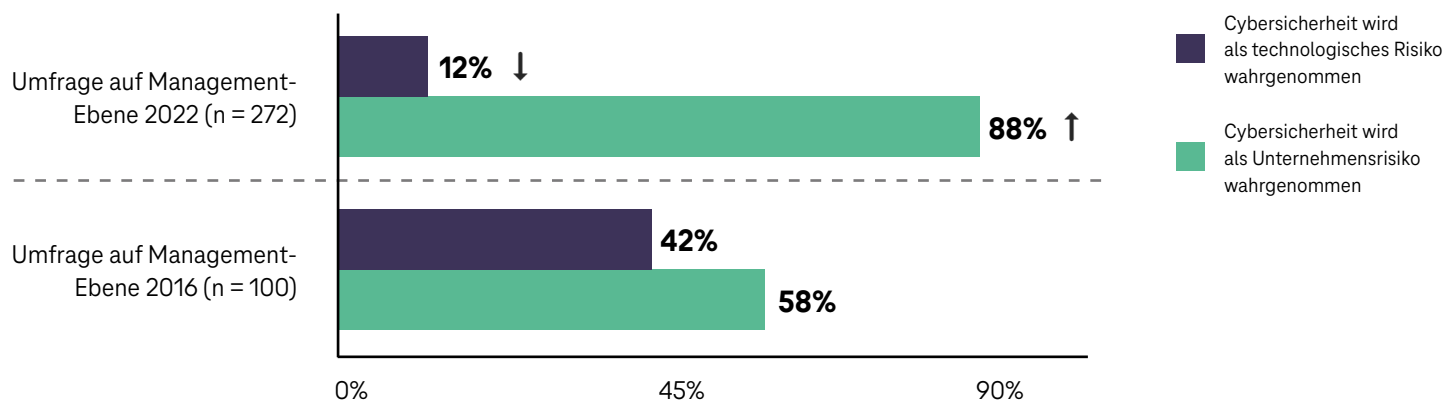
Balance-Akt für die Sicherheitsverantwortlichen in Unternehmen

Wie kann die C-Level Führungsebene diesen Anforderungen begegnen? Das Ziel muss sein, die passende Mischung aus Prävention, Detektion und Reaktion zu etablieren, um sich fortlaufend der sich ändernden Cyberbedrohungslage anzupassen. Es gibt hierzu allgemeingültige und anerkannte Frameworks zur Planung und Bewertung, diese sind aber komplex und erfüllen den gewünschten Zweck nur, wenn auch ausreichend Fachpersonal zur Implementierung und fortlaufenden Betreuung vorhanden ist.

Auch der effektive Einsatz von Künstlicher Intelligenz, wie auch intelligenter Cloud-Mechanismen zur Erkennung und Reaktion auf neueste Angriffstechniken bedingt das Knowhow von Sicherheits-Experten, um die komplexen verfügbaren Technologien zur Verteidigung am Markt bestmöglich zu kombinieren und einzusetzen. Fehlt es am erforderlichen Knowhow, entsteht ein Ungleichgewicht zu Gunsten der Angreifenden.

Wie können Unternehmen den zeitraubenden Prozess der Bewertung von Cyberbedrohungen mit allen zu beachtenden Details umsetzen? Welche finanziellen wie auch organisatorischen und personellen Mittel müssen für eine angemessene Verteidigung eingeplant werden? Vor dem Hintergrund des demografischen Wandels und des herrschenden Fachkräftemangels wird es gerade für KMUs schwierig, entsprechendes Expertenwissen selbst vollständig bereitzustellen. **Hier kann ein Managed Detektion und Response Provider (MDR-P) helfen.**

Wie bewertet die Management-Ebene Cybersicherheit⁴?



Frage: Welche Aussage entspricht dem, wie Cybersicherheit in Ihrem Unternehmen wahrgenommen wird?

Quelle: 2022 Gartner Board of Directors Survey

² <https://dgc.org/bsi-lagebericht-2022/>

³ EU-Cybersicherheit: Firmenchefs sollen für Datenpannen haften

⁴ Gemeint ist hier das Fehlen von Cybersicherheit oder die allgemeine Cybersicherheitslage

Wege in die Zukunft



Anforderungen an die Cyberabwehr

Die Einführung einer Security-Strategie ist kein „Big-bang“-Ereignis, sondern erfordert ein kontinuierliches, systematisches Vorgehen. Eine Security Roadmap zu erstellen, ist der Anfang.

Für eine angemessene Cyberabwehr müssen Unternehmensbedürfnisse definiert und auf mögliche Cyberrisiken abgestimmt werden. Neben der steigenden Bedeutung zur Einhaltung regulatorischer Compliance müssen präventive Technologien, Kontrollmechanismen, Prozesse, Erfahrungen und die eigene Risikobewertung den Weg nach vorn bestimmen.

Eine reine Lösung zur Detektion mit einer Kette von Personen, die auf Ereignisse reagieren, ist heute ein gängiger Ansatz, erfüllt jedoch alleine nicht mehr die notwendigen Anforderungen für eine solide Cyberabwehr. Die Bewertung von Sicherheitsereignissen rund um die Uhr und eine abgestimmte Ausführung von Gegenmaßnahmen durch Spezialisten ist nicht nur personalintensiv, sondern bedarf auch eines sehr hohen Reifegrades für die Detektion, Anwendung von Analyistentekniken und die situationsbedingte Reaktion.

Um diesen Reifegrad zu erreichen, benötigt man ein klares Verständnis über das Zusammenspiel von Angriffstaktik, -technik und -Verfahren (TTP – Tactics, Techniques, and Procedures) und Kenntnisse über etablierte Vorgehensmodelle, wie der Nutzung des MITRE ATT&CK® Frameworks. Der sinnvolle Einsatz geeigneter Technologien zur Detektion und automatisierter Reaktion gelingt nur durch jahrelange Erfahrung im Umgang mit Sicherheitsvorfällen.

Eine regelmäßige Auswertung der Security-Performance und der Security-Strategie belegen ihre Wirksamkeit. Eine konsequente Prüfung und Minimierung von Schwachstellen in der Infrastruktur und den Applikationen verringern viele der alltäglichen Risiken.

Synergien entstehen, wenn diese Aufgaben an einen professionellen Managed Detektion und Response Provider (MDR-P) ausgelagert werden, wo Spezialisten für Cyberabwehr mit ihrer Expertise und passenden Services zur Verfügung stehen.



Die Sicht auf die allgemeine und individuelle Cyberbedrohungslage muss mit der Entwicklungsgeschwindigkeit der Angreifenden mithalten und die Verteidigungsmechanismen einer ständigen Selbstoptimierung unterliegen.

Unser Cybersecurity Mix für Ihren Erfolg

Cyberabwehr umsetzen

Wir sind Ihr professioneller Sparringspartner für Cybersicherheit, mit dem Sie eine für Sie passende Lösung konzipieren und realisieren können.

Als Managed Detektion und Response Provider (MDR-P) bietet die Telekom branchenübergreifende Lösungen zur Prävention, Detektion und Abwehr von Cyber Angriffen und unterstützt Security- und Compliance-Verantwortliche bei der Umsetzung ihrer individuellen Sicherheitsstrategie. Ein praxiserprobtes Einführungs- und Phasenmodell hebt Ihr Sicherheitsniveau in möglichst kurzer Zeit auf ein höheres Level und berücksichtigt den individuellen Ausbau zu einem angemessenen Abdeckungsgrad. Indem die Spezialfähigkeiten verfügbarer Technologien zur Verteidigung wie ein Sicherheitsnetz aus mehreren Lagen zweckbezogen kombiniert werden, wird die Cyberresilienz in Summe viel stärker. Eine sinnvolle Gesamtlösung aus dem Portfolio der Telekom Security bildet sich aus den folgenden Elementen:

Endpoint Protection and Response (EDR)

Als vielversprechend hat sich der Schutz der Endpoint-Systeme erwiesen, um die Angriffsvektoren rund um die Schadsoftware zu kontrollieren. Noch immer zählt die Schadsoftware auf User-Endsystemen zu einer der häufigsten Ursachen einer Betriebsunterbrechung und betrifft alle Branchen und Unternehmensgrößen. Hier ist vor allem Geschwindigkeit gefragt. Die Möglichkeiten der automatisierten Reaktion auf ein identifiziertes Sicherheitsereignis durch eine EDR-Lösung sind am weitesten standardisiert und reduzieren das Risiko einer Ausbreitung von Schadcode im Unternehmensnetzwerk deutlich.

Identity Protection und Access Management

Ein Identity- und Access-Management-System steuert die effektive Verwaltung von Identitäten und Zugriffsrechten auf IT-Ressourcen und trägt dazu bei, Sicherheitsrisiken zu minimieren, Daten zu schützen, Compliance zu gewährleisten und die Kosten für die Verwaltung von IT-Infrastruktur zu optimieren.

Das Credential Leakage Monitoring klärt über gestohlene Zugangsdaten auf, wenn diese im Internet auftauchen. Das Fraudulent Domain Monitoring macht auf aktuelle Phishing-Szenarien aufmerksam, so dass Zugriffsberechtigungen gar nicht erst erbeutet werden können.

Netzwerk und Konnektivität

Bei der digitalen Transformation werden immer mehr Geschäftsprozesse auf hybride Plattformen verlagert und über IT/OT-Netzwerke miteinander verbunden. Immer neue Technologien müssen flexibel in skalierbaren Netzen miteinander kommunizieren und Performance sowie Sicherheit bei gleichzeitiger Agilität garantieren. Die Stabilität des Netzwerks bildet das Rückgrat für die gesamten digitalen Geschäftsprozesse. Lösungen aus dem Bereich DDoS, WebApplicationFirewalls, IDS/IPS und Cloud-Security unterstützen dabei.

Im Netzwerk kann man weitreichende Analysen über die Kommunikationsbeziehung von bekannten wie auch „fremden“ Endsystemen betreiben, deren Schutzcharakter man nicht genau definieren kann. Deshalb ist die Detektion von ungewöhnlichen Veränderungen im Netzwerk erforderlich, um die „schwarzen Schafe“ auch ohne Endpoint-Wissen identifizieren und verfolgen zu können.

Mit einer systemübergreifenden Ereigniskorrelation können auch komplexe Angriffsmuster sichtbar gemacht werden. Die Telekom hat basierend auf dem TTP-Framework der MITRE ATT&CK eine eigene Detection-Scenario-Library für die SIEM-Technologie entwickelt und bietet eine gezielte Strategie zur Detektion und Abwehr von Angriffsvektoren in Unternehmensnetzwerken.



Hybride IT-Infrastrukturen und Applikationen

Die nächste Stufe berücksichtigt die Sicht auf Schwachstellen in den eigenen IT-Systemen. Die Systeme müssen regelmäßig auf Schwachstellen überprüft werden, um potenzielle Einfallstore zu verhindern. Nicht immer ist das unverzügliche Schließen von Schwachstellen möglich. Es bleibt ggf. jedoch die Möglichkeit der konkreten Beobachtung von sicherheitsrelevanten Ereignissen der betroffenen Systeme, um Abweichungen vom Normalzustand zu detektieren.

Auf dieser Stufe bewegen wir uns in Richtung Logprotokollierung und Auswertung über ein systemübergreifendes Eventmanagement. Kurz: eine auf die Anwendung und die unterliegenden Systeme ausgerichtete Detektion mit SIEM-basierter Technologie.

Threat Intelligence

Wer beurteilen möchte, ob es sich um einen ernstesten Security-Vorfall oder um eine False-Positive-Meldung, also einen Fehllarm, handelt, muss die Event-Daten aus den IT-Systemen und Sensoren des Unternehmens mit externen Kontextinformationen anreichern. Heißt: Unternehmen brauchen einen Threat Intelligence Service. Er hilft ihnen, Gefahren schnell zu erkennen und die eigene IT zu schützen, indem er so genannte Indicators of Compromise (IoC) bündelt, diese mit einer Vielzahl weiterer aktueller Informationen zur Bedrohungslage in eine strukturierte Form bringt und sie automatisiert auswertet.

Unter diesen Kompromittierungsindikatoren versteht man all jene Merkmale und Daten, die auf die Kompromittierung eines Computersystems oder Netzwerks hinweisen. Solche Threat Intelligence Services umfassen mehrere Module. Der Vulnerability Advisory Service etwa informiert über neu erkannte Schwachstellen in Hard- und Software und gibt konkrete Empfehlungen, wie man diese detektieren und auch teils direkt beheben kann.

Zum Threat-Intelligence-Ökosystem von Providern wie der Telekom gehören Security-Dienstleister, Forschungsstätten und Behörden, die ihre Erkenntnisse untereinander teilen, um gemeinsam die Schlagkraft zu erhöhen.

Die Sicherheitsexperten der Security Operations Center (SOC) sind jedoch auch in Internetforen und sozialen Medien unterwegs, wo sich Hacker über neue Schwachstellen und Angriffsmethoden austauschen.



Wir managen Ihre Security!

Das Zusammenspiel der passenden Produkte auf End-point-, Netzwerk-/Cloud- und Applikations-Ebene ergibt die Basis für eine schlagkräftige (MDR-)Gesamtlösung.



Deutsche Telekom Security modelliert dieses Zusammenspiel für Sie und bildet den passenden Betrieb als komplett standardisierte Lösung ab.

Frank Westheider

*Chapter Head of Cyber Defense Engineering –
Deutsche Telekom Security GmbH*

Vor seiner Tätigkeit bei der Deutsche Telekom Security GmbH war Frank Westheider bei der Arvato Systems GmbH als Head of Security for Operations für die Cybersicherheit der Service Provider Datacenter verantwortlich.

Weitere Security-Erfahrungen hat er im Rahmen von Security-Incident-Lead-Rollen und im Kontext von PCI-DSS und analogen Compliance- und Informationssicherheits-Themen gesammelt. Auch bei angrenzenden Themen wie BCM und High-Availability Infrastrukturen begleitete er Konzeption und Betrieb.

Sein Herz schlägt für die Technik und komplexe Infrastrukturen. Außerhalb der Arbeit ist er gerne mit dem Motorrad im Mittelgebirge und in den Alpen auf Tour.

frank.westheider@telekom.de

Gunnar Mews

*Security Architekt für Cyber Defense Services –
Deutsche Telekom Security GmbH*

Seit 2005 ist Gunnar Mews als Sales Consultant und Projektleiter für Security Services bei der T-Systems im IT-Security-Umfeld aktiv und ist dabei auch in die Entwicklung von Managed Security Services eingestiegen. Er ist Mitbegründer des ersten Managed Cyber Defense (MCD) Services auf SIEM-Basis von 2007, der noch heute – in moderner Form – Teil des Telekom Security Portfolios ist.

Mit über 17 Jahren Service-Erfahrung trainiert er die Security Sales, Security Consulting sowie das Service Management und ist für die Weiterentwicklung dieser Services verantwortlich. In seiner Freizeit ist er als DIY Heimwerker für die Familie im Einsatz und bereist gern die Welt.

gunnar.mews@telekom.de

Kontakt

E-Mail: security@telekom.de

Web: security.telekom.de

Herausgeber

Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn