



THE QUANTUM BUSINESS MAGAZINE – BENJAMIN RICHTER EDITION

QUANTUM

**CYBER
SECURITY**



**BENJAMIN
RICHTER**

PERSÖNLICHE UND
BERUFLICHE INSIGHTS VOM
CYBER SECURITY EXPERTEN

**MACHEN SIE
AUS NIS2 EINEN
WETTBEWERBS
VORTEIL**



**ENTHUSIASMUS.
FREUNDE.
FAHREN.**

Der Astonishing Drivers Club e.V. ist die Gemeinschaft für alle Aston Martin Enthusiasten von München bis Hamburg. Von Tagestouren, Roadtrips oder unserem Markentreffen: Hier werden nicht nur Tourenfreunde glücklich.

Egal ob Cygnet oder DB 12 - Werde Teil unserer Gemeinschaft und erlebe unvergessliche Momente mit Gleichgesinnten. Es erwarten Dich regionale Stammtische, aktiver Austausch zwischen den Mitgliedern, regelmäßige regionale Ausfahrten und internationale Roadtrips, Clubvorteile bei unseren Partnern und Sponsoren, jährliches Markentreffen uvm.

Astonishing Drivers findest Du in den Sektionen: München, Stuttgart, Rhein / Main, Düsseldorf / NRW & Norddeutschland. Mehr unter astonishingdrivers.com



EDITORS NOTE



Turning a Page

Liebe Leserinnen und Leser, es gibt Momente im Leben, die einen Wendepunkt markieren. Momente, in denen wir eine neue Seite aufschlagen und uns auf eine Reise begeben, die uns zu neuen Horizon-

ten führt. Die Veröffentlichung der Benjamin Richter Quantum Edition ist genau ein solcher Moment für mich.

In den letzten Jahrzehnten hatte ich das Privileg, die Welt der Informationssicherheit aus verschiedenen Perspektiven zu erleben. Diese Erfahrungen haben mir nicht nur wertvolle Einblicke in die Herausforderungen und Chancen der digitalen Transformation gegeben, sondern auch eine tiefe Leidenschaft entfacht, mein Wissen und meine Visionen mit anderen zu teilen.

Meine persönliche Quantum Edition ist mehr als nur ein Magazin. Sie ist eine Einladung, gemeinsam mit mir die komplexen und faszinierenden Facetten der Cyber Security zu entdecken. In einer Zeit, in der technologische Entwicklungen rasant voranschreiten, ist es mein Ziel, euch nicht nur Informationen zu liefern, sondern auch Inspiration und Orientierung zu bieten.

Jeder Artikel in dieser Ausgabe spiegelt meine Überzeugung wider, dass Informationssicherheit nicht nur eine technische Disziplin ist, sondern auch eine kulturelle und strategische Herausforderung. Ich möchte euch zeigen, wie wir durch innovative Ansätze und eine ganzheitliche Perspektive nicht nur sicherer, sondern auch erfolgreicher werden können.

Ich lade dich ein, mit mir diese neue Seite aufzuschlagen und sich auf eine spannende Entdeckungsreise zu begeben. Lass uns gemeinsam die Zukunft gestalten und die Möglichkeiten erkunden, die vor uns liegen.

Herzlichst,
euer Benjamin Richter



MY WAY

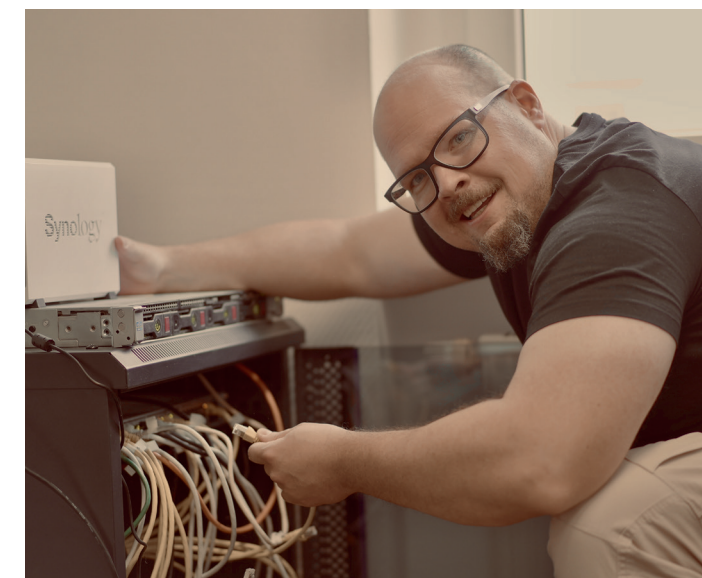
So bin ich als Mensch und Cyber Security Experte

Ich bin jemand, der stets neugierig und wissbegierig ist. Diese Eigenschaften treiben mich an, immer tiefer zu forschen und neue Lösungen zu finden. Als Mensch lege ich großen Wert auf Integrität und Authentizität, was sich direkt in meiner Arbeit als Cyber Predictor widerspiegelt. Ich strebe danach, in jeder Situation ehrlich und transparent zu sein, was mir hilft, vertrauensvolle Beziehungen zu meinen Kunden aufzubauen.

Als Cyber Predictor sehe ich meine Rolle nicht nur als Beruf, sondern als Berufung. Ich habe es mir zur Aufgabe gemacht, Unternehmen nicht nur gegen die Bedrohungen von heute zu wappnen, sondern sie auch auf die Herausforderungen von morgen vorzubereiten.

Meine Philosophie basiert auf der Überzeugung, dass Informationssicherheit mehr ist als nur technische Maßnahmen.

Es geht darum, eine Kultur des Vertrauens und der Wachsamkeit zu schaffen, in der jeder Einzelne eine aktive Rolle spielt. Ich vereine technologische Expertise mit strategischem Denken, denn ich verstehe,



dass die digitale Landschaft sich ständig verändert und dass Unternehmen flexibel und anpassungsfähig sein müssen, um erfolgreich zu sein.

Ich glaube fest daran, dass Wissen geteilt werden sollte. Diese Überzeugung spiegelt sich in meinem Engagement wider, meine Erfahrungen und Erkenntnisse mit anderen zu teilen. Ich möchte Führungskräfte und Teams inspirieren, über den Tellerrand hinauszublicken und Informationssicherheit als integralen Bestandteil ihrer Geschäftsstrategie zu betrachten.

In meiner Rolle als Cyber Predictor bin ich mehr als nur ein Berater – ich sehe mich als Wegbereiter für eine sichere und erfolgreiche digitale Zukunft. Meine Leidenschaft und mein unermüdlicher Einsatz machen mich zu einem unverzichtbaren Partner für Unternehmen, die in der digitalen Welt nicht nur bestehen, sondern florieren wollen.



WAS DU FÜR DEIN UNTERNEHMEN AUS DER BENJAMIN RICHTER - QUANTUM EDITION MITNEHMEN WIRST

In meiner Quantum Edition lade ich dich ein, mit deinem Unternehmen in eine Welt voller Erkenntnisse und praktischer Strategien einzutauchen, die speziell darauf ausgerichtet sind, euch in der digitalen Landschaft sicher und erfolgreich zu navigieren. Hier sind einige der wertvollen Einsichten und Vorteile, die ihr aus diesem Magazin ziehen könnt:

Tiefgehendes Verständnis für Cyber Security: Ich teile mit euch fundiertes Wissen und innovative Ansätze im Bereich der Informationssicherheit. Meine langjährige Erfahrung ermöglicht es mir, euch Einblicke zu bieten, die über das Offensichtliche hinausgehen.

Aktuelle Themen im Fokus: Mit meinem Team beleuchte ich hochaktuelle Themen wie die neue EU-Verordnung NIS2, aber auch Bestandsthemen wie z.B. Information Security Management Systeme (ISMS) nach ISO27001:2022. Ihr werdet umfassend informiert und auf dem neuesten Stand gehalten, um die Anforderungen und Chancen dieser Entwicklungen zu verstehen und zu nutzen.

Praktische Strategien und Werkzeuge: Mein Magazin ist vollgepackt mit umsetzbaren Tipps und Strategien, die ihr direkt in eurem Unternehmen anwenden könnt. Egal, ob es um die Verbesserung eurer Sicherheitsmaßnahmen oder um die Optimierung eurer Geschäftsprozesse geht, ich gebe euch konkrete Werkzeuge an die Hand.

Inspiration und Weitblick: Ich vermittele nicht nur technisches Wissen, sondern inspiriere euch auch dazu, über den Tellerrand hinauszuschauen. Ihr werdet ermutigt, neue Perspektiven einzunehmen und die Informationssicherheit als integralen Bestandteil eurer Geschäftsstrategie zu betrachten.

Vertrauen und Sicherheit: Durch das Verständnis der komplexen Herausforderungen der digitalen Welt werdet ihr in der Lage sein, fundierte Entscheidungen zu treffen und euer Unternehmen sicherer zu machen. Dieses Wissen wird euch helfen, Vertrauen bei euren Kunden und Partnern aufzubauen.

Zukunftsorientierte Lösungen: Meine Quantum Edition bereitet euch nicht nur auf die aktuellen Herausforderungen vor, sondern gibt euch auch die Werkzeuge an die Hand, um zukünftige Risiken zu antizipieren und zu meistern.

Mit meiner Benjamin Richter Quantum Edition seid ihr bestens gerüstet, um die digitale Transformation eures Unternehmens erfolgreich zu gestalten und eure Wettbewerbsfähigkeit zu steigern. Lasst euch von mir auf dieser spannenden Reise begleiten und entdeckt die Möglichkeiten, die vor euch liegen.



INHALT



IMPRESSUM

Herausgeber:
cyber complete GmbH
Benjamin Richter
Weststraße 4
57392 Schmallenberg
Telefon: +49 2972 9775700
E-Mail: b.richter@cybercomplete.de
Web: <https://cybercomplete.de/>

Verantwortlicher für den Inhalt:
Benjamin Richter

Verlag, Graphik, Layout, Realisierung:
GRP Manhattans Media Limited
+49 171 955 80 83
norbert.wittmann@quantum-magazin.com
<https://quantum-magazin.com>

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts übernehmen Verlag und Redaktion keine Gewähr. Für unverlangt eingesandte Manuskripte und unverlangt zugestellte Fotografien oder Grafiken wird keine Haftung übernommen.

4	EDITORIAL	20	NIS2 - BERATUNG & READINESS	48	DARKNET MONITORING MIT DEEPWEBCHECK
5	MY STORY	24	ISO 27001 - MANAGEMENT-SYSTEME	52	ISO 42001 & EU AI ACT - ÜBERBLICK UND BEDEUTUNG
6	WAS NIMMT DER LESER MIT?	30	CISO AS A SERVICE	56	DSGVO VERSTEHEN
7	INHALT	34	MANAGED SECURITY SERVICE PROVIDER	58	DSGVO IN DER PRAXIS
8	ARCHITEKT DER CYBBER SECURITY	38	AKTUELLE TECHNOLOGIEN ZUR CYBER-ABWEHR	62	INTEGRATION DSGVO, NIS2 & ISO 27001
12	INFORMATIONSSICHERHEIT ALS GANZHEITLICHER ANSATZ	42	PENETRATION-TEST NACH BSI-STANDARD	68	SCSMS - CYBER SECURITY MANAGEMENT SYSTEM
16	NIS2 - ÜBERBLICK & BEDEUTUNG			74	TISAX - INFORMATION SECURITY MANAGEMENT SYSTEM / AUTOMOTIVE
				76	IT-PROJEKTMANAGEMENT IN SECURITY
				82	OT IM VISIER - SICHERUNG VON PRODUKTIONSANLAGEN
				86	FIREWALLS, SWITCHES & PATCHMANAGEMENT
				90	KRISE, NOTFALL ODER GLEICH BCM? PRÄVENTIONSMASSNAHMEN
				95	SCHULUNG & SENSIBILISIERUNG
				97	AUSBLICK & ZUKUNFTSTHEMEN

Der Architekt für Cyber Security

Vom IT-Projektleiter zum Vordenker der digitalen Sicherheit. Ein Leben im Dienst der Informationssicherheit



The Cyber Security Architect

Entdecke die Welt der Cybersicherheit mit Benjamin Richter, einem der führenden Köpfe der Branche. In seiner persönlichen Quantum Edition teilt er seine 21-jährige IT- und 16-jährige Security-Erfahrung, enthüllt seine strategischen Ansätze und erklärt, wie Künstliche Intelligenz die Zukunft der digitalen Verteidigung prägen wird. Tauche ein in die faszinierende Reise eines Vordenkers, der die digitale Welt sicherer macht.

Ich bin Benjamin Richter, ein erfahrener IT-Sicherheitsexperte mit über 21 Jahren Erfahrung in der IT und 16 Jahren in der Sicherheitsbranche. Mein beruflicher Weg begann in der Netzwerktechnik und führte mich über verschiedene Stationen bis zur Geschäftsführung der Cyber Complete GmbH. Hier bin ich als Berater, Auditor und Trainer tätig, um Unternehmen bei der Bewältigung der komplexen Herausforderungen der digitalen Sicherheit zu unterstützen.

LEBENSWEG UND KARRIERE

Karriere in der IT: In der Netzwerktechnik sammelte ich wertvolle Erfahrungen, die mir halfen, als IT-Projektleiter für die T-Systems tätig zu werden. Dort leitete ich verschiedene Plattformen und Applikationen, was mir ein tiefes technisches Verständnis und Projektmanagementfähigkeiten vermittelte.

Akademische Grundlagen: Mein wissenschaftlicher Werdegang führte mich über einen MBA, der mir ein tiefes Verständnis für betriebswirtschaftliche Prozesse und strategisches Denken vermittelte. Diese Fähigkeiten waren entscheidend, um die komplexen Anforderungen der IT-Sicherheit in Unternehmensstrategien zu integrieren.

Aufstieg zum CISO: Mit einem ausgeprägten Gespür für Sicherheitsfragen übernahm ich die Rolle des Chief Information Security Officers (CISO). In dieser Position entwickelte und implementierte ich umfassende Sicherheitsstrategien, die den sich ständig ändernden Bedrohungslandschaften gerecht wurden.

Auditor und Trainer: Seit 2018 bin ich nun als geschäftsführender Gesellschafter der Cyber Complete GmbH tätig. Mein Fokus liegt auf der Beratung, dem Audit und der Schulung von Großunternehmen und Konzernen in den Bereichen ISO 27001, NIS2 und DSGVO. Besonders spezialisiert bin ich auf die Automotive-Branche mit ISO 21434 und TISAX, wo ich Unternehmen helfe, die strengen Sicherheitsanforderungen zu erfüllen.

BEDEUTUNG MEINER ERFAHRUNG

Meine 21-jährige IT- und 16-jährige Security-Erfahrung sind dabei von unschätzbarem Wert. Diese Expertise ermöglicht es mir, Unternehmen nicht nur bei der Einhaltung von Sicherheitsstandards zu unterstützen, sondern auch ganzheitliche Sicherheitsstrategien zu entwickeln, die auf die spezifischen Bedürfnisse der Unternehmen zugeschnitten sind. Ich habe ein tiefes Verständnis für die digitale Bedrohungslandschaft entwickelt und setze mich unermüdlich für die Sicherheit meiner Kunden ein.

ZUKÜNFTIGE ROLLE UND KÜNSTLICHE INTELLIGENZ

Die Zukunft der Cybersicherheit sehe ich in der engen Zusammenarbeit mit Künstlicher Intelligenz. KI-Tools bieten die Möglichkeit, Cyberbedrohungen in Echtzeit zu erkennen und abzuwehren, indem sie große Datenmengen analysieren und Muster identifizieren, die auf potenzielle Angriffe hinweisen. In meiner Rolle bei Cyber Complete plane ich, innovative KI-Lösungen zu integrieren, um die Sicherheitsarchitektur von Unternehmen weiter zu stärken.

Ich beschäftige mich intensiv mit den ethischen Fragen der Informationsethik, insbesondere wie weit eine Gesellschaft im Bereich Künstlicher

Intelligenz gehen darf und sollte. Es ist entscheidend, dass wir verantwortungsbewusste KI-Strategien entwickeln, die nicht nur die Sicherheit erhöhen, sondern auch die Privatsphäre und Rechte der Individuen respektieren.

Ein weiterer Aspekt meiner Arbeit ist die Entwicklung von KI-gesteuerten Sicherheitslösungen, die proaktiv Bedrohungen identifizieren und abwehren können. Diese Technologien haben das Potenzial, die Art und Weise, wie wir Cybersicherheit verstehen und umsetzen, grundlegend zu verändern. Sie ermöglichen es uns, von reaktiven zu proaktiven Sicherheitsstrategien überzugehen, die Bedrohungen antizipieren und verhindern, bevor sie Schaden anrichten können.

Mit meiner umfassenden Erfahrung und meinem visionären Ansatz bleibe ich ein unverzichtbarer Partner für Unternehmen, die in der digitalen Welt nicht nur bestehen, sondern weiter wachsen möchten.

IN DER DIGITALEN WELT GIBT ES KEINE PAUSEN. WIR MÜSSEN IMMER EINEN SCHRITT VORAUS SEIN.

INFORMATIONSSICHERHEIT ALS GANZHEITLICHER ANSATZ

**EIN WEGWEISER ZUR UMFASSENDE
DIGITALEN SICHERHEIT**



BE SAVE!

GANZHEITLICHE INFORMATIONSSICHERHEIT: DER SCHLÜSSEL ZUR DIGITALEN RESILIENZ

In einer zunehmend digitalisierten Welt ist Informationssicherheit nicht mehr nur eine technische Herausforderung, sondern ein strategischer Imperativ für Unternehmen jeder Größe. Als erfahrener IT-Sicherheitsexperte mit über zwei Jahrzehnten Erfahrung in der Branche, sehe ich Informationssicherheit als einen ganzheitlichen Ansatz, der weit über die Implementierung von Technologien hinausgeht. Es geht darum, ein Sicherheitsbewusstsein zu schaffen, das alle Ebenen eines Unternehmens durchdringt.

1. DIE SÄULEN DER INFORMATIONSSICHERHEIT

Ein ganzheitlicher Ansatz zur Informationssicherheit basiert auf drei zentralen Säulen: Technologie, Prozesse und Menschen. Diese Elemente müssen in einem harmonischen Zusammenspiel agieren, um effektive Sicherheitsstrategien zu entwickeln:

Technologie: Die Implementierung fortschrittlicher Sicherheitstechnologien ist unerlässlich, um Bedrohungen zu erkennen und abzuwehren. Dazu gehören Fire-

walls, Verschlüsselung, Intrusion Detection Systeme und zunehmend auch Künstliche Intelligenz, die in der Lage ist, Anomalien in Echtzeit zu identifizieren.

Prozesse: Effektive Sicherheitsprozesse stellen sicher, dass Technologien korrekt eingesetzt und kontinuierlich überwacht werden. Dies umfasst die Entwicklung von Richtlinien und Verfahren, die regelmäßige Überprüfung und Anpassung von Sicherheitsmaßnahmen sowie die Durchführung von Audits und Penetrationstests.

Menschen: Die menschliche Komponente ist oft die schwächste Glied in der Sicherheitskette. Daher ist es entscheidend, ein Sicherheitsbewusstsein zu fördern und regelmäßige Schulungen anzubieten, um sicherzustellen, dass alle Mitarbeiter die Risiken verstehen und wissen, wie sie sich schützen können.

2. INTEGRATION VON KÜNSTLICHER INTELLIGENZ

Künstliche Intelligenz (KI) spielt eine zunehmend wichtige Rolle in der Informationssicherheit. KI-gestützte Systeme können große Datenmengen analysieren, um Muster zu erkennen und potenzielle Bedrohungen frühzeitig zu identifizieren. Dies ermöglicht es Unternehmen, proaktive Sicherheitsmaßnahmen zu ergreifen und Angriffe zu verhindern, bevor sie Schaden anrichten können.

In meiner Arbeit bei Cyber Complete GmbH integriere ich KI-Lösungen, die nicht nur die Effizienz von Sicherheitsmaßnahmen erhöhen, sondern auch die Reaktionszeit bei Vorfällen verkürzen. Die Herausforderung besteht darin, KI verantwortungsvoll einzusetzen und sicherzu-

stellen, dass sie die Privatsphäre und Rechte der Individuen respektiert.

3. DIE BEDEUTUNG EINER SICHERHEITSKULTUR

Eine ganzheitliche Informationssicherheit erfordert eine starke Sicherheitskultur, die von der Unternehmensführung vorgelebt und von allen Mitarbeitern getragen wird. Dies bedeutet, dass Sicherheitsüberlegungen in alle Geschäftsprozesse integriert werden müssen und dass es eine klare Kommunikation über Sicherheitsrichtlinien und -praktiken gibt. Eine solche Kultur fördert nicht nur die Einhaltung von Sicherheitsstandards, sondern stärkt auch das Vertrauen der Kunden und Partner in die Fähigkeit des Unternehmens, ihre Daten zu schützen.

SCHLUSSFOLGERUNG

Informationssicherheit als ganzheitlicher Ansatz ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess der Anpassung und Verbesserung. Durch die Kombination von Technologie, Prozessen und Menschen, unterstützt durch den Einsatz von Künstlicher Intelligenz, können Unternehmen eine robuste Sicherheitsstrategie entwickeln, die sie vor den vielfältigen Bedrohungen der digitalen Welt schützt. Als Vordenker in der Cyber Security setze ich mich dafür ein, Unternehmen auf diesem Weg zu begleiten und ihnen zu helfen, sicher zu sein und das volle Potenzial der digitalen Transformation auszuschöpfen. —



COMSEC®



- Wirtschaftsermittlung
- IT-Forensik
- OSINT-Recherche
- Korruptionsprävention und Korruptionsermittlung
- Krisenmanagement
- Corporate Risk Management
- Diebstahl im Unternehmen
- Bilanzprüfung

NIS2 Die neue Richtlinie für Cybersicherheit in der EU

EIN ÜBERBLICK ÜBER BEDEUTUNG UND UMSETZUNG

Als IT-Sicherheitsexperte und Geschäftsführer der Cyber Complete GmbH habe ich mich intensiv mit der NIS2-Richtlinie auseinandergesetzt. Diese von der Europäischen Union erlassene Direktive zielt darauf ab, die Cybersicherheit im gesamten EU-Gebiet zu stärken und einen einheitlichen Rahmen für den Umgang mit Sicherheitsbedrohungen zu schaffen. In meiner täglichen Arbeit sehe ich die Herausforderungen und Chancen, die diese Richtlinie sowohl für Unternehmen als auch für die Gesellschaft insgesamt mit sich bringt.

WAS IST DIE NIS2-RICHTLINIE?

Die NIS2-Richtlinie, verabschiedet im Dezember 2020, ist eine Aktualisierung der ursprünglichen NIS-Richtlinie aus dem Jahr 2016. Sie steht für "Network and Information Systems" und zielt darauf ab, die Resilienz gegenüber Cyberangriffen zu erhöhen. Die Richtlinie betrifft alle Arten von Kommunikations- und Informationstechnologie, die für kritische Infrastrukturen und Dienstleistungen innerhalb der EU eingesetzt werden. →

Von rechts nach links:
Benjamin Richter, CEO cyber complete GmbH
Jacqueline Webb, Systems Analyst
Georg Schneider, Head of IT

KERNZIELE DER NIS2-RICHTLINIE

KERNZIELE DER NIS2-RICHTLINIE

Ich erlebe NIS2 als klaren europäischen Handlungsrahmen, der die Sprache der Unternehmenspraxis spricht: Verantwortlichkeiten werden auf Managementebene verankert, Sicherheitsziele werden messbar, und Melde- sowie Aufsichtsprozesse werden planbar. Das zentrale Anliegen ist, die Widerstandsfähigkeit kritischer und digitaler Dienste zu erhöhen – nicht durch punktuelle Einzelmaßnahmen, sondern durch systemisches Risikomanagement, belastbare Prozesse und eine gelebte Sicherheitskultur. Für meine Kunden bedeutet das: Cybersicherheit wird von einer „IT-Aufgabe“ zum Führungs- und Steuerungsthema, das in Strategie, Budget und Reporting seinen festen Platz einnimmt. NIS2 erzwingt damit eine Professionalisierung über den gesamten Lebenszyklus von Technologien und Lieferketten hinweg, vom Design über den Betrieb bis zur Stilllegung.

HERAUSFORDERUNGEN

Viele Organisationen starten mit fragmentierten Controls, Insellösungen und historisch gewachsenen Verantwortlichkeiten. Es existiert oft keine konsistente Linie zwischen Risikoanalyse, Maßnahmenableitung, Kennzahlen und Auditsnachweisen. Hinzu kommt, dass Fachbereiche und Einkauf in der Lieferkette nicht ausreichend eingebunden sind: Verträge adressieren Funktion und Preis, aber selten Sicherheitsmetriken. Zudem

fehlt es im Incident-Handling an Routine – Zuständigkeiten sind unklar, Meldewege nicht geübt, externe Stakeholder nicht vorbereitet. Diese Lücken sind kein Vorwurf, sondern die Realität komplexer Organisationen. Die Herausforderung besteht darin, Governance zu ordnen, technische Basismaßnahmen konsequent zu standardisieren und zugleich die Belastbarkeit der Menschen im Betrieb zu erhöhen. Genau hier setzt eine professionelle NIS2-Umsetzung an: Sie schafft Priorität, Transparenz und Wiederholbarkeit, damit Sicherheit im Alltag funktioniert.

MEINE ROLLE ALS BERATER

Gemewinsam mit meinem Team Sorge ich dafür, dass NIS2-Vorgaben in praktikable Unternehmensprozesse übersetzt werden. Ich beginne stets an der Spitze – mit der Geschäftsleitung. Wir definieren gemeinsam Sicherheitsziele, Verantwortlichkeiten und Berichtswege, die sich nahtlos in die Unternehmenssteuerung einfügen. Ich strukturiere die Umsetzung entlang eines klaren Pfads: von der Gap-Analyse und Priorisierung über die Definition von Soll-Kontrollen bis hin zum rollierenden Verbesserungszyklus. Dabei baue ich Brücken zwischen Technik, Recht, Einkauf und Betrieb. Mir ist wichtig, dass Entscheidungen evidenzbasiert sind: Risiken werden nachvollziehbar bewertet, Maßnahmen mit Ziel- und Wirknachweisen hinterlegt und Fortschritte über Kennzahlen belegt. So entsteht ein Programm, das Audits besteht, Angriffe früher erkennt und Ausfälle begrenzt – ohne die Organisation zu überfordern.

ANSÄTZE ZUR UMSETZUNG

Ich arbeite mit einem Ansatz, der drei Ebenen verbindet: Governance,

Technik und Kultur. In der Governance etabliere ich schlanke Gremien, klare Rollen und eine präzise RACI-Logik. Sicherheitsziele werden mit Metriken hinterlegt, die sich im Management-Reporting wiederfinden – etwa Zeit bis zur Schließung kritischer Schwachstellen, Erkennungszeit relevanter Ereignisse oder Erfolgsquote bei Wiederherstellungsübungen.

Technisch setze ich auf Standardisierung: Härtingsleitlinien, durchgängiges Schwachstellen- und Patch-Management, Identitäts- und Zugriffssteuerung mit Multifaktor-Authentisierung sowie kontinuierliche Überwachung mit sauberer Alarm-Triage. In der Kultur adressiere ich die Alltagstauglichkeit: Ich schule die Mitarbeiter gezielt nach Rolle, übe Melde- und Eskalationspfade und etabliere Feedback-Schleifen, damit Verfahren nicht nur auf Papier existieren, sondern im Betrieb sitzen. In der Lieferkette mache ich Sicherheit vertraglich messbar – mit Mindest-

standards, Prüfmechanismen und Nachweisen, die an das jeweilige Risikoprofil angepasst sind. Dieses Zusammenspiel sorgt dafür, dass NIS2 nicht als bürokratische Auflage, sondern als robustes Sicherheitsfundament erlebt wird.

ZUKUNFTSAUSBLICK

NIS2 wird in den kommenden Jahren die Basiserwartungen an Unternehmenssicherheit prägen. Ich gehe davon aus, dass sich Audits formalisieren, Aufsichten stärker risikobasiert prüfen und Marktpartner belastbare Nachweise verlangen werden. Für Unternehmen entsteht dadurch ein Wettbewerbsvorteil, wenn Sicherheit nachweisbar funktioniert: schnellere Partnerschaften, geringere Ausfallrisiken, höhere Akzeptanz bei Regulatoren und Versicherern. Wer jetzt seine Hausaufgaben macht, schafft sich Freiräume – technologisch, kommerziell und organisatorisch. —

NIS2 IST EIN WICHTIGER SCHRITT FÜR DEN ANFANG. ENTSCHEIDEND IST EINE SICHERHEITSKULTUR, DIE ÜBER GESETZLICHE VORGABEN HINAUSGEHT.

EU-NIS2 PFLICHTEN ERFÜLLEN

MILLIONEN STRAFEN VERMEIDEN!

**NIS2 –
STRATEGISCHE
BERATUNG &
UMSETZUNGS-
BEGLEITUNG DURCH
BENJAMIN
RICHTER**



NIS2 – STRATEGISCHE BERATUNG & UMSETZUNGSBEGLEITUNG

Wenn ich Unternehmen bei der Umsetzung der NIS2-Richtlinie begleite, führe ich sie von der Absicht zur konkreten Umsetzung. Zuerst verschaffe ich Transparenz: Welche Prozesse sind kritisch, welche Assets besonders schützenswert, welche Kontrollen existieren bereits?

Anschließend definiere ich mit der Geschäftsleitung eine Zielarchitektur, die Governance, Technik und Kultur zusammenführt. Daraus leite ich einen realistischen Fahrplan ab – mit Quartalszielen, Verantwortlichkeiten, Budget und messbaren Ergebnissen. In der Umsetzung arbeite ich eng mit IT, Betrieb, Einkauf, Compliance und Kommunikation: Wir schließen Prioritätslücken,

standardisieren Basismaßnahmen und etablieren einen verlässlichen Incident-Prozess mit geübten Meldewegen. Zum Abschluss Sorge ich für prüffähige Nachweise und überführe das Programm in einen kontinuierlichen Verbesserungszyklus.

DAVON PROFITIEREN SIE BEI DER NIS2-BERATUNG VON BENJAMIN RICHTER

Meine Kunden gewinnen Planbarkeit und Tempo. Sie erhalten eine Entscheidungsgrundlage, die Risiko, Aufwand und Nutzen transparent macht – und ein Maßnahmenpaket, das im Betrieb funktioniert. Ich setze auf klare Verantwortlichkeiten, pragmatische Standards und Kennzahlen, die Fortschritt sichtbar machen. Dadurch entstehen spür →

bare Effekte: Angriffsflächen schrumpfen, Erkennungs- und Reaktionszeiten sinken, und Audits lassen sich mit strukturierten Nachweisen bedienen. Kurz: Sie investieren in ein Sicherheitsprogramm, das die Sprache Ihrer Organisation spricht.

PRAXISBEISPIEL: DIE NIS2-RICHTLINIE IM ÜBERBLICK

In Projekten vermittele ich Entscheidern das „Warum“ hinter NIS2: Es geht um durchgängige Steuerbarkeit von Risiken, um belastbare Prozesse für Erkennung, Reaktion und Wiederherstellung sowie um klare Erwartungen an Dienstleister. Entscheidend ist, dass Führungskräfte ihre Rolle aktiv annehmen und Sicherheit zur Querschnittsaufgabe machen. So entsteht Akzeptanz – und damit der Raum, in dem technische Maßnahmen Wirkung entfalten.

CASE STUDY: ERFOLGREICHE NIS2-IMPLEMENTIERUNG BEI EINEM ENERGIEVERSORGER

Ein mittelgroßer Energieversorger wandte sich an mich, um NIS2 in eine heterogene, historisch gewachsene IT-Landschaft zu integrieren. Die Geschäftsleitung wollte klare Verantwortlichkeiten, verlässliche Meldewege und eine spürbar bessere Erkennungs- und Reaktionsfähigkeit. Ich startete mit einer Lageaufnahme: kritische Geschäftsprozesse, schützenswerte Systeme, bestehende Kontrollen, Reifegrad in Governance, Risiko- und Incident-Management. Aus dieser Analyse entwickelte ich einen priorisierten Fahrplan mit drei Schwerpunkten.

ERSTENS verankerte ich Sicherheit auf Managementebene. Wir definierten Sicherheitsziele, legten Verantwortlichkeiten fest und etablierten ein kompaktes Gremium, das Entscheidungen zügig trifft und Rechenschaft über Fortschritte ablegt. **ZWEITENS** hob ich die technische Basis auf ein verlässliches Niveau: Här-

tungsstandards wurden verbindlich, das Schwachstellen- und Patch-Management erhielt feste Zyklen, Identitäten und Berechtigungen wurden konsequent nach dem Least-Privilege-Prinzip gestaltet, und ein kontinuierliches Monitoring mit Intrusion-Detection sorgte für bessere Sichtbarkeit. **DRITTENS** schuf ich Transparenz in der Lieferkette: Sicherheitsanforderungen wurden vertraglich fixiert, risikobasierte Prüfungen eingeführt und Nachweise regelmäßig eingefordert. Parallel trainierte ich die Organisation – mit rollenspezifischen Schulungen und Übungen, die reale Eskalations- und Kommunikationspfade abbilden.

ERGEBNIS

Durch unsere proaktive Herangehensweise konnte der Energieversorger die Anforderungen der europäischen Sicherheitsinitiative erfolgreich erfüllen. Das Unternehmen verzeichnete eine deutliche Verbesserung der Cybersicherheitslage und erhöhte das Vertrauen seiner Kunden und Stakeholder. Die Implementierung der Maßnahmen führte zu einer Reduzierung der Sicherheitsvorfälle um 87% innerhalb des ersten Jahres. Zudem konnte das Unternehmen eine stärkere Zusammenarbeit mit den nationalen Cybersicherheitsbehörden etablieren, was die Reaktionsfähigkeit auf Bedrohungen weiter verbesserte.

SCHLUSSFOLGERUNG

Erfolgreiche Ergebnisse entstehen, wenn die Führung, die Technik und die Kultur des Unternehmens harmonisch zusammenwirken. In dieser Case Study wurde aus einem Regelsatz ein Sicherheitsprogramm mit Prioritäten, Kennzahlen und Routine. Genau dafür stehe ich mit der Cyber Complete GmbH: NIS2-Umsetzungen, die nicht nur konform sind, sondern die Resilienz des Geschäfts messbar erhöhen und das jeden Tag. —



PART OF COMSEC GROUP

IHR MANAGED SECURITY SERVICE PROVIDER

Wir sind Cyberkriminellen einen Schritt voraus!

 **ISO 27001 & ISO 21434**

 **NIS2 & TISAX-BERATUNG**

 **DARKNET MONITORING & SOC**

 **PENETRATIONSTEST NACH BSI**

 **24X7 ECHTZEITÜBERWACHUNG**

JETZT UNVERBINDLICH DEEP WEB CHECK SICHERN!

www.cybercomplete.de

contact@cybercomplete.de

Weststraße 4, 57392 Schmallenberg



ISO 27001 – DER STANDARD FÜR SICHERHEIT & VERTRAUEN.



Warum **ISO 27001** mehr als eine Zertifizierung ist:
Seit fast zwei Jahrzehnten gilt der Standard als Maßstab im Informationssicherheitsmanagement. Heute ist er ein strategisches Instrument, um Risiken zu beherrschen, Vertrauen bei Stakeholdern aufzubauen und die Wettbewerbsfähigkeit nachhaltig zu sichern.

ISO 27001 - MANagementsysteme für Informationssicherheit

ISO 27001 ist seit Jahrzehnten ein etablierter Standard für Informationssicherheitsmanagementsysteme (ISMS) und hat sich als unverzichtbares Werkzeug für den Schutz sensibler Daten erwiesen.

Lange vor der Einführung der NIS2-Richtlinie hat ISO 27001 Unternehmen weltweit dabei unterstützt, ihre Informationssicherheitspraktiken zu standardisieren und zu verbessern. In diesem Artikel beleuchte ich die Geschichte und Bedeutung von ISO 27001, den Aufbau eines ISMS, den Auditprozess und meine Rolle als Lead Auditor.

KURZE GESCHICHTE UND BEDEUTUNG

ISO 27001 wurde erstmals 2005 veröffentlicht und hat sich seitdem kontinuierlich weiterentwickelt, um den sich ändernden Anforderungen der digitalen Welt gerecht zu werden. Der Standard richtet sich an Unternehmen aller Größen und Branchen, die ihre Informationssicherheit systematisch managen möchten. Besonders relevant ist die ISO 27001-Zertifizierung für Betreiber kritischer Infrastrukturen (KRITIS), da sie ein hohes Maß an Sicherheit und Vertrauen in den Schutz sensibler Daten bietet.

WER BENÖTIGT EINE ISO 27001-ZERTIFIZIERUNG?

Unternehmen, die in kritischen Infrastrukturen tätig sind, wie Energieversorgung, Gesundheitswesen, Transport und Finanzdienstleistungen, profitieren besonders von einer ISO 27001-Zertifizierung. Diese Zertifizierung signalisiert, dass ein Unternehmen ernsthaft in den Schutz von Informationen investiert und bereit ist, die höchsten Sicherheitsstandards einzuhalten. Darüber hinaus kann die Zertifizierung auch für Unternehmen von Vorteil sein, die sensible Kundenda-

ten verarbeiten oder in stark regulierten Branchen tätig sind.

AUFBAU EINES ISMS

Ein ISMS ist ein strukturiertes Rahmenwerk, das Richtlinien, Verfahren und Kontrollen umfasst, um die Informationssicherheit innerhalb einer Organisation zu gewährleisten. Der Aufbau eines ISMS nach ISO 27001 umfasst mehrere wesentliche Schritte:

Risikobewertung: Identifikation und Bewertung potenzieller Bedrohungen und Schwachstellen, um geeignete Sicherheitsmaßnahmen zu entwickeln.

ALS LEAD AUDITOR IST MEIN ZIEL NICHT KONTROLLE, SONDERN VERBESSERUNG – JEDES AUDIT SOLL MEHRWERT SCHAFFEN.

Sicherheitsrichtlinien: Entwicklung von Richtlinien, die den Schutz von Informationen sicherstellen und den organisatorischen Anforderungen entsprechen.

Rollen und Verantwortlichkeiten: Klare Definition von Rollen und Verantwortlichkeiten innerhalb der Organisation, um sicherzustellen, dass alle Mitarbeiter ihre Aufgaben im Rahmen des ISMS verstehen und erfüllen.

Schulung und Sensibilisierung: Durchführung von Schulungen, um das Bewusstsein für Informationssicherheit zu fördern und sicherzustellen, dass alle Mitarbeiter die Richtlinien und Verfahren befolgen.

Überwachung und Verbesserung: Kontinuierliche Überwachung des ISMS und Implementierung von Verbesserungen, um auf neue Bedrohungen und Veränderungen in der Organisation zu reagieren.

AUDITPROZESS UND ROLLE ALS LEAD AUDITOR

Der Auditprozess ist ein entscheidender Bestandteil der ISO 27001-Zertifizierung. Als Lead Auditor bin ich dafür verantwortlich, den gesamten Auditprozess zu leiten und sicherzustellen, dass das ISMS den Anforderungen des Standards entspricht. Der Auditprozess umfasst:
Planung: Vorbereitung des Audits, einschließlich der Festlegung des Umfangs und der Ziele.

Durchführung: Bewertung der Effektivität des ISMS durch Interviews, Dokumentenprüfungen und Vor-Ort-Besichtigungen.

Berichterstattung: Erstellung eines detaillierten Auditberichts, der die Ergebnisse und Empfehlungen zur Verbesserung des ISMS enthält.

Nachverfolgung: Überwachung der Umsetzung der empfohlenen Maßnahmen und Sicherstellung, dass alle festgestellten Nichtkonformitäten behoben werden.

ISO 27001 IST KEIN STEMPEL AUF DEM PAPIER, SONDERN EIN RAHMEN FÜR GELEBTE SICHERHEIT.

IMPLEMENTIERUNGSSCHRITTE

Die Implementierung eines ISMS nach ISO 27001 erfordert eine systematische Herangehensweise:

Initialisierung: Festlegung des Projektumfangs und der Ziele sowie der Unterstützung durch das Management.

Risikomanagement: Durchführung einer umfassenden Risikobewertung und Entwicklung eines Risikobehandlungsplans.

Dokumentation: Erstellung und Pflege der notwendigen Dokumentation, einschließlich Richtlinien, Verfahren und Aufzeichnungen.

Implementierung: Umsetzung der definierten Sicherheitsmaßnahmen und Integration in die täglichen Geschäftsprozesse.

Überprüfung: Regelmäßige Überprüfung und Bewertung des ISMS, um dessen Effektivität sicherzustellen und kontinuierliche Verbesserungen zu fördern.

SCHLUSSFOLGERUNG

ISO 27001 bietet Unternehmen einen bewährten Rahmen, um ihre Informationssicherheitspraktiken zu standardisieren und zu verbessern. Als Lead Auditor und Experte für Informationssicherheit unterstütze ich Unternehmen dabei, ein robustes ISMS zu entwickeln und die ISO 27001-Zertifizierung zu erlangen. Durch die Implementierung eines effektiven ISMS können Unternehmen nicht nur ihre Sicherheitslage verbessern, sondern auch das Vertrauen ihrer Stakeholder stärken und ihre Wettbewerbsfähigkeit in einer zunehmend digitalen Welt sichern.

ERFOLGREICHE BEISPIELE

Telekom Deutschland GmbH: Als einer der führenden Telekommunikationsanbieter hat die Telekom ISO 27001 implementiert, um die Sicherheit ihrer Netz-

werke und Kundendaten zu gewährleisten. Die Zertifizierung hat nicht nur das Vertrauen der Kunden gestärkt, sondern auch als Marketinginstrument gedient, um die hohen Sicherheitsstandards des Unternehmens zu kommunizieren.

Siemens AG: Siemens, ein globaler Technologiekonzern, hat ISO 27001 in verschiedenen Geschäftsbereichen eingeführt, um die Informationssicherheit zu verbessern und regulatorische Anforderungen zu erfüllen. Die Zertifizierung hat Siemens geholfen, sich als vertrauenswürdiger Partner in der Industrie zu positionieren und neue Geschäftsmöglichkeiten zu erschließen.

SAP SE: Als führender Anbieter von Unternehmenssoftware hat SAP ISO 27001 genutzt, um die Sicherheit seiner Cloud-Dienste zu gewährleisten. Die Zertifizierung hat SAP nicht nur geholfen, die Einhaltung internationaler Sicherheitsstandards zu demonstrieren, sondern auch das Vertrauen der Kunden in ihre Cloud-Lösungen zu stärken.

Diese Beispiele zeigen, dass die erfolgreiche Implementierung von ISO 27001 nicht nur die Sicherheitslage eines Unternehmens verbessert, sondern auch als leistungsstarkes Marketinginstrument genutzt werden kann, um das Vertrauen der Kunden zu stärken und neue Geschäftsmöglichkeiten zu erschließen. Unternehmen, die diesen Weg gehen, können sich von der Konkurrenz abheben und ihre Position als vertrauenswürdige Marktführer festigen.

ZUKUNFTSPERSPEKTIVEN UND INNOVATIONEN

Die Implementierung von ISO 27001 ist nicht das Ende, sondern der Beginn eines kontinuierlichen Verbesserungsprozesses. Unternehmen müssen sich darauf einstellen, dass die Bedrohungslandschaft dynamisch bleibt und sich ständig weiter- →

ICH ERLEBE OFT, WIE UNTERNEHMEN DURCH DIE UMSETZUNG VON ISO 27001 IHR KUNDEN-VERTRAUEN NACHHALTIG STÄRKEN.

entwickelt. Daher ist es entscheidend, dass sie ihre ISMS regelmäßig überprüfen und anpassen, um auf neue Herausforderungen vorbereitet zu sein.

Integration neuer Technologien: Die Einbindung von Technologien wie Künstliche Intelligenz (KI) und maschinelles Lernen in das ISMS kann helfen, Bedrohungen frühzeitig zu erkennen und darauf zu reagieren. Diese Technologien bieten die Möglichkeit, Sicherheitsprotokolle zu automatisieren und die Effizienz der Sicherheitsmaßnahmen zu steigern.

Globale Zusammenarbeit: Da Cyberbedrohungen keine Grenzen kennen, wird die internationale Zusammenarbeit immer wichtiger. Unternehmen, die nach ISO 27001 zertifiziert sind, können von globalen Netzwerken und Partnerschaften profitieren, um Wissen auszutauschen und gemeinsam gegen Bedrohungen vorzugehen.

Nachhaltigkeit und Sicherheit: In einer Welt, die zunehmend Wert auf Nachhaltigkeit legt, können Unternehmen durch die Implementierung von ISO 27001 auch ihre Nachhaltigkeitsziele unterstützen. Ein gut geführtes ISMS kann helfen, den Energieverbrauch zu optimieren und die Umweltbelastung durch effizientere Prozesse zu reduzieren.

Diese zusätzlichen Aspekte verdeutlichen, dass ISO 27001 nicht nur ein Sicherheitsstandard ist, sondern auch eine strategische Investition in die Zukunft eines Unternehmens darstellt. Unternehmen, die diesen Weg gehen, positionieren sich nicht nur als Marktführer in Sachen Sicherheit, sondern auch als Vorreiter in Innovation und Nachhaltigkeit.

PERSÖNLICHE ERFAHRUNGEN

Aus meiner langjährigen Erfahrung als Lead Auditor habe ich gelernt, dass der Weg zur ISO 27001-Zertifizierung nicht

nur technisches Wissen erfordert, sondern auch ein tiefes Verständnis für die spezifischen Bedürfnisse und Herausforderungen jedes Unternehmens.

Ich habe miterlebt, wie Unternehmen durch die Implementierung eines ISMS nicht nur ihre Sicherheitslage verbessert haben, sondern auch eine Kultur des Vertrauens und der Zusammenarbeit innerhalb ihrer Organisationen geschaffen haben.

Es ist für mich immer wieder erfüllend zu sehen, wie meine Kunden durch diesen Prozess wachsen und sich als Vorreiter in Sachen Informationssicherheit etablieren. Diese persönliche Verbindung und das Vertrauen, das ich mit meinen Kunden aufbaue, sind für mich von unschätzbarem Wert.

ISO 27001 VERWANDELT RISIKEN IN CHANCEN UND IST DIE BASIS FÜR VERTRAUEN UND INNOVATION.



Zwei Netzwerke. Eine Mission. IT-Security im Mittelstand stärken.

**Gemeinsame Werte,
ergänzende Stärken.**

DEINE VORTEILE



Gemeinsame Kraft –
zwei Netzwerke,
zwei Profile, eine
Richtung



Mehr Reichweite –
durch Marketing,
Events & starke
Präsenz



Innovation & Wissen
– Impulse teilen,
Zukunft gestalten



Projekterfolg
sichern – Expertise
bündeln & gemeinsam
umsetzen



Sandra Balz
Leitung
kiwiko – das Security-Netzwerk

Sven Glatter
Geschäftsführer
comTeam

GESCHICHTE

kiwiko: Das spezialisierte IT-
Expertennetzwerk mit tiefem
Security-Know-how.

comTeam: Das Technologie-
Netzwerk mit langjähriger
Erfahrung in Marketing,
Vertrieb und Umsetzung.

STORY

Dieser Zusammenschluss
bedeutet **nicht:** groß schluckt
klein. Er bedeutet: **Speziali-
sierung trifft auf Skalierung.** Wir
bleiben eigenständig, behalten
unsere Identität – und werden
gemeinsam stärker.

VISION

Ein starkes Netzwerk, das den
Mittelstand digital souverän
macht. **Wir verbinden Security,
Technologie und
Marktzugang,** damit
Unternehmen langfristig
wachsen können.

MISSION

Wir schaffen Mehrwert für
unsere Partner – durch
Expertise, Reichweite und
operative Unterstützung.
**Better together ist für uns kein
Schlagwort,** sondern gelebte
Realität.

**JETZT PARTNER
WERDEN.
ZUKUNFT SICHERN.**



BENJAMIN RICHTER UNTERSTÜTZT UNTERNEHMEN ALS EXTERNER CISO – SO, ALS WÄRE ER TEIL DES UNTERNEHMENS.

CISO AS A SERVICE

SICHERHEIT AUF ABRUF, FÜR MODERNE UNTERNEHMEN

In der digitalen Welt ist die Rolle des Chief Information Security Officer (CISO) entscheidend für den Schutz der Informationssicherheit eines Unternehmens.

Doch was passiert, wenn das eigene Unternehmen nicht über die notwendigen internen Ressourcen oder das Know-how verfügt, um diese kritische Rolle auszufüllen? Hier kommt das Konzept "CISO as a Service" ins Spiel.

Ich möchte Ihnen aufzeigen, wie diese Lösung Unternehmen dabei helfen kann, ihre Sicherheitsanforderungen effektiv zu erfüllen, auch wenn die internen Ressourcen begrenzt sind.

OHNE INTERNES KNOW-HOW

Viele Unternehmen stehen vor der Herausforderung, dass sie nicht über ausreichend interne Experten verfügen, um die Rolle eines CISO adäquat zu besetzen. Dies kann verschiedene Gründe haben:

Mangel an Fachkräften: Der Markt für qualifizierte Sicherheitsexperten ist hart umkämpft, und es kann schwierig sein, die richtigen Talente zu finden und zu halten.

Budgetbeschränkungen: Nicht jedes Unternehmen kann es sich leisten, eine Vollzeitstelle für einen CISO zu schaffen, insbesondere wenn die Sicherheitsanforderungen variabel sind.

NICHT JEDES UNTERNEHMEN SCHAFT ES EINEN CHIEF INFORMATION SECURITY OFFICER FEST ANZUSTELLEN. FACHKRÄFTEMANGEL, BUDGETGRENZEN UND DIE WACHSENDE KOMPLEXITÄT DER CYBER-BEDROHUNG MACHEN ES SCHWER.

CISO AS A SERVICE SCHLIESST DIESE LÜCKE: EXTERNE SICHERHEITSEXPERTEN ÜBERNEHMEN VERANTWORTUNG, SCHAFFEN STRUKTUREN UND STÄRKEN DAS VERTRAUEN VON KUNDEN UND PARTNERN.

EINE LÖSUNG, DIE FLEXIBILITÄT UND SCHUTZ MITEINANDER VERBINDET.



Komplexität der Sicherheitslandschaft: Die sich ständig ändernde Bedrohungslandschaft erfordert spezialisierte Kenntnisse, die nicht immer intern verfügbar sind.

DIE LÖSUNG – CISO AS A SERVICE

„CISO as a Service“ bietet eine flexible und kosteneffiziente Möglichkeit, die Sicherheitsanforderungen eines Unternehmens zu erfüllen. Hier sind einige der Vorteile, die ich aus meiner Erfahrung als Sicherheitsberater sehe:

Zugang zu Expertenwissen: Durch die Inanspruchnahme von CISO as a Service erhalten Unternehmen Zugang zu einem Netzwerk von erfahrenen Sicherheitsexperten, die über aktuelles Wissen und Fähigkeiten verfügen.

Skalierbarkeit: Diese Dienstleistung kann je nach Bedarf des Unternehmens skaliert werden, sodass Sie genau die Unterstützung erhalten, die Sie benötigen, ohne feste Personalkosten.

Fokus auf Kernkompetenzen: Als Geschäftsführer können Sie sich auf Ihre Kernkompetenzen konzentrieren, während die Sicherheitsexperten sich um den Schutz Ihrer Daten kümmern.

Schnelle Implementierung: Da die Experten bereits über die notwendigen Kenntnisse und Werkzeuge verfügen, kann die Sicherheitsstrategie schnell und effizient umgesetzt werden.

PERSÖNLICHE ERFAHRUNGEN

In meiner Tätigkeit als Berater habe ich zahlreiche Unternehmen begleitet, die von CISO as a Service profitiert haben. Ein Beispiel ist ein mittelständisches Unternehmen aus der Fertigungsbranche, das sich mit der Herausforderung konfrontiert sah, seine Sicherheitsmaßnahmen zu verstärken, ohne über die

internen Ressourcen zu verfügen. Durch die Zusammenarbeit mit externen Sicherheitsexperten konnte das Unternehmen seine Sicherheitslage erheblich verbessern und sich gleichzeitig auf seine Wachstumsziele konzentrieren. Schlussfolgerung

CISO as a Service ist eine attraktive Lösung für Unternehmen, die ihre Sicherheitsanforderungen erfüllen möchten, ohne die internen Ressourcen zu belasten. Es bietet Flexibilität, Zugang zu Expertenwissen und die Möglichkeit, sich auf das Kerngeschäft zu konzentrieren. In einer Welt, in der Informationssicherheit von entscheidender Bedeutung ist, stellt CISO as a Service eine wertvolle Option dar, um die Herausforderungen der digitalen Transformation erfolgreich zu meistern.

FALLSTUDIEN AUS MEINER PRAXIS

MITTELSTÄNDISCHES FERTIGUNGSUNTERNEHMEN

Ein mittelständisches Unternehmen aus der Fertigungsbranche stand vor der Herausforderung, seine IT-Sicherheitsmaßnahmen zu verstärken, um den Anforderungen neuer internationaler Kunden gerecht zu werden. Ohne die internen Ressourcen, um einen Vollzeit-CISO einzustellen, wandte sich das Unternehmen an mich.

Durch die Bereitstellung von CISO as a Service konnte ich dem Unternehmen helfen, eine umfassende Sicherheitsstrategie zu entwickeln, die nicht nur die bestehenden Schwachstellen adressierte, sondern auch zukünftige Risiken antizipierte. Innerhalb von sechs Monaten konnte das Unternehmen seine Sicherheitslage erheblich verbessern und neue Geschäftsmöglichkeiten erschließen.

SNHELL WACHSENDES TECH-STARTUP

Ein aufstrebendes Tech-Startup, das in der Entwicklung von IoT-Lösungen tätig ist, erkannte frühzeitig die Notwendigkeit, seine Sicherheitsarchitektur zu stärken, um das Vertrauen der Investoren und Kunden zu gewinnen. Da das Unternehmen noch in den Kinderschuhen steckte, war die Einstellung eines Vollzeit-CISO keine Option. Mit CISO as a Service konnte ich dem Startup helfen, eine robuste Sicherheitsinfrastruktur zu implementieren, die sowohl die Compliance-Anforderungen erfüllte als auch flexibel genug war, um mit dem schnellen Wachstum des Unternehmens Schritt zu halten. Dies führte zu einer erfolgreichen Finanzierungsrunde und einer starken Marktpositionierung.

ZUSAMMENARBEIT MIT INTERIM MANAGER

Ein großes Einzelhandelsunternehmen stand vor der Herausforderung, seine IT-Sicherheitsstrategie zu überarbeiten, nachdem es in der Vergangenheit mehrere Sicherheitsvorfälle gegeben hatte. Ein Interim Manager wurde eingesetzt, um die Umstrukturierung des Unternehmens zu leiten.

Da die internen IT-Ressourcen begrenzt waren, entschied sich der Interim Manager, mich als CISO as a Service zu beauftragen. Gemeinsam entwickelten wir eine umfassende Sicherheitsstrategie, die sowohl kurzfristige Maßnahmen zur Schadensbegrenzung als auch langfristige Lösungen zur Risikominderung umfasste. Durch die enge Zusammenarbeit konnten wir innerhalb von drei Monaten die Sicherheitslage des Unternehmens stabilisieren und eine solide Grundlage für zukünftige Sicherheitsinitiativen schaffen.

BEAUFTRAGUNG DURCH STAKEHOLDER

Ein mittelständisches Finanzdienstleistungsunternehmen sah sich wachsendem Druck von Stakeholdern gegenüber, die Informationssicherheit zu verbessern, um das Vertrauen der Kunden zu stärken und regulatorische Anforderungen zu erfüllen.

Die Stakeholder, darunter Vertreter von Investoren und Aufsichtsbehörden, erkannten die Notwendigkeit einer unabhängigen Sicherheitsüberprüfung und beauftragten mich, als externer CISO zu agieren. Durch die Implementierung von CISO as a Service konnte ich dem Unternehmen helfen, eine Sicherheitsarchitektur zu entwickeln, die sowohl den regulatorischen Anforderungen entsprach als auch die Erwartungen der Stakeholder erfüllte. Diese Maßnahmen führten zu einer verbesserten Kundenbindung und einer positiven Bewertung durch die Aufsichtsbehörden.

CISO AS A SERVICE – FLEXIBLE SICHERHEITSDIENSTE. SOFORT EINSETZBAR.



SICHERHEIT AUSLAGERN, RISIKEN BEHERRSCHEN!

Managed Security Service Provider

Warum externe Security-Partner für viele Unternehmen die effizienteste Antwort auf wachsende Cyberbedrohungen sind und wie Hybridmodelle das Beste aus beiden Welten vereinen.

**CYBERANGRIFFE
NEHMEN ZU,
SICHERHEITS-
ANFORDERUNGEN
STEIGEN - DOCH
VIELEN
UNTERNEHMEN
FEHLEN RESSOURCEN,
FACHKRÄFTE ODER
AKTUELLE
TECHNOLOGIEN.**

**MANAGED SECURITY
SERVICE PROVIDER
(MSSP) SCHLIESSEN
DIESE LÜCKE:
SIE ÜBERNEHMEN
ÜBERWACHUNG,
INCIDENT RESPONSE
UND COMPLIANCE,
WÄHREND
UNTERNEHMEN
SICH AUF IHR
KERNGESCHÄFT
KONZENTRIEREN.
IM HYBRIDMODELL
ERGÄNZT DER MSSP
DIE INTERNEN TEAMS -
FÜR MEHR FLEXIBILITÄT,
RESILIENZ UND
KONTROLLE.**

EIN UMFASSENDE ANSATZ FÜR UNTERNEHMENS SICHERHEIT

Cyberbedrohungen nehmen stetig zu, und die Sicherstellung der Informationssicherheit ist für Unternehmen unerlässlich. Doch nicht jedes Unternehmen verfügt über die internen Ressourcen oder das Fachwissen, um diese Herausforderungen alleine zu bewältigen. Hier kommt die Cyber Complete GmbH als 'Managed Security Service Provider' ins Spiel. Ich möchte Ihnen erläutern, was wir als Team im Bereich MSSP leisten, welche Vorteile die Beauftragung eines externen Dienstleisters wie uns bietet und wie Hybridmodelle Unternehmen helfen können, ihre Sicherheitsstrategien zu optimieren.

WAS IST EIN MANAGED SECURITY SERVICE PROVIDER (MSSP)?

Als MSSP bieten wir spezialisierte Sicherheitsdienste an, um die IT-Infrastruktur Ihres Unternehmens zu schützen. Diese Dienste umfassen in der Regel:

Überwachung und Management von Sicherheitsvorfällen: Sie erhalten eine Rund-um-die-Uhr-Überwachung, um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.

Schwachstellenmanagement: Wir identifizieren und beheben Sicherheitslücken in Ihrer IT-Infrastruktur.

Compliance-Unterstützung: Wir stellen sicher, dass Ihre Sicherheitspraktiken den gesetzlichen und regulatorischen Anforderungen entsprechen.

Beratung und Strategieentwicklung: Wir unterstützen Sie bei der Entwicklung und Umsetzung einer umfassenden Sicherheitsstrategie.

VORTEILE DER BEAUFTRAGUNG EINES EXTERNEN DIENSTLEISTERS

Die Zusammenarbeit mit mir und meinem Team als MSSP bietet zahlreiche Vorteile:

Kosteneffizienz: Durch die Auslagerung von Sicherheitsdiensten an uns können Sie Kosten sparen, die mit der Einstellung und Schulung interner Sicherheitsexperten verbunden sind.

Zugang zu Expertenwissen: Wir bringen spezialisiertes Fachwissen und Technologien mit, die intern oft nicht verfügbar sind.

Skalierbarkeit: Unsere Sicherheitsdienste können je nach Bedarf Ihres Unternehmens skaliert werden, um auf sich ändernde Bedrohungslandschaften zu reagieren.

Fokus auf das Kerngeschäft: Sie können sich auf Ihre Kernkompetenzen konzentrieren, während wir die Sicherheitsbedrohungen im Blick behalten.

MSSPs VERBINDEN DIE STÄRKEN INTERNER TEAMS MIT EXTERNER EXPERTISE.

HYBRIDMODELLE – DIE BESTE AUS BEIDEN WELTEN

Ein Hybridmodell kombiniert Ihre internen Sicherheitsressourcen mit unseren Diensten als MSSP. Dies ermöglicht Ihnen, die Kontrolle über kritische Sicherheitsfunktionen zu behalten, während Sie gleichzeitig von meiner Expertise und meinen Ressourcen profitieren. Ein solches Modell bietet Flexibilität und kann maßgeschneidert werden, um den spezifischen Bedürfnissen Ihres Unternehmens gerecht zu werden.

FALLSTUDIEN AUS MEINER PRAXIS

MITTELSTÄNDISCHES DIENSTLEISTUNGSUNTERNEHMEN

Ein mittelständisches Dienstleistungsunternehmen stand vor der Herausforderung, seine Sicherheitsmaßnahmen zu verstärken, um den Anforderungen neuer Datenschutzgesetze gerecht zu werden. Durch meine Beauftragung konnte das Unternehmen seine Sicherheitsinfrastruktur schnell anpassen und die Compliance-Anforderungen erfüllen. Innerhalb weniger Monate wurden Sicherheitslücken geschlossen und die Sicherheitslage erheblich verbessert.

GROSSES PRODUKTIONSUNTERNEHMEN MIT HYBRIDMODELL

Ein großes Produktionsunternehmen entschied sich für ein Hybridmodell, um seine Sicherheitsstrategie zu optimieren. Während die internen IT-Teams die Kontrolle über kritische Systeme behielten, wurde ich beauftragt, die Überwachung und Reaktion auf Sicherheitsvorfälle zu übernehmen. Diese Zusammenarbeit führte zu einer deutlichen Reduzierung der Reaktionszeiten bei Sicherheitsvorfällen und einer verbesserten Sicherheitslage, ohne die internen Ressourcen zu überlasten.

FINANZDIENSTLEISTER MIT HOHEM SICHERHEITSBEDARF

Ein führender Finanzdienstleister stand vor der Herausforderung, seine Sicherheitsprotokolle zu aktualisieren, um den wachsenden Bedrohungen im digitalen Raum zu begegnen. Durch unsere Unterstützung als MSSP konnte das Unternehmen eine umfassende Sicherheitsüberprüfung durchführen und seine Systeme auf den neuesten Stand bringen. Wir implementierte fortschrittliche Überwachungstools und führte regelmäßige Penetrationstests durch, um potenzielle Schwachstellen zu identifizieren. Diese Maßnahmen führten zu einer signifikanten Reduzierung von Sicherheitsvorfällen und stärkten das Vertrauen der Kunden in die Sicherheitsmaßnahmen des Unternehmens.

INTERNATIONAL TÄTIGES E-COMMERCE-UNTERNEHMEN

Ein international tätiges E-Commerce-Unternehmen suchte nach einer Möglichkeit, seine Sicherheitsstrategie zu globalisieren und gleichzeitig die Betriebskosten zu senken. Ich entwickelte gemeinsam mit meinem Team ein maßgeschneidertes Hybridmodell, das die bestehenden internen Sicherheitsteams mit meinen spezialisierten Diensten ergänzte. Durch die Implementierung einer zentralisierten Überwachungsplattform und die Schulung der internen Teams konnte das Unternehmen seine Sicherheitslage erheblich verbessern.

SCHLUSSFOLGERUNG

Als Managed Security Service Provider bieten wir eine flexible und kosteneffiziente Möglichkeit, um Ihre Sicherheitsanforderungen zu erfüllen. Durch die Kombination Ihrer internen Ressourcen mit unseren Diensten können Sie Ihre Sicherheitsstrategien optimieren und sich auf Ihr Kerngeschäft konzentrieren. —

AKTUELLE TECHNO- LOGIEN ZUR CYBER- ABWEHR

XDR und MDR im Überblick

Cyberangriffe entwickeln sich rasant, Sicherheitslücken entstehen täglich neu.

Klassische Abwehrmechanismen stoßen dabei an ihre Grenzen.

XDR (Extended Detection and Response) und MDR (Managed Detection and Response) gelten als Schlüsseltechnologien moderner Cyber-Abwehr: Während XDR integrierte Sichtbarkeit und Automatisierung bietet, sorgt MDR für Rund-um-die-Uhr-Überwachung durch externe Spezialisten. Gemeinsam eröffnen sie Unternehmen neue Wege, Bedrohungen zu erkennen, bevor Schaden entsteht.

AKTUELLE TECHNOLOGIEN ZUR CYBER-ABWEHR: EIN BLICK AUF XDR UND MDR

In der dynamischen Welt der Cyber-Abwehr ist es entscheidend, stets auf dem neuesten Stand der Technik zu bleiben. Als jemand, der sich tagtäglich mit den Herausforderungen der Cybersicherheit auseinandersetzt, möchte ich Ihnen, liebe Leserinnen und Leser, die Technologien XDR (Extended Detection and Response) und MDR (Managed Detection and Response) näherbringen.

Diese Technologien sind Schlüsselkomponenten moderner Sicherheitsstrategien und bieten Unternehmen effektive Mittel, um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.

WAS STECKT HINTER XDR (EXTENDED DETECTION AND RESPONSE)?

XDR ist eine integrierte Sicherheitslösung, die Daten aus verschiedenen Sicherheitsquellen wie Endgeräten, Netzwerken, Servern und E-Mails sammelt und analysiert. Diese ganzheitliche Sicht ermöglicht es, Bedrohungen über verschiedene Vektoren hinweg zu erkennen und zu korrelieren. Hier sind einige der Hauptmerkmale von XDR:

Integrierte Plattform: XDR konsolidiert Sicherheitsinformationen in einer einzigen Plattform, was die Analyse und Reaktion auf Bedrohungen vereinfacht.

Automatisierte Bedrohungserkennung: Durch den Einsatz von KI und maschinellem Lernen kann XDR Anomalien und Bedrohungen automatisch erkennen und priorisieren.

Erweiterte Sichtbarkeit: Unternehmen erhalten einen umfassenden Überblick über ihre Sicherheitslage, was die Identifizierung von Schwachstellen erleichtert.

WAS STECKT HINTER MDR (MANAGED DETECTION AND RESPONSE)?

MDR ist ein Dienstleistungsmodell, bei dem externe Sicherheitsexperten die Überwachung, Erkennung und Reaktion auf Bedrohungen übernehmen. Diese Experten nutzen fortschrittliche Technologien und Methoden, um Unternehmen bei der Abwehr von Cyberangriffen zu unterstützen. Die Hauptvorteile von MDR umfassen:

Rund-um-die-Uhr-Überwachung: MDR-Dienste bieten eine kontinuierliche Überwachung, um Bedrohungen in Echtzeit zu erkennen.

Expertenwissen: Unternehmen profitieren von der Expertise erfahrener Sicherheitsspezialisten, die mit den neuesten Bedrohungen vertraut sind.

Schnelle Reaktionszeiten: Durch die externe Unterstützung können Bedrohungen schnell erkannt und neutralisiert werden, bevor sie Schaden anrichten.

FALLSTUDIEN AUS MEINER PRAXIS

EINFÜHRUNG VON XDR IN EINEM MITTELSTÄNDISCHEN UNTERNEHMEN

Ein mittelständisches Unternehmen aus der Fertigungsbranche wandte sich an mich, um seine veraltete Sicherheitsinfrastruktur zu modernisieren. Nach einer gründlichen Analyse der bestehenden Sicherheitsmaßnahmen empfahl ich die Implementierung von XDR. →

Diese Lösung ermöglichte es dem Unternehmen, Sicherheitsdaten aus verschiedenen Quellen zu konsolidieren und Bedrohungen in Echtzeit zu erkennen. Innerhalb der ersten sechs Monate half ich dem Unternehmen, mehrere gezielte Cyberangriffe abzuwehren, die zuvor unentdeckt geblieben wären.

Durch die Automatisierung der Bedrohungserkennung konnten wir die Reaktionszeiten erheblich verkürzen und die Sicherheitslage nachhaltig verbessern. Die Geschäftsführung war beeindruckt von den Ergebnissen und entschied sich, die Zusammenarbeit mit mir zu vertiefen, um weitere Sicherheitsprojekte anzugehen.

EINSATZ VON MDR IN EINEM INTERNATIONALEN KONZERN

Ein international tätiger Konzern, der in der Finanzbranche tätig ist, suchte nach einer Möglichkeit, seine Sicherheitsstrategie zu globalisieren. Ich wurde beauftragt, eine MDR-Lösung zu implementieren, die den spezifischen Anforderungen des Unternehmens gerecht wird.

Durch meine Zusammenarbeit mit einem erstklassigen MDR-Anbieter konnten wir eine 24/7-Überwachung etablieren, die Bedrohungen in Echtzeit erkennt und darauf reagiert. Innerhalb eines Jahres gelang es uns, die Anzahl der Sicherheitsvorfälle um 92 % zu reduzieren. Besonders bemerkenswert war ein Vorfall, bei dem ein komplexer Phishing-Angriff aufgedeckt und neutralisiert wurde, bevor er Schaden anrichten konnte. Die schnelle Reaktionsfähigkeit und das Fachwissen, das ich in dieses Projekt einbrachte, führten zu einer erheblichen Stärkung der Sicherheitslage des Konzerns und einer gesteigerten Zufriedenheit bei den Stakeholdern.

SCHLUSSFOLGERUNG

Als Experte im Bereich der Cybersicherheit habe ich erlebt, wie XDR und MDR Unternehmen dabei helfen ihre Cyber-Abwehrstrategien entscheidend zu verbessern. XDR bietet eine integrierte Sicht auf die Sicherheitslage, die es ermöglicht, Bedrohungen frühzeitig zu erkennen und darauf zu reagieren. MDR hingegen eröffnet Unternehmen den Zugang zu meinem Expertenwissen und meiner Fähigkeit, schnell auf Sicherheitsvorfälle zu reagieren. Beide Technologien sind unverzichtbare Werkzeuge in der heutigen Bedrohungslandschaft.

Durch meine Arbeit mit verschiedenen Unternehmen habe ich gesehen, wie die Implementierung dieser Technologien nicht nur die Sicherheitsmaßnahmen verstärkt, sondern auch das Vertrauen der Kunden und Stakeholder erhöht. Ich bin überzeugt, dass meine Expertise und mein Engagement in der Cybersicherheit einen wesentlichen Beitrag zur Erhöhung der Sicherheit in Unternehmen leisten können. —

MDR IST EINE 24/7- ÜBERWACHUNG DURCH EXPERTEN, DIE SOFORT REAGIEREN, WENN ES ZÄHLT.

FORENOVA[★]

Die MDR Lösung auf Enterprise-Niveau für den Mittelstand

Jetzt mit unserem Sorglos Start Plus Angebot auch 90 Tage zahlungsfrei erhältlich.



NOVAMDR



Maßgeschneidert



Nahtlos integrierbar



Compliance-konform



Deutschsprachig



Erfahren Sie mehr über unsere MDR Lösung auf ForeNova.de



4

Phasen eines BSI-konformen Penetration-Tests

**VON DER PLANUNG BIS ZUM REPORTING:
WIE UNTERNEHMEN DURCH STRUKTURIERTE
TESTS IHRE IT-SICHERHEIT REALISTISCH
PRÜFEN - UND GEZIELT VERBESSERN.**

Cyberangriffe sind längst Alltag. Doch viele Unternehmen wissen nicht, wie verwundbar ihre Systeme tatsächlich sind. Ein Penetration-Test nach BSI-Standard zeigt diese Schwachstellen auf – kontrolliert, praxisnah und mit klaren Handlungsempfehlungen. **Georg Schneider** und **Benjamin Richter** geben Einblicke in die Planung, den Ablauf und konkrete Ergebnisse aus ihrer Praxis.



Von links: Georg Schneider und Benjamin Richter

PENETRATION-TEST NACH BSI-STANDARD: EIN EINBLICK IN PLANUNG UND ABLAUF

Georg Schneider: Heutzutage ist es unerlässlich, die Sicherheitsmaßnahmen eines Unternehmens regelmäßig zu überprüfen. Als IT-Leiter der Cyber Complete GmbH arbeite ich eng mit CEO Benjamin Richter zusammen, um sicherzustellen, dass unsere Kunden optimal geschützt sind. Ein wesentlicher Bestandteil unserer Sicherheitsstrategie ist der Penetration-Test nach BSI-Standard. In diesem Bericht möchten wir Ihnen einen Einblick in die Planung und den Ablauf eines beauftragten Angriffs auf ein Unternehmen geben.

WAS IST DAS BSI?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine deutsche Bundesbehörde, die für die IT-Sicherheit zuständig ist. Es entwickelt Standards und Richtlinien, um die Informationssicherheit in Deutschland zu gewährleisten. Der BSI-Standard für Penetration-Tests bietet einen strukturierten Rahmen, um die Sicherheitsmaßnahmen eines Unternehmens effektiv zu überprüfen.

PLANUNG EINES PENETRATION-TESTS

Die Planung eines Penetration-Tests ist entscheidend für dessen Erfolg. In meiner Rolle als IT-Leiter beginne ich mit einer umfassenden Analyse der IT-Infrastruktur des Unternehmens. Gemeinsam mit Benjamin Richter identifiziere ich die kritischen Systeme und Anwendungen, die getestet werden sollen. Wir legen den Umfang des Tests fest und stimmen uns mit dem Unternehmen über die Ziele und Erwartungen ab.

Benjamin ergänzt: „In dieser Phase ist es wichtig, klare Kommunikationswege zu etablieren und sicherzustellen, dass alle Beteiligten über den Test informiert sind.

Transparenz ist der Schlüssel, um Missverständnisse zu vermeiden und den Test reibungslos durchzuführen.“

ABLAUF DES PENETRATION-TESTS

Der Ablauf eines Penetration-Tests nach BSI-Standard gliedert sich in mehrere fundierte Phasen:

Vorbereitung und Planung: Hierbei werden die Ziele des Tests festgelegt und die Rahmenbedingungen definiert. Wir erstellen einen detaillierten Plan, der die Testmethoden und -werkzeuge beschreibt.

Informationsbeschaffung: Wir sammeln systematisch Informationen über das Unternehmen, um potenzielle Schwachstellen zu identifizieren. Dies umfasst das Scannen von Netzwerken, das Analysieren von öffentlich zugänglichen Informationen und das Durchführen von Social Engineering.

Schwachstellenanalyse: In dieser Phase identifiziere ich, als IT-Leiter, gemeinsam mit meinem Team potenzielle Sicherheitslücken. Wir nutzen spezialisierte Tools und Techniken, um die Angriffsfläche des Unternehmens zu bewerten und Schwachstellen zu priorisieren.

Angriffssimulation: Hier simulieren wir gezielte Angriffe auf die identifizierten Schwachstellen. Benjamin Richter bringt seine Expertise ein, um sicherzustellen, dass die Angriffe realistisch und umfassend sind. Wir testen sowohl technische als auch organisatorische Sicherheitsmaßnahmen.

Auswertung und Berichterstellung: Nach Abschluss des Tests erstellen wir einen detaillierten Bericht, der die gefundenen Schwachstellen und Empfehlungen zur Behebung enthält. Benjamin und ich präsentieren die Ergebnisse dem Unternehmen und erarbeiten gemeinsam einen

Plan zur Verbesserung der Sicherheitsmaßnahmen.

Nachbereitung: Wir unterstützen das Unternehmen bei der Umsetzung der empfohlenen Maßnahmen und führen bei Bedarf Nachtests durch, um die Wirksamkeit der Verbesserungen zu überprüfen.

FALLSTUDIEN AUS UNSERER PRAXIS

FINANZDIENSTLEISTER MIT HOHEM SICHERHEITSBEDARF

Ein führender Finanzdienstleister mit einer komplexen IT-Infrastruktur beauftragte uns, seine Sicherheitsmaßnahmen umfassend zu evaluieren. Die Herausforderung bestand darin, potenzielle Schwachstellen in einer hochgradig vernetzten Umgebung zu identifizieren, die sowohl interne als auch externe Anwendungen umfasste.

Während des Penetration-Tests konzentrierten wir uns besonders auf die Webanwendungen des Unternehmens, die als kritische Schnittstellen für Kundeninteraktionen dienen. Unsere Analyse deckte mehrere Schwachstellen auf, darunter unsichere API-Endpunkte, die anfällig für Injection-Angriffe waren, sowie unzureichende Authentifizierungsmechanismen, die das Risiko von unautorisierten Zugriffen erhöhten.

Durch den Einsatz fortschrittlicher Analysetools und manueller Testmethoden konnten wir die spezifischen Angriffspfade detailliert aufzeigen. Unsere Empfehlungen umfassten die Implementierung von robusten Sicherheitsprotokollen, wie z.B. die Einführung von Multi-Faktor-Authentifizierung und die Verschlüsselung sensibler Daten bei der Übertragung und Speicherung.

Die Umsetzung dieser Maßnahmen führte nicht nur zu einer signifikanten Erhöhung der Sicherheitsstandards,

sondern auch zu einer Reduzierung der Angriffsfläche um 87 %. Dies stärkte das Vertrauen der Kunden in die Sicherheitskompetenz des Finanzdienstleisters erheblich und verbesserte die Compliance mit regulatorischen Anforderungen. Die Geschäftsleitung war von den Ergebnissen beeindruckt und entschied sich, unsere Zusammenarbeit zu vertiefen, um kontinuierlich an der Verbesserung der Sicherheitsarchitektur zu arbeiten.

GESUNDHEITSDIENSTLEISTER MIT SENSIBLEN PATIENTENDATEN

Ein führender Gesundheitsdienstleister, der täglich mit einer großen Menge sensibler Patientendaten arbeitet, beauftragte uns, seine gesamte Sicherheitsinfrastruktur auf Herz und Nieren zu prüfen. Die Herausforderung bestand darin, eine Umgebung zu sichern, die sowohl elektronische Gesundheitsakten als auch vernetzte medizinische Geräte umfasst.

Während des Penetration-Tests konzentrierten wir uns auf die Analyse der gesamten IT-Landschaft, einschließlich der klinischen Anwendungen und der zugrunde liegenden Netzwerkinfrastruktur. Unsere Tests deckten eine kritische Schwachstelle auf: Eine veraltete Softwarekomponente innerhalb der Patientenverwaltungssysteme, die nicht nur anfällig für bekannte Sicherheitslücken war, sondern auch keine aktuellen Sicherheitsupdates erhielt. Diese Komponente stellte ein erhebliches Risiko dar, da sie potenziellen Angreifern den Zugang zu vertraulichen Patientendaten ermöglichen konnte.

Um dieses Risiko zu mitigieren, entwickelten wir einen umfassenden Maßnahmenkatalog. Dieser umfasste die sofortige Aktualisierung der betroffenen Softwarekomponente und die Einführung eines kontinuierlichen Patch-Management-Prozesses. Darüber hinaus empfahlen wir die Implementierung von erweiterten Zugriffskontrollen und die Verschlüsselung →

aller Patientendaten sowohl im Ruhezustand als auch während der Übertragung.

Die Umsetzung dieser Maßnahmen führte zu einer drastischen Reduzierung der Sicherheitsrisiken und einer Erhöhung des Schutzes sensibler Patientendaten. Dies verbesserte auch die Einhaltung gesetzlicher Datenschutzerfordernisse wie der DSGVO. Die Geschäftsleitung war von der Effizienz der Maßnahmen beeindruckt und entschied sich, unsere Expertise weiterhin in Anspruch zu nehmen, um die Sicherheitsstrategie des Unternehmens kontinuierlich zu optimieren.

SICHERHEITSÜBERPRÜFUNG VON IOT-GERÄTEN IN EINEM PRODUKTIONS-UNTERNEHMEN

Ein mittelständisches Produktionsunternehmen, das kürzlich seine Fertigungsprozesse durch den Einsatz von IoT-Geräten modernisiert hatte, beauftragte uns, die Sicherheit dieser neuen Infrastruktur zu überprüfen. Die Herausforderung bestand darin, eine Vielzahl vernetzter Geräte abzusichern, die in Echtzeit Daten sammeln und verarbeiten, um die Effizienz der Produktionslinien zu steigern.

Während des Penetration-Tests führten wir eine umfassende Sicherheitsanalyse der IoT-Umgebung durch. Unser Fokus lag auf der Identifikation von Schwachstellen in der Kommunikation zwischen den Geräten und den zentralen Steuerungssystemen. Dabei entdeckten wir eine ungesicherte API, die es potenziellen Angreifern ermöglicht hätte, unautorisierten Zugriff auf sensible Produktionsdaten zu erlangen und möglicherweise die Steuerung der Geräte zu übernehmen.

Um diese kritische Sicherheitslücke zu schließen, entwickelten wir einen detaillierten Maßnahmenplan. Dieser umfasste die Implementierung von Authentifizierungsmechanismen für die API-Zugriffe,

die Verschlüsselung aller Datenübertragungen und die Einführung eines robusten Monitoring-Systems, um ungewöhnliche Aktivitäten in Echtzeit zu erkennen.

Durch die Umsetzung unserer Empfehlungen konnte das Unternehmen nicht nur die Sicherheitslücke schließen, sondern auch die gesamte IoT-Infrastruktur erheblich stärken. Dies führte zu einer erhöhten Betriebssicherheit und einem gesteigerten Vertrauen der Stakeholder in die Innovationskraft und Sicherheitskompetenz des Unternehmens. Die Geschäftsführung war von den Ergebnissen beeindruckt und entschied sich, unsere Expertise weiterhin zu nutzen, um zukünftige technologische Erweiterungen sicher zu gestalten.

SCHLUSSFOLGERUNG

Ein Penetration-Test nach BSI-Standard ist ein unverzichtbares Instrument, um die Sicherheitsmaßnahmen eines Unternehmens zu überprüfen und zu verbessern. Durch die enge Zusammenarbeit zwischen mir, Georg Schneider, und Benjamin Richter können wir unseren Kunden umfassende und praxisnahe Lösungen bieten, die ihre Sicherheitslage nachhaltig stärken. Unsere Fallstudien zeigen, wie wichtig es ist, regelmäßig die eigene IT-Infrastruktur auf Schwachstellen zu überprüfen und entsprechende Maßnahmen zu ergreifen.

WARUM ES SINNVOLL SEIN KANN, ÜBER DEN BSI-STANDARD HINAUSZUGEHEN

Als IT-Leiter bei Cyber Complete sehe ich täglich, wie dynamisch und komplex die Bedrohungslandschaft im Bereich der Cybersicherheit ist. Während der BSI-Standard eine solide Grundlage bietet, gibt es mehrere Gründe, warum es sinnvoll sein kann, über diese Mindestanforderungen hinauszugehen:

PROAKTIVE RISIKOERKENNUNG

Ein Penetrationstest, der über herkömmliche Sicherheitsmaßnahmen hinausgeht, ermöglicht eine tiefere Analyse der IT-Infrastruktur. Solche Tests decken Schwachstellen auf, die in regulären Sicherheitsüberprüfungen oft unentdeckt bleiben. Benjamin Richter betont, dass diese proaktive Herangehensweise entscheidend ist, um potenzielle Risiken frühzeitig zu erkennen und zu beheben.

ABDECKUNG WEITERER STANDARDS

Neben dem BSI-Standard gibt es andere wichtige Sicherheitsstandards wie die DSGVO, ISO 27001, DORA und TIBER-EU. Diese Standards erfordern nicht nur die Implementierung von Sicherheitsmaßnahmen, sondern auch deren regelmäßige Wirksamkeitsprüfung. Penetrationstests sind unerlässlich, um sicherzustellen, dass die Maßnahmen den Anforderungen dieser Standards entsprechen und effektiv sind.

ANPASSUNG AN REALE BEDROHUNGEN

Die Methoden von Angreifern entwickeln sich ständig weiter. Ein Penetrationstest, der über den BSI-Standard hinausgeht, kann helfen, den aktuellen und zukünftigen Bedrohungen einen Schritt voraus zu sein. Benjamin Richter und ich simulieren realistische Angriffsszenarien, damit Unternehmen ihre Abwehrmechanismen kontinuierlich anpassen und verbessern können.

UMFASSENDE PRÜFUNGSBEREICHE

Fortgeschrittene Penetrationstests bieten die Möglichkeit, spezifische Schnittstellen zu untersuchen, die nicht im Fokus des BSI-Standards stehen. Dazu gehören beispielsweise physische Aspekte der IT-Sicherheit oder spezifische Anwendungen und Schnittstellen, die für das Unternehmen von besonderer Bedeutung sind.

VERMEIDUNG VON BETRIEBSBLINDHEIT

Das BSI selbst empfiehlt, externe Prüfer einzusetzen, um Interessenskonflikte und die sogenannte „Betriebsblindheit“ zu vermeiden. Externe Experten bringen frische Perspektiven und unabhängige Bewertungen ein, die entscheidend sein können, um verborgene Schwachstellen zu identifizieren.

ZUSAMMENFASSEND

Ein BSI-konformer Penetrationstest ist ein guter erster Schritt, um die grundlegende Sicherheit eines Unternehmens zu gewährleisten. Für eine effektive Cybersicherheitsstrategie ist es jedoch entscheidend, den Testprozess kontinuierlich weiterzuentwickeln und gegebenenfalls über die Mindestanforderungen des BSI hinauszuwachsen. Gemeinsam mit Benjamin Richter und dem Team von Cyber Complete arbeiten wir daran, unseren Kunden umfassenden Schutz zu bieten, der den sich ständig verändernden Bedrohungen gerecht wird. —

WIR SIMULIEREN ANGRIFFE WIE ECHE HACKER - ABER MIT DEM ZIEL, SCHWACHSTELLEN ZU SCHLIESSEN, BEVOR ANDERE SIE AUSNUTZEN.

Werden Ihre Daten bereits im Darknet gehandelt?



Darknet Monitoring mit **deep web • check**

Deepwebcheck überwacht Foren, Marktplätze und schwer zugängliche Quellen im Darknet in Echtzeit. Kombiniert mit Analysten-Know-how entstehen präzise Hinweise auf Datenleaks, geplante Angriffe und Betrugsversuche. Unternehmen gewinnen Frühwarnzeit, schützen sensible Informationen und schärfen ihre Sicherheitsstrategie.

DARKNET MONITORING MIT DEEPWEBCHECK:

In meiner Rolle als führender Experte bei Cyber Complete habe ich die Möglichkeit, an vorderster Front der Cybersicherheitslandschaft zu arbeiten. Eine der fortschrittlichsten Lösungen, die wir entwickelt haben, ist Deepwebcheck, unsere Plattform für Darknet Monitoring. In diesem Artikel möchte ich tiefere Einblicke in die Funktionsweise dieser Plattform geben und erläutern, welche entscheidenden Vorteile sie Unternehmen bietet.

WAS STECKT HINTER DER PLATTFORM DEEPWEBCHECK?

Deepwebcheck ist mehr als nur ein Tool – es ist ein integraler Bestandteil einer umfassenden Sicherheitsstrategie. Die Plattform wurde entwickelt, um das Darknet und andere schwer zugängliche Bereiche des Internets systematisch zu überwachen. Mit Hilfe fortschrittlicher Algorithmen und maschinellen Lernens durchsucht Deepwebcheck kontinuierlich Foren, Marktplätze und andere Darknet-Quellen nach potenziellen Bedrohungen.

Unsere Technologie ist darauf ausgelegt, verdächtige Aktivitäten zu identifizieren, die auf gestohlene Daten, geplante Angriffe oder andere Sicherheitsrisiken hinweisen. Durch die Kombination automatisierter Prozesse mit der Expertise unseres Teams können wir unseren Kunden Echtzeit-Informationen und präzise Analysen bereitstellen. Dies ermöglicht es uns, nicht nur auf Bedrohungen zu reagieren, sondern ihnen einen Schritt voraus zu sein.

VORTEILE FÜR UNTERNEHMEN DURCH DEN EINSATZ VON DEEPWEBCHECK

FRÜHZEITIGE ERKENNUNG VON BEDROHUNGEN

Einer der größten Vorteile, die ich bei der Implementierung von Deepwebcheck beobachtet habe, ist die Fähigkeit zur frühzeitigen Erkennung von Bedrohungen. Unternehmen können proaktiv auf Sicherheitsrisiken reagieren, bevor sie zu ernsthaften Problemen werden. Diese proaktive Herangehensweise ermöglicht eine schnellere Reaktion und minimiert potenzielle Schäden erheblich.

SCHUTZ SENSIBLER DATEN

Durch die Überwachung des Darknets können wir Hinweise auf gestohlene oder kompromittierte Daten identifizieren. Unternehmen erhalten sofortige Benachrichtigungen, wenn ihre Informationen im Darknet auftauchen, was ihnen ermöglicht, schnell Gegenmaßnahmen zu ergreifen. Diese Fähigkeit, schnell zu handeln, ist entscheidend, um den Schaden zu begrenzen und das Vertrauen der Kunden zu bewahren.

ERWEITERTE SICHERHEITSANALYSEN

Deepwebcheck bietet umfassende Berichte und Analysen, die Unternehmen helfen, ihre Sicherheitsstrategien kontinuierlich zu verbessern. Diese Einblicke sind entscheidend, um die Effektivität bestehender Sicherheitsmaßnahmen zu bewerten und anzupassen. In meiner Erfahrung haben Unternehmen, die diese Analysen nutzen, signifikante Verbesserungen in ihrer Sicherheitslage erzielt. →

CASE STUDIES

FINANZINSTITUT SCHÜTZT KUNDENDATEN

In einem besonders eindrucksvollen Fall arbeitete ich mit einem großen Finanzinstitut zusammen, das Deepwebcheck einsetzte, um seine Kundendaten zu schützen. Während unserer Überwachung entdeckten wir Hinweise auf eine geplante Veröffentlichung sensibler Kundendaten auf einem Darknet-Marktplatz. Diese Entdeckung war von entscheidender Bedeutung, da sie uns ermöglichte, das Institut sofort zu alarmieren. In enger Zusammenarbeit mit ihrem internen Sicherheitsteam konnten wir die betroffenen Daten schnell sichern und den potenziellen Schaden minimieren. Diese proaktive Reaktion bewahrte das Institut vor erheblichen finanziellen Verlusten und Reputationsschäden.

TECHNOLOGIEUNTERNEHMEN VERHINDERT INDUSTRIESPIONAGE

Ein weiteres Beispiel, das die Leistungsfähigkeit von Deepwebcheck unterstreicht, ist unsere Zusammenarbeit mit einem führenden Technologieunternehmen. Das Unternehmen beauftragte uns mit der Überwachung des Darknets, um Hinweise auf Industriespionage zu identifizieren. Unsere Plattform entdeckte verdächtige Aktivitäten, die auf den Verkauf von gestohlenen Prototypen und Forschungsdaten hindeuteten. Durch unsere detaillierten Analysen konnten wir die Sicherheitslücke schnell schließen und die Täter identifizieren. Diese Maßnahmen verhinderten nicht nur den Verlust wertvoller geistiger Eigentumsrechte, sondern schützten auch die Wettbewerbsfähigkeit des Unternehmens.

SCHLUSSFOLGERUNG

Deepwebcheck ist ein unverzichtbares Tool für Unternehmen, die ihre Sicherheitsstrategie auf das nächste Level heben möchten. Durch die kontinuierliche Überwachung des Darknets und die Bereitstellung präziser Analysen können Unternehmen Bedrohungen frühzeitig erkennen und effektiv darauf reagieren.

Da Cyberbedrohungen ständig zunehmen, bietet Deepwebcheck den entscheidenden Vorteil, um sensible Daten zu schützen und das Vertrauen der Kunden zu stärken. Als Teil von Cyber Complete bin ich stolz darauf, Unternehmen dabei zu unterstützen, sich in dieser komplexen Landschaft zu behaupten und ihre Sicherheitsmaßnahmen kontinuierlich zu verbessern. —

DEEPWEBCHECK DURCHSUCHT KONTINUIERLICH DARKNET-FOREN UND MARKTPLÄTZE UND MELDET POTENZIELLE RISIKEN IN ECHTZEIT.

Keine
Cyber Security
ohne gute IT

Keine
gute IT
ohne dass alle sie
verstehen



- der IT-Slam

Unterhaltsam.
Direkt.
Anders.

Die besten Slams aus IT,
Digitalisierung, KI und Cyber Security.
Für ITler und normale Menschen.

Nächste Termine:
Hamburg 19.11.25, Berlin 12.03.26

Tickets unter dslam.info



youtube.com/@dslam-event



Machen sie EU AI ACT & ISO 42001 zu Ihrem Wettbewerbsvorteil

**VOM KI-MANAGEMENT BIS ZU RISIKOKLASSEN:
SO WERDEN REGELN UND TRANSPARENZ ZU
GREIFBAREN VORTEILEN.**

ISO 42001 definiert, wie KI verantwortungsvoll betrieben wird; der **EU AI Act** macht daraus verbindliche Anforderungen. Wer früh auf klare Rollen, nachvollziehbare Modelle und belastbare Kontrollen setzt, senkt Risiken, beschleunigt Audits und stärkt Vertrauen.

Der Bericht zeigt, wie Organisationen Compliance-by-Design etablieren – von Daten- und Modell-Governance bis zu kontinuierlichem Monitoring in kritischen Use Cases.

ISO 42001 & EU AI ACT: ÜBERBLICK UND BEDEUTUNG

Mit jahrelanger Expertise stehen mein Expertenteam und ich bei Cyber Complete an der Spitze der Entwicklungen im Bereich Cybersicherheit und IT-Compliance, wobei wir neue Standards und Regulierungen kontinuierlich im Blick behalten. Zwei der aktuell bedeutendsten Entwicklungen in diesem Bereich sind die ISO 42001 und der EU AI Act. Diese setzen neue Maßstäbe für den Umgang mit Künstlicher Intelligenz (KI) und deren Integration in Unternehmensprozesse. In diesem Bericht möchte ich meine Erfahrungen teilen und erläutern, wie ich Unternehmen dabei geholfen habe,

diese Herausforderungen zu meistern.

Was verlangt die neue Norm ISO 42001?

Die ISO 42001 ist eine internationale Norm, die sich mit der verantwortungsvollen Entwicklung und dem Einsatz von KI-Systemen befasst. Sie legt klare Anforderungen an die Transparenz, Fairness und

Nachvollziehbarkeit von KI-Anwendungen fest. In meiner Arbeit habe ich gesehen, wie wichtig es ist, diese Prinzipien in die Praxis umzusetzen, um das Vertrauen der Kunden zu gewinnen und regulatorische Risiken zu minimieren.

ERFAHRUNG MIT DER UMSETZUNG

Ein besonders prägendes Projekt in meiner Laufbahn war die Zusammenarbeit mit einem führenden Einzelhandelsunternehmen, das Künstliche Intelligenz zur Optimierung seiner Lieferketten für Konsumgüter und Elektronik einsetzte. Die Herausforderung bestand darin, die Transparenz der eingesetzten KI-Algorithmen zu erhöhen, um sowohl interne als auch externe Anforderungen zu erfüllen, insbesondere die der ISO 42001.

OPTIMIERUNG DER LIEFERKETTEN

Das Unternehmen hatte komplexe Lieferketten, die von der Beschaffung der Rohstoffe bis zur Auslieferung der Endprodukte an die Einzelhandelsgeschäfte reichten. Die KI wurde eingesetzt, um Lagerbestände zu verwalten, Nachfrageprognosen zu erstellen und den Transport effizienter zu gestalten. Durch die Implementierung erklärbarer KI-Modelle konnten wir die Entscheidungsprozesse der KI nachvollziehbar machen.

ERKLÄRBARE KI-MODELLE

sind darauf ausgelegt, die Entscheidungsfindung von KI-Systemen transparent und verständlich zu machen. In diesem Projekt bedeutete das, dass wir Algorithmen entwickelten, die ihre Entscheidungen anhand von nachvollziehbaren Kriterien und Datenquellen erklärten. Beispielsweise konnte das System bei Bestandsentscheidungen die zugrunde liegenden Daten wie Verkaufsprognosen, historische Verkaufsdaten und saisonale Trends offenlegen.

ISO 42001 IST DAS BETRIEBSSYSTEM FÜR KI-GOVERNANCE – DER EU AI ACT IST DIE REGULIERUNG, DIE SIE EINFORDERT.

INTEGRATION VON FEEDBACK-SCHLEIFEN

Ein entscheidender Aspekt war die Integration von Feedback-Schleifen in die KI-Modelle. Diese ermöglichten es den Mitarbeitern, die Entscheidungen der KI zu hinterfragen und bei Bedarf manuell einzugreifen. Dies wurde durch ein benutzerfreundliches Dashboard realisiert, das den Mitarbeitern Einblicke in die Entscheidungsprozesse der KI gab und ihnen die Möglichkeit bot, Anpassungen vorzunehmen. Diese Interaktivität führte zu einer signifikanten Steigerung des Vertrauens in die Technologie und ermöglichte es dem Unternehmen, die Anforderungen der ISO 42001 hinsichtlich Transparenz und Nachvollziehbarkeit zu erfüllen.

VERBESSERUNG INTERNER PROZESSE

Die Optimierung der Lieferketten führte zu erheblichen Verbesserungen in mehreren internen Prozessen. Zum Beispiel wurde die Bestandsverwaltung effizienter gestaltet, indem Überbestände reduziert und Engpässe vermieden wurden. Die Nachfrageprognosen wurden präziser, was zu einer besseren Planung der Produktionskapazitäten führte. Zudem wurden die Transportwege optimiert, indem Routen dynamisch angepasst wurden, um Lieferzeiten zu verkürzen und Transportkosten zu senken.

MASSNAHMEN

Durch diese Maßnahmen konnte das Unternehmen nicht nur die Effizienz seiner Lieferketten steigern, sondern auch die Kundenzufriedenheit erhöhen, da Produkte schneller und zuverlässiger verfügbar waren. Dieses Projekt zeigte eindrucksvoll, wie die Implementierung von ISO-konformen KI-Systemen nicht nur regulatorische Anforderungen erfüllt, sondern auch einen direkten wirtschaftlichen Nutzen bringt.

WELCHE VERÄNDERUNGEN BRINGT DER EU AI ACT MIT SICH?

Es ist ein umfassender gesetzlicher Rahmen, der darauf abzielt, KI-Anwendungen nach ihrem Risiko zu kategorisieren und spezifische Anforderungen für jede Kategorie festzulegen. Diese Regelung stellt sicher, dass Hochrisiko-Anwendungen strengen Kontrollen unterliegen.

VERBINDUNGEN ZUM DATENSCHUTZ

Ein zentraler Aspekt sowohl der ISO 42001 als auch des EU AI Act ist der Datenschutz, insbesondere bei hochkritischen KI-Anwendungen. Diese Regelungen stellen sicher, dass der Einsatz von KI die Datenschutzrechte der betroffenen Personen respektiert.

SCHLUSSFOLGERUNG

Die Einführung der ISO 42001 und des EU AI Act markiert einen bedeutenden Schritt in Richtung einer verantwortungsvollen und sicheren Nutzung von KI-Technologien. Als Teil von Cyber Complete sehe ich es als meine Aufgabe, Unternehmen dabei zu unterstützen, diese neuen Anforderungen zu verstehen und umzusetzen. Durch die Einhaltung dieser Standards können Unternehmen nicht nur rechtliche Risiken minimieren, sondern auch das Vertrauen ihrer Kunden stärken und ihre Innovationskraft verantwortungsvoll nutzen. Meine Erfahrungen haben gezeigt, dass mit der richtigen Strategie und den passenden Technologien diese Herausforderungen erfolgreich gemeistert werden können. —



Digital.
Weiter.
Denken.



ISO/IEC 42001 & EU AI Act –

praxisnah für den Mittelstand

Von Governance bis Digitalisierung: Wir machen Ihre KI sicher, regelkonform und alltagstauglich.

KI-Strategie



- Analyse
- Roadmap
- Umsetzung

Compliance & Governance



- ISO/IEC 42001
- EU AI Act
- Risikomanagement

Individuelle Digitalisierung



- Prozessorientiert
- Branchenfokussiert
- Nachhaltig

KI & Compliance

Der EU AI Act und die ISO/IEC 42001 setzen klare Leitplanken für verantwortungsvollen KI-Einsatz. Wir übersetzen diese Anforderungen in konkrete Schritte:

- **KI-Managementsystem (ISO/IEC 42001)**
- **Risikoklassifizierung & Nachweise (EU AI Act)**
- **Transparenz- & Aufsichtspflichten**

So gewinnen Sie Vertrauen, reduzieren Risiken und nutzen KI schneller und wirksamer als Ihre Mitbewerber.

Digitalisierung

KI wirkt nur auf stabilen Prozessen. Darum entwickeln wir **maßgeschneiderte Lösungen**, die Prozesse vereinfachen, Transparenz schaffen und **Mitarbeitende entlasten**: mit modernen **Low- und No-Code-Ansätzen**, offen, wartbar und **branchenspezifisch**.

Raphael Becker
TÜV Rheinland zertifizierter ISO 42001 Professional & KI-Compliance-Beauftragter

bepro solutions GmbH
Oststraße 27 | 57392 Schmallenberg
info@bepro-solutions.de | +49 (0) 2972 963 96 90

**JETZT
BERATUNGSGESPRÄCH
ANFRAGEN –
QR-CODE SCANNEN**





Die DATENSCHUTZ-GRUNDVERORDNUNG

ist mehr als ein Bußgeld-Risiko

So nutzen Sie DSGVO zum strategischen Vorteil

DSGVO VERSTEHEN: LEITFADEN FÜR UNTERNEHMEN

Bei Cyber Complete habe ich mit meinem Team zahlreiche Unternehmen dabei unterstützt, die Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu verstehen und erfolgreich umzusetzen. Die DSGVO ist ein umfassendes Regelwerk, das den Schutz personenbezogener Daten innerhalb der EU sicherstellen soll. In diesem Artikel möchte ich die Struktur, Ziele und Auswirkungen der DSGVO erläutern und aufzeigen, wie Unternehmen sie effektiv anwenden können.

AUFBAU DER DSGVO

Die DSGVO ist in elf Kapitel unterteilt und umfasst insgesamt 99 Artikel. Diese Struktur bietet einen detaillierten Rahmen für den Umgang mit personenbezogenen Daten. Die wichtigsten Kapitel umfassen:

- **Grundsätze:** Artikel 5 beschreibt die Grundsätze der Datenverarbeitung, wie Rechtmäßigkeit, Transparenz und Zweckbindung.
- **Rechte der betroffenen Personen:** Artikel 12 bis 23 legen die Rechte der Personen fest, deren Daten verarbeitet werden, einschließlich des Rechts auf Auskunft, Berichtigung und Löschung.
- **Verantwortlichkeiten der Verantwortlichen:** Artikel 24 bis 43 definieren die Pflichten der Datenverantwortlichen, einschließlich der Notwendigkeit von Datenschutz-Folgenabschätzungen und der Benennung eines Datenschutzbeauftragten.
- **Übermittlung personenbezogener Daten:** Artikel 44 bis 50 regeln die Übermittlung von Daten außerhalb der EU.
- **Rechtsbehelfe, Haftung und Sanktionen:** Artikel 77 bis 84 behandeln die Durchsetzung der DSGVO, einschließlich der Bußgelder.

ZIELE DER DSGVO

Die DSGVO verfolgt mehrere zentrale Ziele:

- **Stärkung der Rechte der Einzelpersonen:** Die Verordnung gibt den Bürgern mehr Kontrolle über ihre persönlichen Daten und stärkt ihre Rechte.
- **Harmonisierung des Datenschutzrechts:** Sie sorgt für ein einheitliches Datenschutzniveau in der gesamten EU, was den grenzüberschreitenden Datenverkehr erleichtert.
- **Erhöhung der Rechenschaftspflicht:** Unternehmen werden verpflichtet, ihre Datenverarbeitungspraktiken zu dokumentieren und nachzuweisen, dass sie die Vorschriften einhalten.

BUSSGELDER UND SANKTIONEN

Eines der bekanntesten Merkmale der DSGVO sind die strengen Bußgelder bei Verstößen. Diese können bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens betragen, je nachdem, welcher Betrag höher ist. Diese Sanktionen unterstreichen die Bedeutung der Einhaltung der DSGVO und motivieren Unternehmen, ihre Datenschutzpraktiken zu überprüfen und zu verbessern.

UMSETZUNG DER DSGVO IN UNTERNEHMEN

- **Datenschutz-Folgenabschätzung (DSFA):** Unternehmen sollten eine DSFA durchführen, um die Risiken ihrer Datenverarbeitung zu bewerten und geeignete Maßnahmen zur Minderung dieser Risiken zu ergreifen.
- **Benennung eines Datenschutzbeauftragten (DSB):** In vielen Fällen ist die Benennung eines DSB erforderlich, um die Einhaltung der DSGVO zu überwachen und als Ansprechpartner für Datenschutzfragen zu dienen.
- **Transparente Datenschutzerklärungen:** Unternehmen müssen klare und verständliche Datenschutzerklärungen bereitstellen, die den Umfang und Zweck der Datenverarbeitung erläutern.
- **Einwilligung und Rechte der Betroffenen:** Unternehmen müssen sicherstellen, dass sie die Einwilligung der betroffenen Personen einholen und deren Rechte respektieren, einschließlich des Rechts auf Auskunft und Löschung.

SCHLUSSFOLGERUNG

Die DSGVO stellt Unternehmen vor Herausforderungen, bietet aber auch die Chance zur Modernisierung ihrer Datenschutzpraktiken. In meiner Rolle bei Cyber Complete unterstütze ich Unternehmen dabei, die DSGVO als strategischen Vorteil zu nutzen. Ich helfe ihnen, rechtliche Risiken zu minimieren und ihre Wettbewerbsfähigkeit zu steigern, indem wir gemeinsam Datenschutzstrategien entwickeln, die Vertrauen schaffen und Prozesse optimieren. Diese Arbeit zeigt mir, dass die DSGVO mehr als nur eine Verpflichtung ist – sie ist eine Chance, die Zukunftsfähigkeit eines Unternehmens zu sichern. —

**RECHTS-
GRUNDLAGE
ZUERST – DATEN-
VERARBEITUNG
DANACH."**

Pretty Easy DSGVO IN DER PRAXIS

Ein Leitfaden für Unternehmen

Typische Stolpersteine

Bei der Umsetzung der DSGVO stoßen Unternehmen häufig auf folgende Herausforderungen:

UNKLARE DATENVERARBEITUNGSPROZESSE:
Viele Unternehmen haben Schwierigkeiten, alle Datenverarbeitungsprozesse vollständig zu dokumentieren.

FEHLENDE EINWILLIGUNGEN:
Oft fehlen klare Einwilligungen der betroffenen Personen, was zu rechtlichen Risiken führen kann.

UNZUREICHENDE TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN:
Der Schutz personenbezogener Daten erfordert sowohl technische als auch organisatorische Maßnahmen, die häufig unzureichend umgesetzt werden.

UNVOLLSTÄNDIGE SCHULUNG:
Mitarbeiter sind oft nicht ausreichend über die Anforderungen und Bedeutung der DSGVO informiert.

Umsetzungsschritte

Um die DSGVO erfolgreich umzusetzen, sollten Unternehmen folgende Schritte beachten:

DATENINVENTAR ERSTELLEN:
Identifizieren Sie alle personenbezogenen Daten, die Ihr Unternehmen verarbeitet, und dokumentieren Sie die entsprechenden Prozesse.

RISIKOBEWERTUNG UND DSFA:
Führen Sie eine Datenschutz-Folgenabschätzung (DSFA) durch, um Risiken zu identifizieren und geeignete Maßnahmen zur Risikominderung zu ergreifen.

EINWILLIGUNGEN EINHOLEN:
Stellen Sie sicher, dass Sie die Einwilligung der betroffenen Personen



für die Verarbeitung ihrer Daten haben und dass diese Einwilligungen dokumentiert sind.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN:
Implementieren Sie angemessene Sicherheitsmaßnahmen, um personenbezogene Daten zu schützen, und aktualisieren Sie diese regelmäßig.

SCHULUNGEN DURCHFÜHREN:
Schulen Sie Ihre Mitarbeiter regelmäßig in den Anforderungen der DSGVO und der Bedeutung des Datenschutzes.

Best Practices

TRANSPARENTE KOMMUNIKATION:
Informieren Sie Kunden und Partner klar und verständlich über die Verarbeitung ihrer Daten.

REGELMÄSSIGE AUDITS:
Führen Sie regelmäßige Audits durch, um die Einhaltung der DSGVO sicherzustellen und Schwachstellen zu identifizieren.

DATENSCHUTZ DURCH TECHNIKGESTALTUNG:
Integrieren Sie Datenschutz in die Entwicklung neuer Produkte und Prozesse („Privacy by Design“).

Rolle des Datenschutzbeauftragten

Der Datenschutzbeauftragte (DSB) spielt eine zentrale Rolle bei der Umsetzung der DSGVO:

BERATUNG UND SCHULUNG:
Der DSB berät das Unternehmen in allen Fragen des Datenschutzes und schult die Mitarbeiter.

ÜBERWACHUNG DER EINHALTUNG:
Er überwacht die Einhaltung der DSGVO und anderer Datenschutzvorschriften.

ANSPRECHPARTNER FÜR BETROFFENE:
Der DSB dient als Ansprechpartner für betroffene Personen und die Aufsichtsbehörden.

RISIKOBEWERTUNG:
Er unterstützt bei der Durchführung von Datenschutz-Folgenabschätzungen und der Bewertung von Risiken.

Schlussfolgerung

Die Umsetzung der DSGVO in der Praxis erfordert sorgfältige Planung und kontinuierliche Anpassung. Durch die Vermeidung typischer Stolpersteine, die Umsetzung bewährter Praktiken und die Einbindung eines kompetenten Datenschutzbeauftragten können Unternehmen nicht nur rechtliche Risiken minimieren, sondern auch das Vertrauen ihrer Kunden stärken und Datenschutz als Wettbewerbsvorteil nutzen. In meiner Arbeit bei Cyber Complete habe ich gesehen, wie Unternehmen durch eine strategische Herangehensweise an die DSGVO ihre Prozesse optimieren und gleichzeitig ihre Marktposition stärken können. ____

WER ZWECKE KLAR DEFINIERT, BRAUCHT SELTENER EINWILLIGUNGEN.

DSGVO in der Praxis

Die erfolgreiche Umsetzung der DSGVO in Unternehmen verschiedener Branchen gehört zu den Kernkompetenzen, die mein Team und ich bei Cyber Complete entwickelt haben. Die DSGVO ist nicht nur ein rechtlicher Rahmen, sondern auch eine Chance, Datenschutz als Wettbewerbsvorteil zu nutzen. In diesem Artikel möchte ich typische Stolpersteine, wesentliche Umsetzungsschritte, Best Practices und die Rolle des Datenschutzbeauftragten (DSB) erläutern.

DER STRATEGISCHE FAHRPLAN

Cleverer
Integration
von DSGVO,
NIS2 und
ISO 27001



I

TEGRATION VON DSGVO, NIS2 & ISO 27001

Eine effiziente Verzahnung von DSGVO, NIS2 und ISO 27001 in Unternehmensstrukturen steht im Mittelpunkt meiner Projekte, die ich mit meinem spezialisierten Team bei Cyber Complete durchführe. Diese drei Regelwerke bieten einen umfassenden Rahmen für Datenschutz und Informationssicherheit, doch ihre gleichzeitige Umsetzung kann Herausforderungen mit sich bringen. In diesem Artikel beleuchte ich die Synergien und Konflikte, die sich aus der Integration dieser Standards ergeben, und zeige auf, wie integrierte Managementsysteme Effizienz schaffen können.

SYNERGIEN UND KONFLIKTE

SYNERGIEN

- **Ganzheitlicher Sicherheitsansatz:** Die Integration von DSGVO, NIS2 und ISO 27001 ermöglicht einen umfassenden Ansatz für Datenschutz und Informationssicherheit. Während die DSGVO den Schutz personenbezogener Daten fokussiert, adressiert ISO 27001 die allgemeine Informationssicherheit und NIS2 die Netz- und Informationssicherheit kritischer Infrastrukturen.
- **Effizienz durch gemeinsame Prozesse:** Durch die Harmonisierung von Prozessen und Kontrollen können Unternehmen redundante Maßnahmen vermeiden und Ressourcen effizienter nutzen.

KONFLIKTE

- **Unterschiedliche Schwerpunkte:** Während die DSGVO primär auf den Schutz personenbezogener Daten abzielt, liegt der Fokus von ISO 27001 auf der allgemeinen Informationssicherheit und von NIS2 auf der Netzwerksicherheit. Diese unterschiedlichen Schwerpunkte können zu Konflikten bei der Priorisierung von Maßnahmen führen.
- **Komplexität der Umsetzung:** Die gleichzeitige Umsetzung mehrerer Regelwerke kann zu einer erhöhten Komplexität führen, insbesondere wenn unterschiedliche Abteilungen involviert sind.

EFFIZIENZ DURCH INTEGRIERTE MANAGEMENTSYSTEME

Integrierte Managementsysteme (IMS) bieten eine Lösung zur Bewältigung der Komplexität bei der Umsetzung mehrerer Regelwerke. Sie ermöglichen es Unternehmen, Prozesse zu harmonisieren, Verantwortlichkeiten klar zu definieren und die Einhaltung der verschiedenen Standards effizient zu überwachen.

BEST PRACTICES

- **Zentralisierte Governance-Struktur:** Eine zentrale Governance-Struktur erleichtert die Koordination zwischen den verschiedenen Regelwerken und Abteilungen. Dies fördert eine einheitliche Strategie und reduziert die Gefahr von Überschneidungen und Konflikten.

- **Risikobasierter Ansatz:** Ein risikobasierter Ansatz ermöglicht es Unternehmen, Prioritäten zu setzen und Ressourcen gezielt einzusetzen. Dies ist besonders wichtig, um die Anforderungen der verschiedenen Standards effektiv zu erfüllen.
- **Regelmäßige Schulungen:** Kontinuierliche Schulungen für Mitarbeiter stellen sicher, dass alle Beteiligten die Anforderungen und Ziele der integrierten Standards verstehen und umsetzen können.

CASE STUDY: INTEGRATION IM GESUNDHEITSWESEN

Ein großes Krankenhausnetzwerk, das in mehreren Regionen tätig ist, stand vor der Herausforderung, die Anforderungen der DSGVO, NIS2 und ISO 27001 zu integrieren, um den Schutz sensibler Patientendaten zu gewährleisten. In meiner Rolle als Berater bei Cyber Complete übernahm ich die Leitung dieses komplexen Projekts.

PROJEKTUMSETZUNG

1. INITIALE ANALYSE UND PLANUNG

- **Bestandsaufnahme der Datenverarbeitung:** Zunächst führten wir eine umfassende Bestandsaufnahme aller Datenverarbeitungsprozesse durch. Dies umfasste die Identifikation aller Systeme, die personenbezogene Daten verarbeiten, sowie die Bewertung der bestehenden Sicherheitsmaßnahmen.
- **Stakeholder-Engagement:** Wir etablierten ein interdisziplinäres Team, bestehend aus IT-Spezialisten, Datenschutzexperten, Klinikpersonal und der Geschäftsführung, um sicherzustellen, dass alle relevanten Perspektiven berücksichtigt werden.

2. RISIKOMANAGEMENT UND DSFA

- **Durchführung einer Datenschutz-Folgenabschätzung (DSFA):** Wir identifizierten kritische Risiken in der Datenverarbeitung, insbesondere im Hinblick auf die elektronische Patientenakte und die Kommunikation mit externen Partnern.
- **Entwicklung eines risikobasier-ten Maßnahmenplans:** Basierend auf den Ergebnissen der DSFA entwickelten wir einen Maßnahmenplan, der technische, organisatorische und prozessuale Anpassungen umfasste.

3. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

- **Implementierung von Verschlüsselungstechnologien:** Wir führten fortschrittliche Verschlüsselungstechnologien ein, um die Vertraulichkeit und Integrität sensibler Daten zu gewährleisten. Dies umfasste sowohl die Datenübertragung als auch die Datenspeicherung.
- **Zugriffsmanagement und Authentifizierung:** Ein mehrstufiges Authentifizierungssystem wurde eingeführt, um sicherzustellen, dass nur autorisierte Mitarbeiter Zugriff auf sensible Daten haben. Dies wurde ergänzt durch regelmäßige Überprüfungen der Zugriffsrechte.
- **Netzwerksicherheit und NIS2-Konformität:** Durch regelmäßige Penetrationstests und die Implementierung von Intrusion Detection Systemen (IDS) stellten wir sicher, dass die Netzwerksicherheit den Anforderungen von NIS2 entspricht. →

4. ZENTRALISIERTE GOVERNANCE UND SCHULUNG

- **Etablierung einer zentralen Governance-Struktur:** Wir benannten einen Datenschutzbeauftragten und einen Informationssicherheitsbeauftragten, die gemeinsam für die Überwachung der Compliance verantwortlich waren. Diese Struktur ermöglichte eine klare Verantwortungszuweisung und eine effiziente Koordination der Maßnahmen.

- **Mitarberschulungen:** Regelmäßige Schulungen wurden durchgeführt, um das Bewusstsein der Mitarbeiter für Datenschutz und Informationssicherheit zu schärfen. Dies umfasste sowohl allgemeine Schulungen als auch spezifische Workshops für IT-Personal und Klinikmitarbeiter.

ERGEBNISSE

- **Verbesserte Sicherheitsarchitektur:** Durch die Integration der Regelwerke konnte das Krankenhausnetzwerk seine IT-Infrastruktur erheblich absichern. Die Einführung fortschrittlicher Technologien und Prozesse führte zu einer signifikanten Reduzierung von Sicherheitsvorfällen.
- **Stärkung des Vertrauens:** Die transparente Kommunikation der Datenschutzmaßnahmen gegenüber Patienten und Partnern stärkte das Vertrauen in die Organisation. Dies führte zu einer positiven Wahrnehmung und einer stärkeren Bindung der Patienten an das Netzwerk.
- **Effizienzsteigerung:** Die zentrale Governance-Struktur und der risikobasierte Ansatz führten zu einer Reduzierung des Audit-Aufwands und einer gesteigerten Effizienz im Betrieb. Die Harmonisierung der Prozesse ermöglichte es, die Compliance-Kosten deutlich zu senken.

Diese Case Study zeigt, wie ich durch die strategische Integration von DSGVO, NIS2 und ISO 27001 Unternehmen dabei unterstützen kann, nicht nur die Einhaltung gesetzlicher Anforderungen sicherzustellen, sondern auch ihre Sicherheitsarchitektur zu optimieren und ihre Marktposition zu stärken.

SCHLUSSFOLGERUNG

Die Integration von DSGVO, NIS2 und ISO 27001 bietet Unternehmen die Möglichkeit, Datenschutz und Informationssicherheit ganzheitlich zu betrachten. Durch die Nutzung von Synergien und die Überwindung potenzieller Konflikte können Unternehmen nicht nur die Einhaltung gesetzlicher Anforderungen sicherstellen, sondern auch ihre Effizienz steigern und das Vertrauen ihrer Kunden stärken. In meiner Arbeit bei Cyber Complete habe ich gesehen, wie Unternehmen durch die strategische Integration dieser Standards ihre Sicherheitsarchitektur optimieren und ihre Marktposition erheblich stärken können. —

ISO LIEFERT DAS BETRIEBS-SYSTEM, DSGVO UND NIS2 DIE PFLICHTEN.



Rohländer Beteiligungen

Wir sind der Mehrwert-Partner für Startups und Unternehmen und agieren als „Strategische Denker“ & „Ergebnis-Gestalter“!

- Startup-Founding & -Management
- Kapitalbeschaffung
- Zugang zu Premium-Vermögensverwaltungen
- Stiftungen: Gründung, Verwaltung & Strategie
- Diskrete Begleitung bei Unternehmensnachfolge
- Unternehmensübernahmen & -beteiligungen
- Resilienz-Management

MARTIN ROHLÄNDER BETEILIGUNGEN

Rohländer Beteiligungen
Martin Rohländer
+49 176 - 23 20 98 29

mr@nutz-mein-netzwerk.jetzt
www.nutz-mein-netzwerk.jetzt

CYBER- SICHER- HEIT IN DER AUTO- MOBIL INDU- STRIE



CSMS – CYBER SECURITY MANAGEMENT SYSTEM:

Neue
Anforderungen
für OEMs
durch die
ISO 21434
Richtlinie

Vernetzte Autos brauchen Schutz: ISO 21434 gibt die Regeln, CSMS ist der Plan – wie Hersteller Hacker stoppen.

Die Transformation der ISO 21434-Anforderungen in praxistaugliche Lösungen für OEMs (Original Equipment Manufacturers) der Automobilindustrie prägt unter anderem meine tägliche Arbeit mit meinem Team bei Cyber Complete. Diese Norm stellt einen Meilenstein in der Automobilindustrie dar, da sie spezifische Anforderungen an das Cyber Security Management System (CSMS) definiert, um die Sicherheit vernetzter Fahrzeuge zu gewährleisten.

HINTERGRUND DER ISO 21434

Die ISO 21434 ist eine internationale Norm, die speziell für die Automobilindustrie entwickelt wurde, um die Cybersicherheit von Fahrzeugen zu standardisieren. In einer Zeit, in der Fahrzeuge zunehmend vernetzt sind und über das Internet kommunizieren, steigt das Risiko von Cyberangriffen erheblich. Die Norm bietet einen strukturierten Ansatz, um diese Risiken zu managen und die Sicherheit von Fahrzeugen über ihren gesamten Lebenszyklus hinweg zu gewährleisten.

ZIELE DER ISO 21434

- **Schutz vor Cyberangriffen:** Fahrzeuge sind heute nicht mehr nur mechanische Maschinen, sondern hochkomplexe, vernetzte Systeme. Ein Beispiel für eine Bedrohung ist der unbefugte Zugriff auf das Fahrzeugnetzwerk, der es einem Angreifer ermöglichen könnte, die Kontrolle über kritische Systeme wie Bremsen oder Lenkung zu übernehmen. Ein weiteres Beispiel ist der Diebstahl sensibler Daten, wie Standortinformationen oder persönliche Daten der Insassen.

- **Sicherheitsmanagement:** Die Norm fordert von OEMs, dass sie ein systematisches Sicherheitsmanagement implementieren, das alle Phasen des Fahrzeuglebenszyklus abdeckt – von der Entwicklung über die Produktion bis hin zur Nutzung und Entsorgung. Dies stellt sicher, dass Sicherheitsaspekte von Anfang an berücksichtigt werden und kontinuierlich überwacht und verbessert werden.
- **Kontinuierliche Verbesserung:** Die Bedrohungslandschaft ändert sich ständig, und neue Schwachstellen können jederzeit entdeckt werden. Ein Beispiel hierfür ist die Entdeckung neuer Schwachstellen in der Fahrzeugsoftware, die es Angreifern ermöglichen könnten, Schadsoftware einzuschleusen. Die ISO 21434 fordert, dass OEMs Mechanismen einführen, um auf solche neuen Bedrohungen schnell zu reagieren und die Sicherheitsmaßnahmen entsprechend anzupassen.

ANFORDERUNGEN AN DAS CSMS

Ein Cyber Security Management System (CSMS) gemäß ISO 21434 ist ein umfassender Rahmen, der OEMs dabei hilft, die Cybersicherheit von Fahrzeugen systematisch zu verwalten. Die Anforderungen an ein CSMS umfassen mehrere kritische Komponenten, die sicherstellen, dass alle Aspekte der Cybersicherheit abgedeckt sind.

1. RISIKOBEWERTUNG UND -MANAGEMENT

- **Systematische Risikoidentifikation:** OEMs müssen potenzielle Cyberrisiken systematisch identifizieren. Dies beinhaltet die Analyse aller Fahrzeugkomponenten und -systeme, um Schwachstellen zu erkennen, die von Angreifern ausgenutzt werden könnten. Ein Beispiel ist die Risikoanalyse von drahtlosen Kommunikationsschnittstellen, die für externe Angriffe anfällig sein könnten.



- **Risikobewertung und Priorisierung:** Nach der Identifikation werden die Risiken bewertet und priorisiert, basierend auf ihrer potenziellen Auswirkung und Eintrittswahrscheinlichkeit. Dies ermöglicht es, Ressourcen gezielt auf die kritischsten Bedrohungen zu konzentrieren.
- **Risikominderungsstrategien:** OEMs müssen effektive Strategien zur Risikominderung entwickeln und implementieren. Dies kann technische Maßnahmen wie die Implementierung von Firewalls oder Intrusion Detection Systemen umfassen, sowie organisatorische Maßnahmen wie die Schulung von Mitarbeitern.

2. SICHERHEITSANFORDERUNGEN UND SPEZIFIKATIONEN

- **Entwicklung klarer Sicherheitsanforderungen:** Für jede Fahrzeugkomponente müssen klare Sicherheitsanforderungen definiert werden, die sicherstellen, dass sie gegen identifizierte Bedrohungen geschützt sind. Dies umfasst sowohl Hardware- als auch Softwarekomponenten.
- **Integration in den Entwicklungsprozess:** Sicherheitsanforderungen müssen von Anfang an in den Entwicklungsprozess integriert werden, um sicherzustellen, dass Sicherheitsaspekte nicht erst nachträglich berücksichtigt werden. Dies erfordert eine enge Zusammenarbeit zwischen den Entwicklungs- und Sicherheitsteams.

→

3. SICHERHEITSVALIDIERUNG UND VERIFIKATIONEN

- Regelmäßige Sicherheitsüberprüfungen: Die Wirksamkeit der implementierten Sicherheitsmaßnahmen muss regelmäßig überprüft werden. Dies beinhaltet Tests und Audits, um sicherzustellen, dass die Maßnahmen den aktuellen Bedrohungen standhalten.
- Verifikation der Sicherheitsanforderungen: OEMs müssen sicherstellen, dass alle definierten Sicherheitsanforderungen erfüllt werden, bevor ein Fahrzeug auf den Markt gebracht wird. Dies erfordert umfassende Tests und Validierungen in realen Szenarien.

4. INCIDENT-RESPONSE-PLAN

- **Entwicklung eines Incident-Response-Plans:** OEMs müssen Pläne entwickeln, um schnell und effektiv auf Sicherheitsvorfälle reagieren zu können. Ein gut definierter Incident-Response-Plan umfasst die Erkennung, Analyse und Behebung von Sicherheitsvorfällen sowie die Kommunikation mit betroffenen Stakeholdern.
- **Kontinuierliche Verbesserung:** Nach einem Vorfall sollten die Reaktionen und Maßnahmen analysiert werden, um den Incident-Response-Plan kontinuierlich zu verbessern und zukünftige Vorfälle effektiver zu bewältigen.

HERAUSFORDERUNGEN

- Komplexität der Fahrzeugarchitektur: Moderne Fahrzeuge sind hochkomplexe, vernetzte Systeme, die zahlreiche elektronische Steuergeräte (ECUs), Sensoren und Kommunikationsschnittstellen umfassen. Diese Komplexität stellt eine erhebliche Herausforderung bei der Implementierung eines effektiven Cyber Security Management Systems (CSMS) dar. Ein Beispiel ist die Sicherstellung der Integrität und Vertraulichkeit der Daten, die zwischen verschiedenen Fahrzeugkomponenten

ausgetauscht werden, insbesondere in einem Umfeld, in dem drahtlose Kommunikation zunehmend üblich ist.

- **Schnelllebigende Bedrohungslandschaft:** Die Bedrohungslandschaft im Bereich der Automobil-Cybersicherheit entwickelt sich rasant weiter. Neue Schwachstellen in Software und Hardware werden ständig entdeckt, was eine kontinuierliche Anpassung der Sicherheitsmaßnahmen erfordert. Ein Beispiel ist die Notwendigkeit, auf Zero-Day-Exploits zu reagieren, die das Potenzial haben, kritische Fahrzeugfunktionen zu kompromittieren.

BEST PRACTICES

- **Interdisziplinäre Zusammenarbeit:** Eine erfolgreiche Implementierung eines CSMS erfordert die enge Zusammenarbeit zwischen verschiedenen Abteilungen, einschließlich IT, Entwicklung, Produktion und Qualitätssicherung. Diese interdisziplinäre Zusammenarbeit stellt sicher, dass Sicherheitsaspekte in allen Phasen

IM ZEITALTER VON OTA-UPDATES ENDET VERANTWORTUNG FÜRS AUTOMOBIL NICHT MIT DER AUSLIEFERUNG.

DAS VERNETZTE AUTOMOBIL IST HEUTE EIN ROLLENDER COMPUTER UND SOMIT TEIL EINER ANGRIFFSFLÄCHE

des Fahrzeuglebenszyklus berücksichtigt werden. In meiner Erfahrung bei Cyber Complete habe ich gesehen, wie wichtig es ist, dass alle Beteiligten ein gemeinsames Verständnis für Cybersicherheitsziele entwickeln und umsetzen.

- **Kontinuierliche Schulung und Sensibilisierung:** Regelmäßige Schulungen sind entscheidend, um das Bewusstsein für Cybersicherheit auf allen Ebenen der Organisation zu stärken. Dies umfasst nicht nur technisches Personal, sondern auch Führungskräfte und Mitarbeiter in der Produktion. Die Schulungen sollten aktuelle Bedrohungen und Best Practices abdecken, um sicherzustellen, dass alle Mitarbeiter in der Lage sind, potenzielle Sicherheitsrisiken zu erkennen und angemessen zu reagieren.
- **Technologieüberwachung und Innovation:** OEMs sollten kontinuierlich neue Technologien und Methoden

zur Verbesserung der Cybersicherheit evaluieren und implementieren. Dies umfasst die Nutzung von fortschrittlichen Verschlüsselungstechnologien, Intrusion Detection Systemen (IDS) und Anomalieerkennung. In meiner Rolle als Berater habe ich oft betont, wie wichtig es ist, proaktiv zu sein und in Forschung und Entwicklung zu investieren, um der Bedrohungslandschaft einen Schritt voraus zu sein.

- **Etablierung eines robusten Incident-Response-Frameworks:** Ein effektiver Incident-Response-Plan ist entscheidend, um schnell und effizient auf Sicherheitsvorfälle reagieren zu können. Dies umfasst die Definition klarer Prozesse für die Erkennung, Analyse und Behebung von Vorfällen sowie die Kommunikation mit internen und externen Stakeholdern. Ein gut etabliertes Framework ermöglicht es OEMs, die Auswirkungen von Vorfällen zu minimieren und wertvolle Erkenntnisse zur Verbesserung der Sicherheitsmaßnahmen zu gewinnen.

SCHLUSSFOLGERUNG

Die Einführung der ISO 21434 stellt einen bedeutenden Schritt zur Verbesserung der Cybersicherheit in der Automobilindustrie dar. OEMs sind gefordert, ein robustes Cyber Security Management System zu implementieren, um den neuen Anforderungen gerecht zu werden. Durch die Umsetzung der ISO 21434 können OEMs nicht nur die Sicherheit ihrer Fahrzeuge erhöhen, sondern auch das Vertrauen ihrer Kunden stärken und ihre Marktposition sichern. In meiner Arbeit bei Cyber Complete habe ich gesehen, wie Unternehmen durch die strategische Implementierung eines CSMS ihre Sicherheitsarchitektur optimieren und gleichzeitig innovative Technologien nutzen können, um den Herausforderungen der Zukunft gewachsen zu sein. —

TISAX: SICHERHEITSSTANDARD DER AUTOMOBIL- INDUSTRIE

Der Sicherheitscheck für die Autowelt. Bestanden? Dann steht sicherer Zusammenarbeit nichts im Wege.

Ob große OEMs oder kleine Zulieferer – alle müssen beweisen, dass sie höchste Standards beim Schutz sensibler Daten einhalten.

TISAX sorgt dafür, dass Informationen wie Designs, technische Details oder Produktionspläne nicht in die falschen Hände geraten. TISAX schafft Vertrauen in einer komplexen Lieferkette – und wird damit zum entscheidenden Faktor für erfolgreiche Partnerschaften in der Automobilbranche.

TISAX – WAS IST DAS EIGENTLICH?

Stell dir vor, TISAX ist wie ein Sicherheitscheck für Unternehmen in der Automobilindustrie. Genau wie du dein Passwort schützt, um deine Social-Media-Konten sicher zu halten, hilft TISAX Unternehmen dabei, ihre wichtigen Informationen und Daten zu schützen. Es ist ein System, das sicherstellt, dass alle in der Automobilbranche – von den großen Autoherstellern bis zu den kleinen Zulieferern – die gleichen hohen Sicherheitsstandards einhalten. So können sie sicher zusammenarbeiten und sich darauf verlassen, dass ihre Daten sicher sind.

WARUM IST TISAX SO WICHTIG?

In der Automobilwelt arbeiten viele verschiedene Unternehmen zusammen, um ein Auto zu bauen. Dabei werden viele wichtige Informationen ausgetauscht, wie zum Beispiel neue Designs oder technische Details. Wenn diese Informationen in die falschen Hände geraten, könnte das großen Schaden anrichten. TISAX sorgt dafür, dass alle diese Informationen sicher bleiben, indem es überprüft, ob die Unternehmen die richtigen Sicherheitsmaßnahmen getroffen haben.

WIE FUNKTIONIERT TISAX?

TISAX funktioniert wie ein großer Sicherheitsleitfaden. Hier sind ein paar Dinge, die es macht:

RISIKEN ERKENNEN:

TISAX hilft Unternehmen dabei, herauszufinden, wo ihre Daten gefährdet sein könnten. Das ist so, als ob du überprüfst, ob deine Haustür wirklich abgeschlossen ist, bevor du das Haus verlässt.

SICHERHEITSMASSNAHMEN UMSETZEN:

Wenn ein Unternehmen weiß, wo es Schwachstellen gibt, kann es Maßnahmen ergreifen, um diese zu beheben. Das könnte bedeuten, bessere Passwörter zu verwenden oder spezielle Software zu installieren, die Hacker fernhält.

REGELMÄSSIGE ÜBERPRÜFUNGEN:

TISAX sorgt dafür, dass Unternehmen regelmäßig überprüfen, ob ihre Sicherheitsmaßnahmen noch funktionieren. Das ist wie ein regelmäßiger Check-up beim Arzt, um sicherzustellen, dass alles in Ordnung ist.

WARUM VERTRAUEN UNTERNEHMEN TISAX?

Unternehmen vertrauen TISAX, weil es von der Automobilbranche selbst entwickelt wurde. Das bedeutet, dass es genau auf die Bedürfnisse und Herausforderungen dieser Branche zugeschnitten ist. Wenn ein Unternehmen TISAX-zertifiziert ist, zeigt das, dass es die Sicherheit seiner Informationen ernst nimmt und bereit ist, die notwendigen Schritte zu unternehmen, um sie zu schützen.

SCHLUSSFOLGERUNG

In meiner Rolle bei Cyber Complete unterstütze ich Unternehmen dabei, TISAX in ihren Systemen zu implementieren. Ich arbeite eng mit ihnen zusammen, um sicherzustellen, dass sie die Anforderungen von TISAX erfüllen und ihre Informationssicherheit auf ein neues Niveau heben. Durch gezielte Beratung und maßgeschneiderte Lösungen helfe ich ihnen, die Herausforderungen der Cybersicherheit zu meistern und ihre Daten effektiv zu schützen. —

«IT-SICHERHEITS- PROJEKTE IM ALLTAG: WAS WIRKLICH ZÄHLT»

**Stakeholder bündeln:
So bringen Sie Cyber Security,
Management und Endnutzer
auf Kurs.**

IT-PROJEKTMANAGEMENT IN DER SECURITY

Die Leitung von Projekten zur Stärkung der Sicherheitsinfrastruktur in Unternehmen bildet einen zentralen Bestandteil meiner Tätigkeit im Bereich Cybersicherheit und IT-Projektmanagement. IT-Projektmanagement in der Security ist ein komplexer Prozess, der strategische Planung, präzise Ausführung und kontinuierliche Anpassung erfordert. In diesem Bericht werde ich die wesentlichen Erfolgsfaktoren, die Rolle der Stakeholder, das Risiko-Management und die konkreten Projektphasen anhand eines Beispiels erläutern.

ERFOLGSFAKTOREN

KLARE UND MESSBARE ZIELE:

Ein erfolgreiches IT-Sicherheitsprojekt beginnt mit klar definierten und messbaren Zielen. Diese Ziele sollten spezifisch, messbar, erreichbar, relevant und zeitgebunden (SMART) sein, um eine klare Richtung vorzugeben und den Fortschritt zu überwachen.

EFFEKTIVE KOMMUNIKATION UND ZUSAMMENARBEIT:

Die Kommunikation zwischen den Projektbeteiligten muss effizient und transparent sein. Regelmäßige Meetings und Updates sind entscheidend, um sicherzustellen, dass alle Stakeholder informiert sind und an einem Strang ziehen.

AGILITÄT UND ANPASSUNGSFÄHIGKEIT:

In der dynamischen Welt der IT-Sicherheit ist es unerlässlich, agil zu bleiben und sich schnell an neue Bedrohungen und Technologien anzupassen. Ein agiles Projektmanagement-Framework, wie Scrum oder Kanban, kann dabei helfen, flexibel auf Veränderungen zu reagieren.

STAKEHOLDER

Stakeholder spielen eine entscheidende Rolle im IT-Projektmanagement, da sie die Richtung und den Erfolg des Projekts maßgeblich beeinflussen. Zu den wichtigsten Stakeholdern gehören:

IT-SICHERHEITSTEAMS:

Diese Teams sind für die technische Umsetzung und den Betrieb der Sicherheitslösungen verantwortlich. Sie sorgen dafür, dass die Implementierung den Sicherheitsanforderungen entspricht.

GESCHÄFTSFÜHRUNG UND MANAGEMENT: Sie stellen die notwendigen Ressourcen bereit und treffen strategische Entscheidungen. Ihr Engagement ist entscheidend, um die Priorität des Projekts innerhalb der Organisation sicherzustellen.

ENDBENUTZER UND MITARBEITER:

Sie sind die primären Nutzer der Sicherheitslösungen. Ihr Feedback ist wichtig, um die Benutzerfreundlichkeit und Effektivität der Implementierung sicherzustellen.

RISIKOMANAGEMENT

Effektives Risiko-Management ist ein zentraler Bestandteil des IT-Projektmanagements in der Security. Es umfasst:

IDENTIFIKATION VON RISIKEN:

Systematische Erfassung potenzieller Risiken, die den Projekterfolg gefährden könnten, wie z. B. technische Herausforderungen, Ressourcenengpässe oder Compliance-Anforderungen.

RISIKOBEWERTUNG UND -PRIORISIERUNG: Analyse der identifizierten Risiken hinsichtlich ihrer Wahrscheinlichkeit und potenziellen Auswirkungen, um sie entsprechend zu priorisieren. Entwicklung von Risikomindestrategien: Implementierung von Maßnahmen zur Reduzierung der identifizierten Risiken, wie z. B. durch zusätzliche Schulungen, die Einführung von Backup-Systemen oder die Anpassung von Prozessen.

CASE STUDY | IT-SECURITY-ROLLOUT BEI DER REGUPOL GERMANY GMBH

Die Leitung von Projekten zur Stärkung der Sicherheitsinfrastruktur ist ein zentraler Bestandteil meiner Arbeit im Bereich Cybersicherheit und IT-Projektmanagement. →

Bild © Adobe Stock #444773772

Diese Fallstudie beleuchtet ein umfassendes IT-Sicherheitsprojekt, welches bei der REGUPOL Germany GmbH & Co. KG im Sommer 2021 begann und im Frühjahr 2024 abgeschlossen wurde. Ziel war es, ein robustes Information Security Management System (ISMS) nach ISO 27001 zu etablieren und die IT-Infrastruktur zu härten.

PROJEKTSTART UND GAP-ANALYSE

Ich wurde als externer IT-Projektleiter zu diesem Projekt hinzugezogen. Der erste Schritt war eine dreitägige GAP-Analyse, um die aktuelle Sicherheitslage zu bewerten. Diese Analyse diente als Grundlage für die weitere Planung.

ERFOLGSFAKTOREN

Klare und messbare Ziele: Die Ziele des Projekts wurden von Anfang an klar definiert. Dazu gehörte die Etablierung eines auditfähigen ISMS nach ISO 27001 und die Härtung der IT-Infrastruktur.

ERSTELLUNG EINES MASSNAHMENPLANS

Basierend auf der GAP-Analyse wurde ein detaillierter Maßnahmenplan erstellt. Dieser Plan umfasste verschiedene Arbeitspakete, die schrittweise umgesetzt wurden, um die Sicherheitslage zu verbessern. Zu den wichtigsten Maßnahmen gehör-

ten: Aufbau eines ISMS nach ISO 27001: Dies beinhaltete die Entwicklung von Sicherheitsrichtlinien, die Schulung von Mitarbeitern und die Implementierung von Sicherheitskontrollen. Ein besonderer Fokus lag auf dem Patchmanagement, um Sicherheitslücken zu schließen.

DURCHFÜHRUNG EINES PENETRATION-TESTS

Ein weiterer entscheidender Schritt war die Durchführung eines Penetration-Tests nach BSI-Standard.

RISIKO-MANAGEMENT

Wir identifizierten potenzielle Risiken, bewerteten sie hinsichtlich ihrer Wahrscheinlichkeit und entwickelten Strategien zur Risikominderung.

PROJEKTABSCHLUSS

Das Projekt wurde im Frühjahr 2024 erfolgreich abgeschlossen. Das Ergebnis war ein auditfähiges Managementsystem nach ISO 27001:2022, das die Sicherheitslage der REGUPOL erheblich verbesserte.

SCHLUSSFOLGERUNG

Diese Fallstudie zeigt, dass ein erfolgreiches IT-Sicherheitsprojekt klare Ziele, effektive Kommunikation, Agilität und ein starkes Risiko-Management erfordert._____

WENN ES UM DIGITALE
SICHERHEIT GEHT, VERTRAUEN WIR
AUF CYBER COMPLETE.



EIN UNTERNEHMEN MIT GROSSER PRODUKTVIELFALT

REGUPOL zählt zu den weltweit führenden Verarbeitern von wiedergewonnenen Elastomeren. Daraus entstehen leistungsstarke Sportböden, Fallschutzböden, Antirutschmatten zur Ladungssicherung, Produkte zur Trittschalldämmung und Schwingungsisolierung sowie Schutz- und Trennlagen für Bauanwendungen.

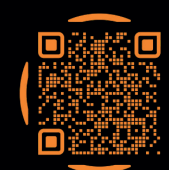


DIGITALE EXZELLENZ: DAS SYSTEMHAUS, DAS MEHR ALS IT BIETET

- ✓ IT-Sicherheit: Backups, Antivirus, Firewalling
- ✓ Gastro & Hotel-Lösungen: EC-Geräte, Kassensysteme & Digital Signage
- ✓ Gebäudesicherheit & Automatisierung
- ✓ Beratungen und Implementierungen rund um Microsoft 365
- ✓ Business Service-Abonnements
- ✓ Umsetzung & Betreuung relevanter Sicherheitsstandards (NIS2, TISAX, KRITIS)

ZUKUNFT GESTALTEN, RISIKEN ABSICHERN

Vertrauen Sie auf proaktive und zukunftsichere IT-Lösungen, die den komplexen Anforderungen Ihrer Branche gerecht werden. Mit unseren maßgeschneiderten IT-Service-Abos erhalten Sie nicht nur Sicherheit und Stabilität, sondern auch die Innovationskraft, um sich von Mitbewerbern abzuheben.

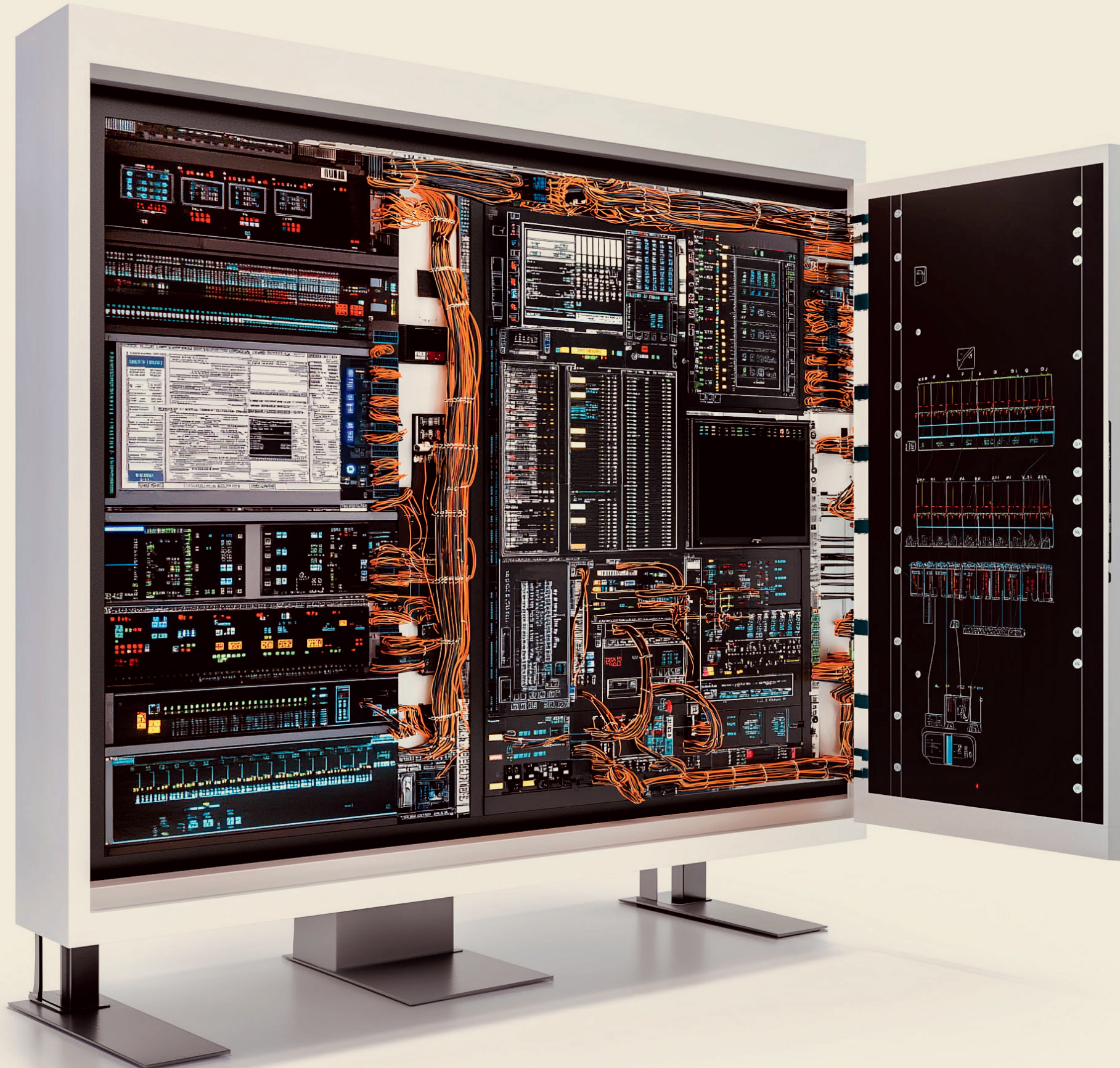


MEET THE TEAM
UNSERE GESCHICHTE
& UNSER TEAM



DIREKTER DRAHT
ZU UNS!





OT IM VISIER

**Wenn Produktionsanlagen,
Versorgungssysteme und
Sicherheit angreifbar werden.**

*Warum der Schutz von Steuerungssystemen zur
Lebensader moderner Gesellschaften wird – und
wie Cyberangriffe auf OT zur realen Bedrohung für
Sicherheit, Versorgung und Wirtschaft werden.*

OT-SECURITY: SCHUTZ KRITISCHER INFRASTRUKTUREN IM DIGITALEN ZEITALTER

In meiner Karriere als Cybersicherheitsexperte habe ich oft die besondere Herausforderung erlebt, die mit der Sicherung von Operational Technology (OT) einhergeht. OT umfasst die Hardware und Software, die physische Geräte und Prozesse überwacht und steuert – von Produktionsanlagen bis hin zu Versorgungsnetzen. Besonders im Bereich der kritischen Infrastrukturen (KRITIS) ist OT-Security von entscheidender Bedeutung. In diesem Artikel teile ich meine Erfahrungen und Erkenntnisse über die Sicherung dieser essenziellen Systeme.

DIE BEDEUTUNG VON OT-SECURITY

OT-Systeme sind das Rückgrat vieler kritischer Infrastrukturen, wie Energieversorgung, Wasserwirtschaft, Transportwesen und Produktion. Ihre Sicherheit ist daher von nationalem Interesse. Ein erfolgreicher Angriff auf OT-Systeme kann nicht nur finanzielle Schäden verursachen, sondern auch die öffentliche Sicherheit gefährden. In meiner Arbeit habe ich gesehen, wie wichtig es ist, dass Unternehmen die spezifischen Risiken und Herausforderungen von OT-Security verstehen und adressieren.

HERAUSFORDERUNGEN IN DER OT-SECURITY

VERALTETE SYSTEME

Viele OT-Systeme sind über Jahrzehnte gewachsen und basieren auf veralteter Technologie, die ursprünglich nicht für die Vernetzung und die heutigen Bedrohungen ausgelegt war. Die Modernisierung dieser Systeme ist oft komplex und kostspielig, aber unerlässlich.

INTEGRATION VON IT UND OT

Die zunehmende Vernetzung von IT- und OT-Systemen bietet viele Vorteile, bringt aber auch neue Sicherheitsrisiken mit sich. In meiner Praxis habe ich erlebt, wie wichtig es ist, diese beiden Welten sicher zu integrieren, um Angriffsvektoren zu minimieren.

SPEZIFISCHE BEDROHUNGEN

OT-Systeme sind oft Ziel von Angriffen, die darauf ausgerichtet sind, physische Prozesse zu stören. Diese Angriffe erfordern spezielle Sicherheitsmaßnahmen, die über traditionelle IT-Sicherheitslösungen hinausgehen.

STRATEGIEN ZUR SICHERUNG VON OT-SYSTEMEN

RISIKOBEWERTUNG UND PRIORISIERUNG

Ein erster Schritt zur Sicherung von OT-Systemen ist die Durchführung einer umfassenden Risikobewertung. In meinen Projekten beginne ich stets damit, die kritischsten Systeme zu identifizieren und Maßnahmen zu priorisieren, die den größten Sicherheitsgewinn versprechen.

NETZWERKSEGMENTIERUNG

Durch die Segmentierung von Netzwerken können Unternehmen das Risiko von Angriffen reduzieren, indem sie den Zugriff auf kritische Systeme einschränken. Diese Strategie hat sich in meiner Erfahrung als äußerst effektiv erwiesen, um die Ausbreitung von Bedrohungen zu verhindern.

SICHERHEITSBEWUSSTSEIN UND SCHULUNG

Wie in vielen Bereichen der Cybersicherheit ist auch hier der Faktor Mensch entscheidend. Ich lege großen Wert darauf, dass Mitarbeiter regelmäßig geschult werden, um Sicherheitsrichtlinien zu verstehen und umzusetzen.

CASE STUDY – SICHERUNG EINER ENERGIEVERSORGUNGSANLAGE

HINTERGRUND

In einem meiner jüngsten Projekte wurde ich von einem großen Energieversorger beauftragt, die Sicherheitslage seiner OT-Systeme zu evaluieren und zu verbessern. Diese Anlage versorgt mehrere Millionen Haushalte mit Strom und ist somit ein kritisches Element der nationalen Infrastruktur. Angesichts der zunehmenden Bedrohungen durch Cyberangriffe war es von größter Bedeutung, die Sicherheitsmaßnahmen zu stärken.

HERAUSFORDERUNGEN

Bei der ersten Analyse identifizierte ich mehrere wichtige Herausforderungen:

- **Veraltete Technologie:** Viele der Steuerungssysteme waren über 20 Jahre alt und nicht für die heutige vernetzte Welt ausgelegt.
- **Fehlende Integration:** Die IT- und OT-Systeme waren isoliert, was zu ineffizienten Prozessen und Sicherheitslücken führte.
- **Unzureichende Überwachung:** Es gab keine kontinuierliche Überwachung der OT-Systeme, was die Erkennung von Anomalien erschwerte.

STRATEGISCHE MASSNAHMEN

Um diese Herausforderungen anzugehen, entwickelte ich einen mehrstufigen Plan:

1. **Risikobewertung und Priorisierung:** Zunächst führten wir eine umfassende Risikobewertung durch, um die kritischsten Systeme zu identifizieren. Dies half uns, die Maßnahmen zu priorisieren, die den größten Einfluss auf die Sicherheit haben würden.
2. **Modernisierung der Infrastruktur:** In Zusammenarbeit mit dem internen IT-Team des Unternehmens begannen wir mit der schrittweisen Modernisierung der veralteten Steuerungssysteme. Dies umfasste die Implementierung von Firewalls und Intrusion Detection Systemen (IDS), die speziell für OT-Umgebungen ausgelegt sind.
3. **Netzwerksegmentierung:** Wir segmentierten das Netzwerk, um den Zugriff auf kritische Systeme zu beschränken. Dies beinhaltete die Einrichtung von VLANs und die Implementierung von strengen Zugriffsrichtlinien, um sicherzustellen, dass nur autorisiertes Personal Zugriff auf sensible Bereiche hatte.
4. **Echtzeit-Überwachung und Anomalieerkennung:** Wir führten ein System zur kontinuierlichen Überwachung ein, das in der Lage war, Anomalien in Echtzeit zu erkennen. Dies ermöglichte es uns, potenzielle Bedrohungen proaktiv zu identifizieren und zu neutralisieren.
5. **SCHULUNGSPROGRAMME:** Parallel dazu entwickelten wir ein umfassendes Schulungsprogramm für die Mitarbeiter. Ziel war es, das Bewusstsein für Sicherheitsrisiken zu schärfen und die Belegschaft in den neuesten Sicherheitspraktiken zu schulen.

ERGEBNISSE

Die Implementierung dieser Maßnahmen führte zu einer signifikanten Verbesserung der Sicherheitslage der Anlage:

- **Reduzierte Angriffsfläche:** Durch die Modernisierung und Segmentierung wurde die potenzielle Angriffsfläche erheblich reduziert.
- **Schnellere Reaktionszeiten:** Dank der Echtzeit-Überwachung konnten Bedrohungen schneller erkannt und abgewehrt werden.
- **Erhöhtes Sicherheitsbewusstsein:** Die Schulungsprogramme führten zu einem gesteigerten Sicherheitsbewusstsein unter den Mitarbeitern, was das Risiko menschlicher Fehler verringerte.

SCHLUSSFOLGERUNG

Dieses Projekt verdeutlichte mir erneut, wie wichtig eine ganzheitliche Sicherheitsstrategie ist, die sowohl technische als auch menschliche Faktoren berücksichtigt. Die Zusammenarbeit mit dem Energieversorger war ein eindrucksvolles Beispiel dafür, wie maßgeschneiderte Sicherheitslösungen dazu beitragen können, kritische Infrastrukturen effektiv zu schützen. Es war eine herausfordernde, aber äußerst lohnende Erfahrung, die mir gezeigt hat, wie entscheidend es ist, stets einen Schritt voraus zu denken, um die Sicherheit unserer lebenswichtigen Systeme zu gewährleisten. In meiner Rolle bei Cyber Complete bin ich bestrebt, Unternehmen dabei zu unterstützen, ihre OT-Sicherheit zu stärken und somit einen wesentlichen Beitrag zur nationalen Sicherheit zu leisten. —

ALTE SYSTEME IN DIE MODERNE ZU BRINGEN, IST EINE KUNST FÜR SICH.



WAS UNTERNEHMEN
ÜBER FIREWALLS, SWITCHE
UND PATCHMANAGEMENT
WISSEN SOLLTEN - UND WIE
SIE DAMIT AUSFÄLLE,
SICHERHEITSLÜCKEN UND
DATENVERLUSTE
VERMEIDEN KÖNNEN.

Firewalls, Switche *und*

Patch- management

OPTIMIERUNG DER IT-INFRASTRUKTUR:

Ein tiefer Einblick in Firewalls, Switche und Patchmanagement

Die IT-Infrastruktur bildet das Fundament jedes modernen Unternehmens. Sie gewährleistet nicht nur die Effizienz und Kontinuität der Geschäftsprozesse, sondern schützt auch vor den vielfältigen Bedrohungen der digitalen Welt. In diesem Bericht beleuchte ich die entscheidenden Komponenten einer effektiven IT-Infrastruktur: Firewalls, Switche und Patchmanagement.

FIREWALLS: DIE ERSTE VERTEIDIGUNGSLINIE

Firewalls sind essenzielle Sicherheitsvorrichtungen, die den Datenverkehr zwischen internen Netzwerken und externen Quellen überwachen und kontrollieren. Sie fungieren als Barriere, die unerwünschte Zugriffe blockiert und legitimen Datenverkehr zulässt. In meiner Erfahrung als IT-Sicherheitsexperte sind Firewalls unerlässlich, um Netzwerke vor Bedrohungen wie Malware, unautorisierten Zugriffen und Datenlecks zu schützen.

ARTEN VON FIREWALLS

- **Hardware-Firewalls:** Diese physischen Geräte werden zwischen dem internen Netzwerk und dem Internet platziert. Sie bieten eine robuste Sicherheitsbarriere und sind ideal für den Schutz großer Netzwerke.
- **Software-Firewalls:** Diese werden auf einzelnen Geräten installiert und bieten Schutz auf Anwendungsebene. Sie sind besonders nützlich für den Schutz von Endgeräten in einem Netzwerk.
- **Next-Generation Firewalls (NGFW):** Diese modernen Firewalls kombinieren die Funktionen traditioneller Firewalls

mit erweiterten Sicherheitsfunktionen wie Intrusion Prevention Systems (IPS), Deep Packet Inspection (DPI) und Anwendungsbewusstsein. Sie bieten einen umfassenderen Schutz gegen komplexe Bedrohungen.

BEST PRACTICES FÜR DEN EINSATZ VON FIREWALLS

REGELMÄSSIGE AKTUALISIERUNG: Firewalls sollten regelmäßig aktualisiert werden, um neue Bedrohungen abzuwehren.

KONFIGURATIONSÜBERPRÜFUNG: Regelmäßige Überprüfung der Firewall-Regeln und -Konfigurationen, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entsprechen.

PROTOKOLLIERUNG UND ÜBERWACHUNG: Kontinuierliche Überwachung der Firewall-Protokolle, um ungewöhnliche Aktivitäten frühzeitig zu erkennen.

SWITCHE: DIE NETZWERKARCHITEKTEN

Switche sind entscheidend für die Netzwerkarchitektur, da sie den Datenverkehr innerhalb eines Netzwerks effizient leiten. Sie verbinden Geräte innerhalb eines Netzwerks und sorgen dafür, dass Datenpakete schnell und sicher an ihr Ziel gelangen. Switche spielen eine zentrale Rolle bei der Optimierung der Netzwerkleistung und der Sicherstellung einer stabilen Verbindung.

Arten von Switchen

- **Unmanaged Switch:** Diese einfachen Geräte sind leicht zu installieren und zu verwenden, bieten jedoch keine erweiterten Funktionen. Sie eignen sich für kleine Netzwerke mit minimalen Anforderungen.
- **Managed Switch:** Diese bieten erweiterte Funktionen wie VLANs (Virtual Local Area Networks), QoS (Quality of

Service) und Port-Spiegelung. Sie sind für größere Netzwerke, die eine feinere Kontrolle und Verwaltung erfordern.

- **Layer 3 Switch:** Diese kombinieren die Funktionen von Routern und Switchen und ermöglichen das Routing von Datenpaketen zwischen verschiedenen Netzwerken. Sie sind besonders nützlich in großen, komplexen Netzwerkimgebungen.

BEST PRACTICES FÜR DEN EINSATZ VON SWITCHEN

NETZWERKSEGMENTIERUNG: Verwendung von VLANs zur Segmentierung des Netzwerks, um die Sicherheit zu erhöhen und den Datenverkehr effizienter zu verwalten.

QOS-EINSTELLUNGEN: Implementierung von QoS, um sicherzustellen, dass kritische Anwendungen die notwendige Bandbreite erhalten.

REGELMÄSSIGE WARTUNG: Überprüfung und Aktualisierung der Switch-Konfigurationen, um sicherzustellen, dass sie den aktuellen Anforderungen entsprechen.

PATCHMANAGEMENT: DIE UNSICHTBARE SCHUTZSCHICHT

Patchmanagement ist ein kritischer Aspekt der IT-Sicherheit, der oft übersehen wird. Es umfasst das Aktualisieren von Software und Betriebssystemen, um Sicherheitslücken zu schließen und die Leistung zu verbessern. Unregelmäßiges Patchmanagement kann zu erheblichen Sicherheitsrisiken führen, da Angreifer bekannte Schwachstellen ausnutzen können.

BEST PRACTICES IM PATCHMANAGEMENT

REGELMÄSSIGE ÜBERPRÜFUNG: Kontinuierliche Überwachung auf verfügbare Updates und Patches, um sicherzustellen, dass alle Systeme auf dem neuesten Stand sind.

AUTOMATISIERUNG: Einsatz von Tools zur Automatisierung des Patch-Prozesses, um menschliche Fehler zu minimieren und die Effizienz zu steigern.

TESTEN VOR DER IMPLEMENTIERUNG: Patches sollten in einer Testumgebung geprüft werden, um sicherzustellen, dass sie keine unerwünschten Auswirkungen auf die Systeme haben.

SCHLUSSFOLGERUNG

Eine gut optimierte IT-Infrastruktur ist entscheidend für die Sicherheit und Effizienz eines Unternehmens. Durch die richtige Auswahl und Implementierung von Firewalls, Switchen und einem effektiven Patchmanagement können Unternehmen ihre Netzwerke schützen und ihre Leistungsfähigkeit maximieren. In meiner Rolle als IT-Sicherheitsexperte bin ich bestrebt, Unternehmen dabei zu unterstützen, ihre Infrastruktur kontinuierlich zu verbessern und an die sich wandelnden Anforderungen der digitalen Welt anzupassen.

SWITCHE SIND DIE VERKEHRS- ARCHITEKTEN DER DATEN – WENN SIE VERSAGEN, STEHT ALLES STILL.



DER ERNSTFALL

*Sind Sie
vorbereitet?*

Krise, Notfall oder gleich BCM? Benjamin Richter zeigt, was je nach Unternehmensgröße sinnvoll ist und welche Tests wirklich zählen – Kommunikation, IT-Wiederherstellung, Evakuierung, Szenario-Drills. Mit Praxisbeispiel: so wird ein Mittelständler messbar widerstandsfähiger.

K Mit meiner Expertise als Business Continuity Manager (BCM) habe ich festgestellt, dass die Fähigkeit eines Unternehmens, auf unerwartete Ereignisse zu reagieren, entscheidend für seinen Fortbestand ist. Ob es sich um eine IT-Panne, einen

Cyberangriff oder eine Naturkatastrophe handelt, Unternehmen müssen vorbereitet sein. In diesem Bericht teile ich meine Erkenntnisse über die Bedeutung von Krisenmanagement, Notfallplänen und BCM und wie ich einem mittelständischen Unternehmen geholfen habe, seine Präventionsmaßnahmen zu stärken.

KRISENMANAGEMENT VS. NOTFALLPLÄNE VS. BCM

- **Krisenmanagement:** In meiner Arbeit beziehe ich mich auf die kurzfristige Reaktion auf ein plötzliches Ereignis, das den normalen Geschäftsbetrieb unterbricht. Es umfasst die sofortige Mobilisierung von Ressourcen, um die Auswirkungen der Krise zu minimieren und den Betrieb so schnell wie möglich wiederherzustellen.
- **Notfallpläne:** Diese Pläne sind spezifische Protokolle, die im Falle eines Notfalls aktiviert werden. Sie konzentrieren sich auf die Sicherstellung der Sicherheit von Mitarbeitern und Vermögenswerten und beinhalten oft Evakuierungspläne, Kommunikationsstrategien und erste Maßnahmen zur Schadensbegrenzung.
- **Business Continuity Management (BCM):** BCM ist ein umfassender

Ansatz, der über das reine Krisenmanagement hinausgeht. Es umfasst die Identifizierung potenzieller Bedrohungen und die Bewertung ihrer Auswirkungen auf den Geschäftsbetrieb. Mein Ziel ist es, die Widerstandsfähigkeit des Unternehmens zu stärken, indem Strategien entwickelt werden, um den Betrieb trotz Störungen aufrechtzuerhalten.

WAS MACHT JE NACH UNTERNEHMENSGRÖSSE SINN?

KLEINE UNTERNEHMEN

- **Fokussierung auf Notfallpläne:** Ich empfehle kleinen Unternehmen, sich auf die Entwicklung robuster Notfallpläne zu konzentrieren, die einfach zu implementieren sind. Diese Pläne sollten klare Anweisungen für den Umgang mit häufigen Bedrohungen wie IT-Ausfällen oder physischen Sicherheitsvorfällen enthalten.
- **Ressourcenoptimierung:** Aufgrund begrenzter Ressourcen ist es entscheidend, dass kleine Unternehmen ihre vorhandenen Mittel optimal nutzen. Dies kann durch die Schulung von Mitarbeitern in mehreren Rollen und die Nutzung externer Berater für spezifische Sicherheitsanalysen erreicht werden.

MITTLERE UNTERNEHMEN

- **Erweiterung auf Krisenmanagement:** Mittlere Unternehmen können von einem formellen Krisenmanagement-Team profitieren, das regelmäßig geschult wird, um auf verschiedene Szenarien zu reagieren. Dies hilft, die Reaktionszeit zu verkürzen und die Effizienz bei der Bewältigung von Krisen zu erhöhen.
- **Integration von BCM-Elementen:** Obwohl vollständiges BCM möglicher-

weise nicht praktikabel ist, können mittlere Unternehmen beginnen, Elemente davon zu integrieren, wie z. B. die Durchführung von Business Impact Analysen (BIA) und die Identifizierung kritischer Geschäftsprozesse.

GROSSE UNTERNEHMEN

- **Umfassendes BCM-Programm:** Große Unternehmen sollten ein vollständiges BCM-Programm implementieren, das alle Aspekte von Risikoanalysen bis hin zur Wiederherstellung von Geschäftsprozessen abdeckt. Diese Programme sollten regelmäßig überprüft und aktualisiert werden, um neuen Bedrohungen gerecht zu werden.
- **Regelmäßige Tests und Übungen:** Große Unternehmen haben die Ressourcen, um regelmäßige BCM-Tests und Übungen durchzuführen. Diese sollten Szenarien umfassen, die von Cyberangriffen bis hin zu Naturkatastrophen reichen, um die Wirksamkeit der Pläne zu überprüfen und Schwachstellen zu identifizieren.

WAS SOLLTE GETESTET WERDEN?

Unabhängig von der Unternehmensgröße sollten folgende Aspekte regelmäßig getestet werden:

Kommunikationspläne: Stellen Sie sicher, dass alle Mitarbeiter wissen, wie sie im Notfall kommunizieren sollen. Testen Sie die Kommunikationskanäle auf Zuverlässigkeit und Geschwindigkeit.

IT-Disaster-Recovery-Pläne: Überprüfen Sie die Fähigkeit, IT-Systeme nach einem Ausfall schnell wiederherzustellen. Dies umfasst Backup- und Wiederherstellungsprozesse sowie die Verfügbarkeit von Ersatzhardware.

Evakuierungsübungen: Führen Sie regelmäßig Evakuierungsübungen durch,

um sicherzustellen, dass alle Mitarbeiter die Notausgänge kennen und wissen, wie sie sicher das Gebäude verlassen können.

Szenario-basierte Übungen: Simulieren Sie spezifische Bedrohungsszenarien, um die Reaktionsfähigkeit des Unternehmens zu testen und Verbesserungsmöglichkeiten zu identifizieren.

CASE STUDY: IMPLEMENTIERUNG EINES BCM-PROGRAMMS BEI EINEM MITTELSTÄNDISCHEN UNTERNEHMEN

HINTERGRUND

Ich wurde von einem mittelständischen Unternehmen beauftragt, ihre Präventionsmaßnahmen zu stärken. Das Unternehmen, das in der Fertigungsindustrie tätig ist, erkannte die Notwendigkeit, seine Geschäftsprozesse gegen potenzielle Störungen abzusichern. →

IM MITTELSTAND MACHT EIN TRAINIERTES KRISENTEAM DEN UNTERSCHIED IN MINUTEN.

PROJEKTPHASEN

- **Initiale Risikoanalyse:** Ich führte eine umfassende Risikoanalyse durch, um die größten Bedrohungen für den Geschäftsbetrieb zu identifizieren. Dies umfasste sowohl interne Risiken wie IT-Ausfälle als auch externe Risiken wie Lieferkettenunterbrechungen.
- **Business Impact Analyse (BIA):** Gemeinsam mit dem Management bewertete ich die kritischen Geschäftsprozesse und ihre Abhängigkeiten, um die potenziellen Auswirkungen von Unterbrechungen zu verstehen. Dies half, Prioritäten für die Wiederherstellung festzulegen.
- **Entwicklung von BCM-Strategien:** Basierend auf den Ergebnissen der BIA entwickelte ich maßgeschneiderte BCM-Strategien, die auf die spezifischen Bedürfnisse und Ressourcen des Unternehmens abgestimmt waren. Dazu gehörten Pläne für die Notfallwiederherstellung und alternative Lieferkettenstrategien.
- **Schulung und Sensibilisierung:** Ich führte Schulungen für alle Mitarbeiter durch, um das Bewusstsein für BCM zu schärfen und sicherzustellen, dass jeder seine Rolle im Notfall versteht.
- **Testen und Optimierung:** Das Unternehmen führte regelmäßige Tests und Übungen durch, um die Wirksamkeit des BCM-Programms zu überprüfen. Die Ergebnisse dieser Tests wurden genutzt, um die Pläne kontinuierlich zu verbessern.

ERGEBNISSE

Durch die Implementierung des BCM-Programms konnte das Unternehmen seine Widerstandsfähigkeit erheblich

steigern. Die Mitarbeiter waren besser auf Notfälle vorbereitet, und die Geschäftsprozesse konnten auch in Krisensituationen aufrechterhalten werden. Meine Expertise half dem Unternehmen, Schwachstellen zu identifizieren und gezielte Verbesserungen vorzunehmen.

SCHLUSSFOLGERUNG

Die Wahl zwischen Krisenmanagement, Notfallplänen und BCM hängt stark von der Größe und den spezifischen Anforderungen eines Unternehmens ab. Während kleine Unternehmen möglicherweise mit grundlegenden Notfallplänen beginnen, können größere Organisationen von einem umfassenden BCM-Ansatz profitieren.

Meine Arbeit zeigt, wie ein gezielter Ansatz zur Stärkung der Präventionsmaßnahmen eines Unternehmens führen kann. In meiner Rolle bei Cyber Complete unterstütze ich Unternehmen dabei, die für sie passenden Präventionsmaßnahmen zu entwickeln und zu implementieren, um ihre Widerstandsfähigkeit zu stärken und ihre Geschäftsprozesse zu schützen.

DER BESTE ZEITPUNKT FÜR PRÄVENTION WAR GESTERN. DER ZWEITBESTE IST JETZT.

Schulung & Sensibilisierung

Der Schlüssel zur echten Sicherheitskultur

Meine Erfahrung im Bereich Cybersicherheit hat mir wiederholt gezeigt, dass Technologie allein nicht ausreicht, um ein Unternehmen vor Bedrohungen zu schützen. Der Faktor Mensch spielt eine entscheidende Rolle bei der Aufrechterhaltung der Sicherheit. In diesem Artikel möchte ich die Bedeutung der Mitarbeitersensibilisierung, das Design von Trainingsprogrammen und das Change Management im Kontext von Sicherheitsmaßnahmen beleuchten, insbesondere im Hinblick auf die NIS2-Richtlinie.

BEDEUTUNG DER MITARBEITER-SENSIBILISIERUNG

Die Sensibilisierung der Mitarbeiter ist ein wesentlicher Bestandteil jeder Sicherheitsstrategie. In meinen Projekten habe ich oft erlebt, wie ein gut informierter Mitarbeiterstamm die erste Verteidigungslinie gegen Cyberbedrohungen bildet. Schulungen tragen dazu bei, das Bewusstsein für potenzielle Gefahren zu schärfen und den Mitarbeitern die notwendigen Werkzeuge an die Hand zu geben, um sicherheitsbewusste Entscheidungen zu treffen.

TRAININGSDESIGN UND CHANGE MANAGEMENT

TRAININGSDESIGN

Ein effektives Trainingsprogramm muss gut durchdacht und auf die spezifischen Bedürfnisse des Unternehmens zugeschnitten sein. In meiner Praxis setze ich auf eine Kombination aus theoretischen Inhalten und praktischen Übungen, um sicherzustellen, dass die Mitarbeiter nicht nur das "Was", sondern auch das "Wie" verstehen. Die Integration von realen Szenarien in das Training hilft den Teilnehmern, das Gelernte direkt anzuwenden.

CHANGE MANAGEMENT

Die Einführung neuer Sicherheitsmaßnahmen erfordert oft eine Veränderung der Unternehmenskultur. Change Management ist daher ein kritischer Aspekt bei der Implementierung von Sicherheitsstrategien. Ich habe festgestellt, dass eine transparente Kommunikation und die Einbindung der Mitarbeiter in den Veränderungsprozess entscheidend sind, um Widerstände zu minimieren und Akzeptanz zu fördern. →

NIS2 BERATUNGSKOMPONENTEN

Bei der Beratung zur NIS2-Richtlinie lege ich besonderen Wert darauf, dass Unternehmen nicht nur technische Maßnahmen ergreifen, sondern auch ihre Mitarbeiter in den Prozess einbinden. Die Schulung und Sensibilisierung der Belegschaft ist ein zentraler Bestandteil, um die Anforderungen der Richtlinie zu erfüllen und die Sicherheitskultur nachhaltig zu stärken.

DER FAKTOR MENSCH

Der Faktor Mensch ist oft das schwächste Glied in der Sicherheitskette. In meiner Arbeit betone ich, dass es nicht ausreicht, lediglich technische Lösungen zu implementieren. Die Mitarbeiter müssen verstehen, welche Rolle sie im Sicherheitsprozess spielen und wie ihre Handlungen die Sicherheit des gesamten Unternehmens beeinflussen können.

VOR- UND NACHTEILE BEIM EINSATZ VON ELEARNING PLATTFORMEN**VORTEILE**

- **Flexibilität:** eLearning-Plattformen bieten den Mitarbeitern die Möglichkeit, Schulungen in ihrem eigenen Tempo und zu Zeiten zu absolvieren, die in ihren Arbeitsalltag passen. Dies erhöht die Teilnahmebereitschaft und den Lernerfolg.
- **Kosteneffizienz:** Durch den Einsatz von eLearning können Unternehmen die Kosten für Präsenzs Schulungen und Reisekosten reduzieren. In meiner Erfahrung ist dies besonders für größere Unternehmen von Vorteil, die Schulungen an mehreren Standorten durchführen müssen.
- **Skalierbarkeit:** eLearning ermöglicht es, Schulungsinhalte schnell und effizient an eine große Anzahl von Mitarbeitern zu vermitteln.

NACHTEILE

- **Fehlende Interaktivität:** Ein Nachteil von eLearning-Plattformen kann die fehlende persönliche Interaktion sein. In meinen Projekten habe ich festgestellt, dass der direkte Austausch mit Trainern und anderen Teilnehmern oft zu einem tieferen Verständnis der Inhalte führt.
- **Motivationsprobleme:** Nicht alle Mitarbeiter sind von Natur aus motiviert, sich selbstständig weiterzubilden. Hier ist es wichtig, Anreize zu schaffen und den Fortschritt zu überwachen.
- **Technische Barrieren:** Der Zugang zu und die Nutzung von eLearning-Plattformen kann für einige Mitarbeiter eine Herausforderung darstellen, insbesondere wenn sie nicht mit der Technologie vertraut sind.

SCHLUSSFOLGERUNG

Die Schulung und Sensibilisierung von Mitarbeitern ist ein unverzichtbarer Bestandteil jeder Sicherheitsstrategie. Durch gut gestaltete Trainingsprogramme und effektives Change Management können Unternehmen die Sicherheitskultur stärken und die Anforderungen der NIS2-Richtlinie erfüllen.

Der Einsatz von eLearning-Plattformen bietet viele Vorteile, erfordert jedoch auch Maßnahmen, um die Nachteile zu überwinden. In meiner Rolle bei Cyber Complete unterstütze ich Unternehmen dabei, maßgeschneiderte Schulungsprogramme zu entwickeln, die den Faktor Mensch in den Mittelpunkt stellen und die Sicherheitskultur nachhaltig verbessern.



AUSBLICK & ZUKUNFTS- THEMEN

Zum Schluss der Blick nach vorn:
Was morgen über Cybersicherheit entscheidet –
und welche Weichen wir heute stellen.

EU-CYBERSTRATEGIE

Die europäische Cyberstrategie ist ein umfassender Plan der Europäischen Union, um die Cybersicherheit in Europa zu stärken und die digitale Souveränität zu gewährleisten. Diese Strategie zielt darauf ab, Europa widerstandsfähiger gegenüber Cyberangriffen zu machen und die Zusammenarbeit zwischen den Mitgliedstaaten zu verbessern. In meiner Arbeit bei Cyber Complete sehe ich, wie wichtig es ist, dass Unternehmen die Anforderungen dieser Strategie verstehen und umsetzen.

WARUM IST DIE EUROPÄISCHE CYBERSTRATEGIE WICHTIG?

- **Schutz der digitalen Infrastruktur:** Ich lege großen Wert darauf, dass kritische Infrastrukturen, wie Energieversorgung, Gesundheitswesen und Verkehr, die für das tägliche Leben unerlässlich sind, geschützt werden.
- **Förderung von Innovation und Vertrauen:** Durch die Schaffung eines sicheren digitalen Umfelds fördere ich Innovation und stärke das Vertrauen der Bürger und Unternehmen in digitale Dienste.
- **Internationale Zusammenarbeit:** Ich unterstütze die Zusammenarbeit mit internationalen Partnern, um globale Cyberbedrohungen gemeinsam zu bekämpfen.

ENTWICKLUNGEN IM CYBER SECURITY-MARKT

Der Security-Markt entwickelt sich ständig weiter, um den sich ändernden Bedrohungen gerecht zu werden. In meiner Erfahrung sehe ich einen Trend hin zu integrierten Sicherheitslösungen, die mehrere Schutzebenen bieten.

ENTWICKLUNGEN, DIE DIE CYBERSICHERHEIT PRÄGEN WERDEN

Die ständige Weiterentwicklung der Cybersicherheit ist für uns nicht nur Herausforderung, sondern Inspiration – wir genießen und sind Teil dieser Dynamik. Die Bedrohungslandschaft verändert sich ständig, und es ist entscheidend, dass wir nicht nur auf aktuelle Herausforderungen reagieren, sondern auch einen Blick in die Zukunft werfen. In diesem letzten Artikel möchte ich einige der wichtigsten Zukunftsthemen beleuchten, darunter KI-Sicherheit, gesetzliches Monitoring, die europäische Cyberstrategie und die Entwicklungen im Cyber Security-Markt. Ich werde auch die Perspektive für Cyber Complete skizzieren.

4 WICHTIGE ENTWICKLUNGEN IM CYBER SECURITY-MARKT

1. ZERO TRUST ARCHITEKTUR:

Diese Sicherheitsstrategie basiert auf der Annahme, dass Bedrohungen sowohl innerhalb als auch außerhalb des Netzwerks existieren. Daher wird jedem Zugriff auf Unternehmensressourcen nur nach strenger Authentifizierung und Autorisierung gewährt. Dies minimiert das Risiko von Datenlecks und unbefugtem Zugriff.

2. CLOUD-SICHERHEIT: Mit der zunehmenden Verlagerung von Daten und Anwendungen in die Cloud investieren Unternehmen in Sicherheitslösungen, die speziell für Cloud-Umgebungen entwickelt wurden. Diese Lösungen bieten Schutz vor Datenverlust und unbefugtem Zugriff in einer zunehmend dezentralisierten IT-Infrastruktur.

3. ENDPOINT PROTECTION: Da Mitarbeiter zunehmend von verschiedenen Standorten aus arbeiten, ist der Schutz von Endgeräten wie Laptops und Smartphones wichtiger denn je. Moderne Endpoint Protection-Lösungen bieten umfassenden Schutz vor Malware, Phishing-Angriffen und anderen Bedrohungen, die auf mobile und entfernte Geräte abzielen.

4. MANAGED SECURITY SERVICES:

Viele Unternehmen entscheiden sich dafür, ihre Sicherheitsmaßnahmen an spezialisierte Dienstleister auszulagern. Diese Managed Security Service Provider (MSSPs) bieten Expertise und Ressourcen, um Sicherheitsstrategien zu optimieren und kontinuierlichen Schutz zu gewährleisten, ohne dass Unternehmen eigene, umfangreiche Sicherheitsinfrastrukturen aufbauen müssen.

PERSPEKTIVE FÜR CYBER COMPLETE

Für Cyber Complete sehe ich eine vielversprechende Zukunft. Ich bin bestrebt, an der Spitze der technologischen Entwick-

lungen zu bleiben und unseren Kunden innovative Sicherheitslösungen anzubieten.

MEINE VISION UND STRATEGIE

- **Fokus auf KI-Sicherheit:** Ich investiere in die Entwicklung von KI-gestützten Sicherheitslösungen, die Bedrohungen schneller erkennen und abwehren können.
- **Erweiterung der Compliance-Dienstleistungen:** Mit der zunehmenden Regulierung im Bereich Cybersicherheit biete ich umfassende Dienstleistungen an, um Unternehmen bei der Einhaltung gesetzlicher Vorschriften zu unterstützen.
- **Partnerschaften und Zusammenarbeit:** Durch die Zusammenarbeit mit führenden Technologieanbietern und Forschungseinrichtungen stelle ich sicher, dass unsere Kunden Zugang zu den neuesten Innovationen haben.
- **Bildung und Sensibilisierung:** Ich setze auf Schulungsprogramme, um das Bewusstsein für Cybersicherheit zu schärfen und unsere Kunden in die Lage zu versetzen, proaktiv auf Bedrohungen zu reagieren.

SCHLUSSFOLGERUNG

Die Zukunft der Cybersicherheit ist dynamisch und voller Herausforderungen. Themen wie die europäische Cyberstrategie und die Entwicklungen im Security-Markt werden in den kommenden Jahren von zentraler Bedeutung sein. In meiner Rolle bei Cyber Complete bin ich entschlossen, diese Herausforderungen anzugehen und unseren Kunden die bestmöglichen Lösungen zu bieten.

Gemeinsam können wir die Zukunft der Cybersicherheit gestalten und eine sichere digitale Welt schaffen.

Ihr Benjamin Richter & Team

33% SPAREN 4 MAL LESEN MAGAZIN + E-PAPER + NEWSLETTER

EIN JAHR LANG
DIE VOLLE PACKUNG:

BUSINESS PUNK

Das Magazin für alles, was in Wirtschaft und Lifestyle wichtig ist und wird. Für alle, die heute schon die Welt von morgen begreifen wollen. Hol dir jetzt die volle Ladung Inspiration.

KOMMT VERSANDKOSTENFREI!

4 Ausgaben bequem und pünktlich direkt nach Hause.

IMMER ZUERST

Einen Tag früher lesen als alle anderen.

AUCH DIGITAL

Du hast BUSINESS PUNK inklusive der digitalen Ausgabe immer dabei und liest wo und wann du willst.

NEWSLETTER

Im Abonnement mit dabei und immer dienstags und freitags: relevante Infos, die Dich weiterbringen – direkt aus der Redaktion.



DAS
BUSINESS-
LIFESTYLE-MAGAZIN
INKL. E-PAPER UND
NEWSLETTER:
45,00 €

(statt 67,96 € beim Kauf der einzelnen Ausgaben des Magazins)



SICHERE DIR GLEICH HIER ALLE VORTEILE:

BUSINESS-PUNK.COM/KOMBI

089 - 85 85 3879

1 Jahr BUSINESS PUNK (4 mal Magazin frei Haus + 4 mal E-Paper zur Nutzung auf mobilen Geräten + Bezug des zweimal pro Woche erscheinenden Newsletters).

Es besteht ein 14-tägiges Widerrufsrecht. Zahlungsziel: 14 Tage nach Rechnungserhalt. Alle Preisangaben inkl. MwSt. und Versand.

Anbieter des Abonnements ist die BUSINESS PUNK GMBH. Fulfillment, Betreuung und Abrechnung erfolgen durch Cover Service GmbH & Co. KG als leistenden Unternehmer.