Ausgabe 5

CM Magazin

MANAGED SERVICES - Im innovativen Fokus

Verhalten bei IT-Problemen

Ruhe bewahren & IT-Problem melden!

Lieber einmal mehr als einmal zu wenig Kontakt aufnehmen:

07243 99167-20
hilfe@connectingmedia.de

- Wer meldet den Vorfall?
- Weches IT-System ist betroffen?
- Wie haben Sie mit dem IT-System gearbeitet? Was haben Sie beobachtet?
- Wann ist das Ereignis eingetroffen?
- Wo befindet sich das betroffene IT-System? (Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Connecting Media

GANZHEITLICHE IT SECURITY LÖSUNGEN AUS EINER HAND

Eines der höchsten Gebote in Sachen IT und Cyber Security ist, die Schwachstellen der eigenen IT-Infrastruktur zu schließen. Doch wie soll etwas geschlossen und beseitigt werden, wenn man gar nicht genau absehen kann wo diese liegen oder in Zukunft liegen könnten?

Im Gespräch mit vielen Unternehmen zeigt sich immer wieder das Ausmaß des Problems und der dringende Handlungsbedarf. Wo liegt die Lösung? Wo der richtige Weg? Wie pflege ich zu sagen: „100% Sicherheit gibt es nicht“, aber man kann versuchen, möglichst nah heranzukommen. Und dafür gibt es viele und umfangreiche, aber auch bedarfsgerechte Lösungen sehr wohl “Made in Germany”. Ein Ansatz, der dabei nicht außer Acht gelassen werden darf, ist die ganzheitliche Betrachtung mit innovativem Fokus – ausgerichtet auf Lösungen, die auch zu Ihnen und Ihrem Unternehmen passen.

Ein Stück Hilfestellung für diese Aufgabe finden Sie u. a. in unserem Leitfaden ‚Ihr Weg zu IT Security im Unternehmen‘ (ab S. 24). Aber auch SecFried (S. 14) und das Security Audit (S. 16) stehen Ihnen dabei zur Seite. Ebenfalls mit im Gepäck: der spannende Artikel zur NIS-2-Richtlinie und dem Cyber Resilience Act sowie unser Interview zu künstlicher Intelligenz mit dem HDT-Journal.

Ihr Andreas Kunz
CEO & Founder, Connecting Media GmbH

CONNECTING MEDIA

Als Ihr Ansprechpartner für umfassende, sichere und digitale Lösungen in den Bereichen IT Service und IT Security sowie Datenschutz, schaffen wir es komplexe Sachverhalte einfach darzustellen und Ihre Anfragen lösungsorientiert umzusetzen. Durch ständigen Wissensaustausch und enge Zusammenarbeit mit validierten Lösungspartnern bieten wir Ihnen Lösungen mit dem höchsten Maß an Sicherheit und nach Ihren Voraussetzungen.

Connecting Media

INHALTSVERZEICHNIS

SEITE

Aus Gründen der besseren Lesbarkeit verwenden wir in den nachfolgenden Texten die männliche Form (generisches Maskulinum). Wir meinen immer alle Geschlechter im Sinne der Gleichbehandlung. Die verkürzte Sprachform hat redaktionelle Gründe und ist wertfrei.

Newsletter!
Registrieren Sie sich für die 'CM e-News' und bleiben Sie am Puls der Zeit in Sachen IT Security, Digitalisierung & Datenschutz:
www.connectingmedia.de/newsletter


Erleben Sie uns 24/7 in unserem
virtuellen Showroom.
Erleben statt nur sehen!
www.connectingmedia.de/showroom

MIT SICHERHEIT

Der rasante technologische Wandel und immer komplexer werdende IT-Systeme konfrontieren Unternehmer mit neuartigen Fragestellungen. Wer diese ungemein vielschichtigen Themenbereiche im Unternehmen aus eigener Kraft stemmen möchte, muss viel Zeit und Energie investieren, die dann an anderen wichtigen Stellen fehlen.

Connecting Media nimmt Ihnen diese Last von den Schultern und stellt Ihr Unternehmen in den Bereichen IT Security, IT Service und Datenschutz optimal für die Zukunft auf. Vom Stecker bis zum Nutzer vor dem Bildschirm wickeln wir Ihre IT-Projekte ab. Das können reine Infrastruktur-Projekte sein bis hin zu Schwachstellen-Checks und ganzen Sicherheitskonzepten.

Wir sind ein kleines aber hochspezialisiertes Team. Durch flache Hierarchien, kurze Wege und viel Raum für neue Ideen leben wir die Dynamik von der andere nur reden. Gestützt auf unsere langjährige Erfahrung bei internationalen Distributoren aus dem IT Security-Bereich und IT-Serviceanbietern wissen wir auf was es ankommt und wohin wir wollen. Dabei liegt unser Fokus nicht im Verkauf, sondern das passende Konzept zu finden, indem wir unseren Kunden wirklich aufmerksam zuhören und deren Bedenken ernstnehmen. In jedem Fachgebiet stehen Ihnen zertifizierte Experten zur Seite.

Dank unserer Experten und Partner können wir Ihnen ein Komplettpaket aus einer Hand bieten. Das garantiert einen reibungslosen Ablauf und minimiert Ihren eigenen Handlungsbedarf. So können Sie sich ganz auf den Ausbau und die Umsatzsteigerung Ihres Unternehmens konzentrieren – wir übernehmen für Sie den „lästigen“ Rest.

Unser komplettes Lösungs-Portfolio
finden Sie unter

www.connectingmedia.de/services

SERVICES

Managed IT Services
Mit unseren individuellen Managed Service-Bausteinen geben Sie Ihre IT-Tasks in erfahrene und vertrauensvolle Hände. So steht die Basis Ihres Unternehmens sicher da und entlastet die firmeneigenen Ressourcen.

Managed IT Security Services
Sie möchten IT-Sicherheitslücken nicht nur ins Blaue hinein beheben, sondern wirklich die Schwachstellen schließen, die für Ihr Unternehmen von Gefahr sind? Das erreichen wir mit Ihnen durch sogenannte Pentests innerhalb unseres www.secaud.it

STARK VERNETZT

CyberLago e.V.

Netzwerk der Digitalexperten in der internationalen Bodenseeregion und zentrale Anlaufstelle in allen Fragen rund um Digitalisierung, digitale Transformation und IT.

Cyberforum e.V.

Das größte regional aktive Hightech. Unternehmer.Netzwerk. in Europa. Vom Start-up und der Softwareschmiede über den erfahrenen Unternehmer und internationalen Informationstechnologie-Anbieter bis hin zu Forschungseinrichtungen und Universitäten. Eine Plattform für Networking als direkte Verbindung von Kompetenz, Business-Kontakten und Karriereaussichten.

German Mittelstand e.V.

Eine national und international anerkannte Marke. Wir tragen die DNA des ehrbaren Kaufmanns in uns und suchen international gleichgesinnte Unternehmerinnen und Unternehmer. Willkommen im Club des Next Generation Unternehmertum.

HubWerk01, Bruchsal

Ein lebendiger Ort im Zeichen des digitalen Wandels. Start-ups sowie auch große Unternehmen finden die idealen Flächen zum kreativen Arbeiten in kleinen Projektteams. Darüber hinaus vernetzt das HubWerk01 die regionale Wirtschaft gezielt miteinander, um den Austausch von Erfahrungen, Fachwissen und Expertise zu fördern und neue Möglichkeiten der Zusammenarbeit zu eröffnen.

MANAGED IT SERVICES

Managed IT Services (IT-Service-Management) bezeichnet die Auslagerung von IT-Management-Aufgaben an einen externen IT-Dienstleister mittels eines Service-Vertrag (Service Level Agreement – SLA). Hierbei übernimmt der IT-Dienstleister bestimmte Aufgaben, dies kann beinhalten:

- **Überwachung der IT-Infrastruktur**
- **Wartung von Hard- und Software**
- **Administration von Datenbanken und Netzwerken**
- **Management von IT-Sicherheit**
- **Unterstützung bei IT-Projekten.**

MANAGED SECURITY SERVICES

Managed Security Services sind eine spezialisierte Form von Managed IT Services, bei der ein IT-Sicherheitsdienstleister die Verantwortung für die Überwachung, Wartung und den Schutz der IT-Sicherheitsinfrastruktur eines Unternehmens übernimmt. Es umfasst eine Vielzahl von Sicherheitsdienstleistungen, die aus der Ferne oder vor Ort im Unternehmen bereitgestellt werden können:

- **Netzwerk-, Cloud- und Endpoinsicherheit**
- **Identitäts- und Zugriffsmanagement**
- **Compliance- und Risikomanagement**
- **Bedrohungs-und Schwachstellenmanagement**
- **Incident Response und Forensik.**

Patrick Niendorf
IT-Abteilung
Bauck GmbH

Um die Vorgaben unserer Cyberversicherung erfüllen zu können benötigten wir einen IST-Zustand unserer Systeme und Netze, sowie einen Überblick der vorhandenen bzw. möglichen Einfallstore. Durch das Security Audit mit Connecting Media wurde eine solide Grundlage für die versicherungstechnische Absicherung geschaffen und die Weichen gelegt, um weitere fundierte Entscheidungen für unser Unternehmen treffen zu können.

Damit ist es aber noch nicht getan, sondern die Zusammenarbeit fängt hier erst an. Mit dem Connecting Media Control Center (CMCC) erhalten wir für unser laufendes Geschäft einen Baukasten für einfache, zuverlässige und umfassende Kontrolle unseres Netzwerks. Auf die weitere Security Unterstützung von Connecting Media greifen wir hier vertrauensvoll zurück.

UNSERE SERVICES

Mit unserem Managed Security Services bieten wir Ihnen eine schnelle Reaktionszeit auf Sicherheitsvorfälle, kontinuierliche Überwachung rund um die Uhr sowie einen umfassenden Schutz vor Cyberangriffen. Zudem können Sie durch die Auslagerung von internen Ressourcen sparen und die Compliance mit den geltenden Datenschutz- und Sicherheitsbestimmungen vereinbaren.

Profitieren Sie von unserer Expertise und Erfahrung und entlasten Sie durch die Auslagerung von IT-Aufgaben Ihre eigenen Mitarbeiter. Rücken Sie die Kernkompetenzen einzelner Abteilungen oder des gesamten Unternehmens wieder in den Mittelpunkt.

www.connectingmedia.de/services

CONNECTING MEDIA - SERVICE PAKETE

Mit unseren individuell angepassten Service Bausteinen erhalten Sie genau den Service den Sie benötigen:

Security - Umfassende Lösung zur Überwachung und Absicherung Ihrer IT-Geräte.

Sie erhalten einen kompletten Security-Scan Ihrer gesamten IT. Erkennung Sie Sicherheitslücken (CVE-Scan) und erhalten Sie Verhaltensanalyse von Netzwerk-Angriffen (Intrusion Detection System), Best-Practise Security-Konfigurationen u.v.m.

Inventarisierung - Dauerhaftes Scanning Ihrer IT-Umgebung .

Schaffen Sie ein Live-Abbild Ihrer IT-Infrastruktur aller IP-kommunizierenden Geräte. Sowie Automatische Erkennung und unbegrenzte IP-Inventarisierung aller Netzwerkgeräte, sowie deren Klassifizierung.

Patchmanagement - Endgeräte (Clients und Server) stets auf dem aktuellen Stand.

Über den selbst gehosteten Paketmanager werden Windows-Updates und 3rd Party-Updates auf Ihre Systeme ausgespielt. Sie können die Software dabei automatisiert verteilen oder userbasiert über das Softwarekiosk selbst.

Netzwerkkontrolle - Zentrale Steuerung des gesamten Netzwerks.

Alle Netzwerkgeräte werden zentral überwacht und administriert. Updates und Änderungen können jederzeit verwaltet und umgesetzt werden. Bei der Warnmeldung einer Überlastung, lassen sich die „Verursacher“ mit der Einzelgeräte-Ansicht problemlos entlarven und die Fehler gezielt und unverzüglich beheben.

Benutzer Control Center - Selbsterklärendes Informationsportal für Ihre Mitarbeitenden.

Geben Sie Ihren Mitarbeitern ein einfach zu bedienendes Softwarekiosk an die Hand mit dem diese sich einen Überblick über Ihre Geräte, die darauf installierten Programme und ausstehende Updates verschaffen. Außerdem können Benutzer bei Problemen direkt Kontakt aufnehmen und die Fernwartung einleiten.

Kundenportal - Gezielte Schulungen halten Ihre Mitarbeiter fit.

Auch veröffentlichen wir dort Trainingsvideos zu Awareness- und Datenschutzschulungen oder aufgezeichnete Webinare von spannenden Sessions, die wir auf Events oder mit unseren Lösungspartnern erarbeitet haben.

DIE CM CLOUD MIT HÖCHSTEN STANDARDS

Eine private Cloud-Infrastruktur bietet zahlreiche Vorteile gegenüber öffentlichen Cloud-Diensten. Zum einen behalten Unternehmen die volle Kontrolle über ihre Daten und Anwendungen und können sicherstellen, dass ihre Compliance-Anforderungen erfüllt werden. Zum anderen bietet eine private Cloud-Infrastruktur höhere Sicherheitsstandards und Schutz vor Datenverlusten durch eine lokale Datenspeicherung.

Im Hochverfügbarkeitsrechenzentrum der Telemaxx in Karlsruhe stellt Connecting Media, eine eigene private Cloud-Infrastruktur zur Verfügung. Diese verfügt über Zertifizierungen nach ISO 27001 und TÜVIT EN50600 Verfügbarkeitsklasse 3. Mit dieser Infrastruktur können Kunden ihre Daten und Anwendungen in einer sicheren und zuverlässigen Umgebung hosten, die von Connecting Media selbst betrieben und verwaltet wird.

Nur die Ressourcen zahlen, die Sie nutzen

Außerdem bieten wir eine skalierbare Infrastruktur, die es Unternehmen ermöglicht, schnell und flexibel auf Änderungen in der Geschäftsdynamik zu reagieren. Kunden können Ressourcen und Kapazitäten nach Bedarf anpassen und zahlen nur für die Ressourcen, die sie tatsächlich nutzen.

Mit der Nutzung der privaten Cloud-Infrastruktur steigern Sie die Effizienz und Produktivität Ihres Unternehmens und stellen gleichzeitig sicher, dass Ihre Daten sicher und geschützt sind. Mit einem engagierten Support-Team, das rund um die Uhr verfügbar ist, können Sie sicher sein, dass Ihre IT-Infrastruktur jederzeit betreut und gewartet wird.

Zu unserem Leistungsspektrum zählen:

Pentest as a Service (PaaS)
Permanentes Schwachstellenscanning & Pentesting Ihrer IT-Infrastruktur

Infrastruktur as a Service (IaaS)
Hosting und Betrieb Ihrer IT

Security as a Service (SaaS)
Hosting und Betrieb Ihrer Sicherheitslösungen

Backup as a Service (BaaS)
Skalierbares backup Ihrer Daten und Geräte

Monitoring as a service (MaaS)
Permanente Überwachung der Verfügbarkeit Ihrer IT-Infrastruktur

Security Operation Center (SOCaaS)
Ihre Sicherheitsleitstelle zur permanenten Überwachung Ihres Unternehmens

KUNDENSTIMMEN

Christian Körber & Frank Martin
Geschäftsführung
KM-TGA GmbH

Unsere erste Zusammenarbeit mit Connecting Media betraf die Grundeinrichtung unseres neu gegründeten Planungsbüros. Sprich vom Server, Arbeitsplatzrechner und der Telefonanlage über Internetverträge, Handyverträge, die Smart Home-Einrichtung hin zur Einrichtung der Programme sowie die Erarbeitung eines Backup- und Schutzkonzepts. Nachdem wir intensiv mit Connecting Media zusammengearbeitet haben und diese uns ein super Rundumangebot geliefert haben, lief in wirklich kürzester Zeit die komplette IT. Großartige Tipps zur Erstellung unserer Homepage und sonstige Infos in Bezug auf die IT waren für Connecting Media selbstverständlich. Besonders hervorzuheben sind die freundlichen Mitarbeiter und deren Fachkompetenz. Wir bedanken uns herzlichst für diese großartige Arbeit und empfehlen Connecting Media jederzeit weiter.

Dr. Patrick Näher
Facharzt für Allgemeinmedizin,
Sportmedizin, Naturheilverfahren,
Chirotherapie, Akupunktur
Gemeinschaftspraxis Claudia Obert & Patrick Näher

Die neue Gesetzeslage (Implementierung der DSGVO) hatte einige Auswirkungen auf uns als Arztpraxis, vor allem mit der Herausforderung, dass Sie so nicht für uns gemacht war. Es gab unzählige unabhängige Schreiben und Dokumente von verschiedenen Stellen, aber es war recht unübersichtlich und keiner wusste genau was Sache ist. Mit Hilfe von Connecting Media konnte ich meine Skepsis überwinden und mussten kein Fachchinesisch lernen. Die neue Sachlage und Notwendigkeiten wurden mir fachmännisch aber vor allem verständlich vermittelt. Mit der Beratung und Betreuung von Connecting Media habe ich keine Ängste und Sorgen mehr in dieser Hinsicht und fühle mich rechtlich sicher aufgestellt.

Ingo Müller
Geschäftsführer
Autohaus Müller

Bevor wir von Connecting Media betreut wurden, hatten wir schon langjährig mit einem All-in-One Servicepartner zusammen gearbeitet, kamen aber an den Punkt, das wir nicht mehr so zufrieden waren. Für uns der richtige Zeitpunkt einen Wechsel zu haben. Über das private Umfeld kamen wir dann zu Connecting Media. Gestartet haben wir die Zusammenarbeit mit der Umstellung unserer IT-Umgebung, welche durch Andreas Kunz und sein Technik-Team sehr gut umgesetzt wurde.

Meine Mitarbeiter und ich schätzen sehr die Erreichbarkeit und den schnellen Service des Supports auch vor Ort in unserem Autohaus. Dadurch gibt es viel Entlastung für das gesamte Team und keine Angst mehr vor IT-Ausfällen, welche unseren Arbeitsablauf behindern würden. Einen Ansprechpartner für alle IT-Belage zu haben ist äußerst wichtig für mich und den haben wir mit Connecting Media gefunden.

Steffen Heil
Vorstand
Auerbach Stiftung

Als gemeinsames Mitglied des HubWerk01 in Bruchsal war es nur eine Frage der Zeit, dass wir uns über den Weg laufen würden und für uns war es von der IT-technischen Sicht der perfekte Zeitpunkt dafür. Wir standen vor ein paar zentralen Fragestellungen: Wie sichern wir unser WLan, mit dem auch Kinder und Jugendliche arbeiten? Wie sichern wir unsere Daten auf einfache Art und Weise?

Connecting Media gestaltete mit uns den Netzwerkumbau und -ausbau aktiv mit und punktete durch die schnelle und zuverlässige sowie kompetente Umsetzung. Nun sind unsere Netzwerkanforderungen einfach und umfänglich gelöst.

Auch in Sachen digitaler Zusammenarbeit konnten wir mit der Hilfe von Connecting Media wieder einen Schritt machen mit der Einführung und dem Management der O365 Suite. Auf Basis dieser Erfahrung, lassen wir zukünftig unser IT-Monitoring inklusive des Patchmanagement über Connecting Media laufen. Wir freuen uns weiterhin für die Betreuung unserer IT auf Connecting Media zählen zu können. Für uns ein rundum Sorglos-Paket.

WEITERE KUNDENSTIMMEN FINDEN SIE AUCH AUF GOOGLE.

Sie möchten auch guten Service weitergeben, dann schreiben Sie über Ihre Erfahrung mit unserem Service und persönlichen Kontakt eine Google-Rezension.

Sicher wie SecFried

Jede Geschichte hat eine wahre Analogie.

Wie aus Siegfried dem Drachentöter SecFried wurde und Sie Ihr Unternehmen ganzheitlich digital sicher aufstellen.

Kennen Sie Ihr digitales Lindenblatt?

Die Angriffsflächen und Gefahren von “Siegfried dem Drachentöter” aus der Nibelungensage sind so aktuell wie jeher. Er hat sich sicher geglaubt und wurde durch seine Schwachstelle zu Fall gebracht.

Wo liegt Ihr ‚digitales‘ Lindenblatt?

Mit diesen Bausteinen aus technischen, organisatorischen und menschlichen Faktoren, stellen Sie Ihr Unternehmen ganzheitlich sicher auf:

SECURITY AUDIT

Externer Scan

Alle externen IP-Adressen der Firma | Darknet Crawling nach geleakten Accounts/ Informationen | BSI-Kriterien & DSGVO-Check der Webseite

Interner Scan

4x /24er Netze | Erstellung einer Asset Map Ihrer IP-Geräte | Pentest und Schwachstellenscan | Detaillierter Bericht mit Handlungsempfehlungen

COMPLIANCE SCAN

Fragenkatalog zur organisatorischen Sicherheit

AWARENESS

30 Tage unsere immersive Awareness-Plattform

Security Audit

SICHERHEIT DURCH SICHTBARKEIT!

HÄTTEN SIE IHN ENTDECKT?

Sicherheitslücken entstehen oft durch veraltete Software oder fehlerhafte Konfigurationen. Das sind offene Türen für Angreifer, die Sie schließen müssen, um sich gegen unbefugte Zugriffe abzusichern.

Erkennen Sie Schwachstellen, bevor diese ausgenutzt werden. Mit unserer vollumfänglichen, teilautomatisierten Schwachstellenüberprüfung bieten wir Ihnen eine einmalige oder auch regelmäßige Analyse Ihres IT-Sicherheitszustandes.

Neutral, objektiv und verständlich.

SECURITY AUDIT

Externer Scan

Alle externen IP-Adressen der Firma | Darknet Crawling nach geleakten Accounts/Informationen | BSI-Kriterien & DSGVO-Check der Webseite

Interner Scan

4x /24er Netze | Erstellung einer Asset Map Ihrer IP-Geräte | Pentest und Schwachstellenscan | Detaillierter Bericht mit Handlungsempfehlungen

ZUBUCHBARE LEISTUNGEN

- Ausführliche Reportbesprechung
- Detaillierte Handlungsempfehlungen
- Weitere 4x /24er Netze für den internen Scan
- Unterstützung bei der Behebung aufgedeckter Schwachstellen

IHRE VORTEILE

- Planung, Durchführung & Auswertung durch unsere IT Security Spezialisten
- Made in Germany, DSGVO-konform (vollständige Löschung aller Daten nach der Reporterstellung)
- Keine gebundenen Ressourcen, keine langfristigen Verpflichtungen

Monika Sanders
Financial Planner & Prokuristin
fintag Finanzdienstleistungs- und Treuhand AG

Wir stehen vor der Herausforderung, dass unsere IT von internen sowie externen Personen betreut wird, mit der Unterstützung von Connecting Media konnten wir mit dem Security Audit die offenen Türen und Gefahren erkennen. Am Anfang der Zusammenarbeit war ich neugierig, wie ich unsere IT extern testen lassen kann. Davor war mir nicht bekannt, dass diese Möglichkeit als Geschäftsfeld existiert. Für mein Unternehmen war das Security Audit wichtig, damit wir gewährleisten können das die sensiblen Daten, mit denen wir als Finanzdienstleister tagtäglich zu tun haben, auch abgesichert sind.

Nachdem wir intensiv mit Connecting Media zusammengearbeitet haben, können wir nun an den Ergebnissen des Security Audits arbeiten, sodass wir sehr gut abgesichert sind – und diese Sicherheit auch unseren Kunden kommunizieren. Auch reduzieren wir dadurch das Risiko von IT Security Vorfällen und den damit verbundenen Kosten wegen Betriebsausfall. Connecting Media hat die Informationen aus dem Security Audit und die Situation in der wir uns befinden sehr verständlich aufbereitet, auch für Mitarbeiter, deren Schwerpunkt nicht in der IT liegt. Die Offenheit und Zuverlässigkeit in der Kommunikation war ausgezeichnet.

Sonja Gumnior
Leitung Qualitäts-
/Projektmanagement
Cosack GmbH & Co. KG

Die Zusammenarbeit mit Connecting Media war einer der wertvollen Kontakte, die sich aus der Seminarveranstaltung ‚sichere IT-Infrastruktur' des FFI - Fachverband Faltschachtel-Industrie, ergeben hat. Mit der Durchführung des Security Audit wurden uns die aktuellsten Schwachstellen aufgezeigt und eine ganz andere und vollumfängliche Sicht auf unsere IT-Landschaft und deren Stand der Sicherheit eröffnet. Jetzt geht es an die schnelle Behebung dieser Stellschrauben, wir freuen uns, dass wir hier weiterhin die Projektunterstützung und das Projektmanagement von Connecting Media erhalten.

SERVICECockpit

SIEM, Monitoring und ISMS für den Mittelstand

Je abhängiger ein Unternehmen von seiner IT-Infrastruktur wird, desto weitreichender sind die Folgen bei einem Ausfall. Und je mehr interne, schützenswerte Informationen auf digitaler Ebene verfügbar werden, desto größer ist die Gefahr von Datenlecks oder Cyberangriffen. Insbesondere mittelständische Unternehmen geraten häufig in den Fokus von Kriminellen. Denn häufig fehlen diesen Firmen das Risikobewusstsein oder auch die finanziellen oder personellen Ressourcen, um die eigenen Sicherheitsstandards der rasanten digitalen Entwicklung mit immer komplexer werdenden Systemen anzupassen.

Ohne ganzheitlichen Ansatz geht es nicht

Mit einem integrativen Ansatz und einem umfassenden Blick auf die IT-Systeme lässt sich dies lösen. Es soll dabei nicht ein weiteres Datensilo entstehen, sondern vorhandene Systeme und Informationen lesbar und bedienbar machen. Bei einer Fehleranalyse kann so zielgerichtet gearbeitet werden und alles in einer Oberfläche zentral vereinen.

Wer ein Informationssicherheitsmanagementsystem (ISMS) eingeführt hat, muss sich nicht länger um seine Daten sorgen, weiß das Unternehmen für zukünftige Entwicklungen gestärkt und kann sich mit seinen hohen Sicherheitsstandards im Idealfall auch noch vom Wettbewerb abheben. Für das ISMS gilt es dennoch, permanent eine Vielzahl von Hard- und Softwarekomponenten, Netzwerken, Cloud-Lösungen und weiteren Bausteinen der firmeneigenen IT zu kontrollieren.

Das ServiceCockpit

„Mit unserem ISMS der nächsten Generation hat der Nutzer alles ganz einfach im Blick“, bringt CEO Andreas Kunz das Produkt auf den Punkt. Das ServiceCockpit fasst dazu unzählige Datenquellen zusammen, bereitet sie nutzerfreundlich auf und vereint sie unter einer übersichtlichen Benutzeroberfläche. Mit dem Entwicklungsstandort in Deutschland spiegelt das ServiceCockpit ebenfalls die hiesigen Datenschutzrichtlinien wider. So werden Informationssicherheit und Gefahrenabwehr für Ihr Unternehmen zum Kinderspiel.

Ihre Vorteile im Überblick

- **Konfigurierbare Alarmierungen**
- **Managed Security**
- **IoT-Kompatibilität**
- **Integration von Cloud-Systemen**
- **Skalierbarkeit**
- **Entlastung von Ressourcen**
- **Erweiterbarkeit**

Lückenlose Überwachung und einfache System-Inventarisierung

Das ServiceCockpit bildet beliebig viele Komponenten der IT-Infrastruktur Ihres Unternehmens unter einer übersichtlichen Oberfläche ab und integriert sich perfekt in die bestehende Systemlandschaft. So behalten Sie auch bei komplexen Systemen immer die Kontrolle.

Office 365

Mit dieser Integration konsumieren wir alle Alerts & Events zum Betrieb Ihrer M365 Dienste.

ENGINSIGHT

Diese Integration verwandelt das Service-Cockpit in einen virtuellen Hacker und scannt Ihr Unternehmen nach Schwachstellen durch Pentests.

PAESSLER PRTG NETWORK MONITOR

Zentralisierung Ihre PRTG Sensoren und PRTG Events.

SOPHOS

Alerts Ihrer Sophos Central sowie Security Stati Ihrer Sophos gemanagten Geräte werden zentralisiert.

riverbird

Integration von Device Informationen, Asset Management und Alerting.

';--have i been pwned?

Prüfung Ihrer Firmen E-Mail Accounts nach Password Breaches.

Offensity by | A1 Digital

Die durch Offensity erstellten Scans und gefundene CVEs werden ins CMSC integriert.

Nagios

Der Nagios Agent kann über das CMSC zentral ausgerollt werden und somit die gängigen Windows / Unix Checks zum Monitoring benutzt werden.

Verfügbarkeit der von Ihnen betriebenen Webserver und Zertifikatsmonitoring Ihrer Webdienste.

Einfache Netzwerkscans nach freien IP-Adressen und Verfügbarkeit Ihrer Geräte per ICMP.

REST API

Mit der REST API können Sie die Daten des ServiceCockpits jederzeit mit anderen Werkzeugen teilen und weiterverarbeiten.

Sie haben weitere Systeme, die über eine REST-API verfügen, aber nicht aufgelistet sind?

Sprechen Sie uns an und wir entwickeln einen individuellen Connector für Sie.

SERVICECockpit

ERLEBEN SIE ES SELBST!

Weitere Informationen sowie die Terminvereinbarung zum kostenfreien Demotermin mit 14 Tage Teststellung finden Sie unter:

www.ServiceCockpit.io
07243 99167-00
vertrieb@connectingmedia.de

Die Kombination

Praxisnahe und effiziente Cybersecurity-Plattform aus Deutschland für mittelständische Unternehmen, KRITIS und öffentliche Träger. Eine einmalige Kombination aus Angriff und Verteidigung

ENGINSIGHT

Monitoring für den Mittelstand
Das ServiceCockpit fasst unzählige Datenquellen zusammen, bereitet sie benutzerfreundlich auf und vereint sie unter einer übersichtlichen Benutzeroberfläche. So werden Informationssicherheit und Gefahrenabwehr für Ihr Unternehmen zum Kinderspiel.

SERVICECockpit

LÖSUNGSPARTNER
Connecting Media GmbH

Ansprechpartner für umfassende sichere und digitale Lösungen in den Bereichen IT Service, IT Security und Datenschutz

Andreas Kunz
Geschäftsführer

LÖSUNGSANWENDER
Stadt Ettlingen

Eine Stadt von hoher Lebensqualität und exzellenter Infrastruktur im Albtal zwischen Nordschwarzwald und Rhein.

Oliver Hermann
Leiter IuK-Abteilung

Die Herausforderung

Wir wollten aus organisatorisch-technischen Gründen weg von einem Produkt-Sammelsurium in unserer IT. Dabei standen diese Fragestellungen auf der Agenda:

- Was ist unser Status quo? Wo stehen wir gerade?
- Wo lauern die wirklichen Gefahren?
- Wie steht es um das Thema IT-Sicherheit?

Durch viele Impulse u. a. durch Gespräche und Events von Connecting Media GmbH, kamen wir zur Überzeugung, dass wir unsere Maßnahmen im Bereich IT-Sicherheit weiter optimieren müssen.

Die Lösung sollte nicht noch mehr Arbeit verursachen, sondern verständlich und zielorientiert sein. Ein Anspruch war es zudem, möglichst deutsche Hersteller zu favorisieren, sofern die Anforderungen und die Innovationskraft des Unternehmens gegeben sind.

Mit dem Security Audit können wir genau diese Themen angehen und erhalten Sicherheit durch Sichtbarkeit. Durch teilautomatisierte Schwachstellenscans konnten wir die Lücken aufdecken, die wir schützen müssen. Doch wie wird dies in einer Kommune implementiert, in der es weder dedizierte Security Consultants gibt oder gar ein Security Operation Center (SOC)?

Die Lösung

In engem Austausch mit der Connecting Media GmbH, wurde die Test-Engine der Firma Enginsight als passende Lösung evaluiert. Mittels der Asset-Erfassung und den teilautomatisierten Pentests, erhalten wir alles lesbar aufbereitet, was wir brauchen, um Systemrisiken bewerten und gezielt Maßnahmen einleiten zu können. Mit Software-Agents lässt sich neben Sicherheits-ereignissen auch die Verfügbarkeit und Performance überwachen. Die Überwachung von selbst betriebenen Webapplikationen und automatisierten Prüfungen nach BSI runden für uns diese Lösung wunderbar ab.

Worin hat dieses Produkt gepunktet?

Neben dem einfachen Roll-out und der Datenaufbereitung in deutscher Sprache punktet die Lösung mit dem Erhalten von direkten Handlungsempfehlungen und möglichen Konfigurationsverbesserungen für Hosts. Einen weiteren Pluspunkt bietet die Lösung durch die Kombination des hauseigenen Produkts von Connecting Media GmbH, dem ServiceCockpit. So konnte das zentrale Logging und Alerting komplett integriert werden und wir erhalten alles in einer benutzerfreundlichen Übersicht. Dies erspart uns nicht nur viel Zeit, sondern gibt uns die Gewissheit und Absicherung, dass keine wichtigen Informationen untergehen und wir uns eine Flanke unbemerkt öffnen.

LEITFADEN

Der Weg zur IT Security in Ihrem Unternehmen

Sichere Rahmenbedingungen sind die Basis aller Digitalisierungsvorhaben Ihres Unternehmens. Durch den intensiv erlebten Digitalisierungsboom der letzten Jahre nehmen nicht nur die völlig neuen Möglichkeiten exponentiell zu, sondern geradezu im Gleichschritt auch die Gefahren. Das Thema IT Security ist mittler- weile nicht nur ein Nischenthema, das für den „Mittelständler“ weit weg ist.

Spätestens durch die ständige Medienpräsenz von Hackerangriffen, lahmgelegten Firmen und Erpressungsgelder in Millionenhöhe im Jahre 2022, ist nun umso mehr bewusst geworden, dass hier dringender Nachholbedarf besteht.

Mit diesem Leitfaden möchten wir aus Ihnen keinen Security Experten machen, sondern unsere Erfahrung der letzten 20 Jahre aus nationalen und internationalen IT Security Projekten teilen.

Alle Leitfäden und Fachartikel zu diesem Thema haben einen gemeinsamen Konsens:

SIE als CHEF sind die wichtigste Person, wenn es um das Thema Cybersicherheit im Unternehmen geht.

Sie entscheiden nicht nur, sondern Sie sind auch am Ende die Person, die Verantwortung für dieses Thema übernehmen muss.

Der Leitfaden ist demnach so aufbereitet, dass der Blickwinkel auf den Unternehmer dem Chef liegt. Denn so wie Sie Ihr Geschäft führen; sich täglich neu erfinden, neuen Herausforderungen entgegenblicken und kreative neue Ansätze entwickeln, ist auch die Basis, die Sie für eine Sicherheitskultur im Unternehmen benötigen. Wir haben Ihnen dieses Thema so zugänglich wie möglich aufbereitet, damit Sie umgehend mit den ersten Schritten in die Umsetzung starten können.

IT Security bleibt nicht stehen, sie ändert sich täglich.

Bausteine einer Sicherheitskultur

Wie bei vielen unternehmerischen Entscheidungen und Tätigkeiten ist es auch in Bezug auf IT und Cybersicherheit wichtig gewisse Grundbausteine mit einer klaren Definition festzulegen. Auf diese sollten Sie keineswegs verzichten, da diese über Erfolg oder Misserfolg Ihrer Sicherheitskultur entscheiden werden. Denn setzen Sie hier Ihre Prioritäten falsch, nützen Ihnen die teuersten Investitionen in Sicherheitsprodukte nichts.

Ihre Assets

Ihre Assets sind physikalische oder digitale Geräte/Systeme, die in Ihrem Unternehmen geschützt werden müssen und/oder deren Ausfall Sie auf keinen Fall riskieren wollen.

Es kann sich hier zum Beispiel um die Internetleitung handeln, denn fällt diese aus, können Ihre Mitarbeiter nicht mehr arbeiten, Services und Systeme wie z.B. ein Web-shop ist nicht mehr erreichbar, Industrieanlagen oder die gesamte Produktion stehen still. Damit verlieren Sie plötzlich minütlich bares Geld!

Rechtliche Vorgaben

IT Sicherheit darf nicht nur von der technischen Seite betrachtet werden. Je nach Firmensitz und Betrieb Ihrer Systeme, gibt es bestimmte Regeln, die von staatlicher und behördlicher Seite zu beachten sind. Hier finden Sie die wichtigsten Gesetze:

- *Europäische Datenschutz-Grundverordnung (EU-DSGVO) – Regelt die Handhabung zur Erfassung und Verarbeitung personenbezogener Daten*
- *Arbeitsschutzgesetz – Regeln für den Arbeitsalltag Ihrer Mitarbeiter, wichtig Transparenz sicherstellen.*
- *Telemediengesetz (TMG) - Gilt für alle elektronischen Informations- und Kommunikationsdienste*
- *Bundesdatenschutzgesetzt (BDSG-neu) - Konkretisierung und Ergänzung zur Europäischen Datenschutz-Grundverordnung (EU-DSGVO)*
- *IT Security Gesetz 2.0 - Zur Erhöhung der Sicherheit informationstechnischer Systeme*

Lassen Sie branchenspezifische Richtlinien nicht außer Acht. Diese sind allerdings in die Betrachtung nicht mit einbezogen. Wir empfehlen Ihnen sich unbedingt über die spezifischen Rahmenbedingungen Ihrer Branche zu informieren.

Ihre Mitarbeiter

Technische Mittel können nur bis zu einem bestimmten Grad die Informationssicherheit gewährleisten, u.a. weil technischer Schutz oft reaktiv ist. Der Mensch dagegen kann proaktiv handeln, vorausgesetzt, er ist durch Informationen und Kompetenzaufbau über Informationssicherheit entsprechend sensibilisiert.

Um Mitarbeiter zur „menschlichen Firewall“ zu entwickeln, ist es notwendig, potenzielle Gefahren und deren mögliche Folgen zu verdeutlichen, und die Belegschaft in Mitverantwortung im Hinblick auf die Informationssicherheit zu nehmen. Dies gelingt, wenn Vorgesetzte das Thema zur Chefsache machen.

Fördern Sie den Kompetenzerwerb, etwa durch Motivationsmittel, Schulungen und Informationsveranstaltungen. Wer Commitment zeigt und mit gutem Vorbild vorangeht, ist glaubwürdig und darf auch Commitment erwarten.

Definition Informationssicherheit

Der Begriff Informationssicherheit beschreibt den Schutz von Informationswerten nach mindestens drei Schutzzielen:

Vertraulichkeit	***Integrität***	***Verfügbarkeit***
Informationen sind nur berechtigten Personen zugänglich	Informationen sind vor unrechtmäßiger oder außerplanmäßiger Veränderung gesichert	Informationen sind zu jeder Zeit verfügbar und können bei Problemen wiederhergestellt werden.

Wenn Unternehmen Maßnahmen zur Informationssicherheit implementieren, sollten diese immer mindestens eines dieser Ziele verfolgen.

Vertraulichkeit

Die Herleitung für dieses Grundprinzip ist gut aus dem Alltag abzuleiten. Die Definition ist einem sofort be- wusst, denn die Vertraulichkeit von Informationen bedeutet diese von unbefugten Zugriff Dritter zu schützen. Um dies umsetzen zu können, muss einem bewusst sein wer zum Kreis befugter Personen gehört.

Zu Maßnahmen, die der Vertraulichkeit von Informationen dienen, gehören:

- Verschlüsselung von Daten
- Zugangssteuerung
- Physische Sicherheit und Umgebungssicherheit
- Betriebssicherheit
- Kommunikationssicherheit

Verfügbarkeit

Was nutzen vertraulich behandelte, integre Daten, wenn Nutzer nicht in dem Moment an sie herankommen, in dem sie benötigt werden? Beim Schutzziel der Verfügbarkeit geht es darum, die technologische Infrastruktur aufzubauen, die Daten und Informationen verfügbar machen. Oder deutlicher ausgedrückt: Systemausfälle zu verhindern. Gehen Daten doch einmal verloren, ist es ebenfalls Aufgabe der Informationssicherheit, den Betriebszustand so schnell wie möglich wiederherzustellen – zum Beispiel durch Backups.

Zu Maßnahmen, die der Verfügbarkeit von Informationen dienen, gehören:

- Risikoanalyse
- Anschaffung, Entwicklung und Instandhalten von Systemen
- Management von Informationssicherheitsvorfällen
- Betriebliches Kontinuitätsmanagement
- Kommunikationssicherheit

Integrität

Auch hier wieder der Blick in den Alltag: Personen, die man als integer bezeichnet, sind verlässlich! Beziehen wir das nun auf die Integrität von Daten und Informationen, ist gemeint, dass sie sich nicht unbemerkt oder unzulässig verändern lassen und somit immer korrekt und verlässlich bereitgestellt werden. In gewisser Weise spielt auch hier die Vertraulichkeit mit hineinalso der Schutz vor unbefugtem Zugriff. Doch Integrität meint vor allem den Schutz vor unbemerkten Veränderungen. Oft passieren diese weniger durch Menschen und mehr durch fehlerhafte Systeme und Prozesse.

Zu Maßnahmen, die der Integrität von Informationen dienen, gehören:

- Zugangssteuerung
- Management der Werte
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Steuerung und Überwachung des Datenflusses
- Zugriffssteuerungen

Deutschland • Digital • Sicher • BSI

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online - Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund **116,6 Millionen** zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

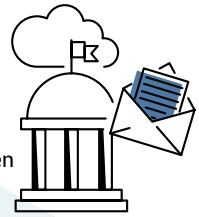
20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem Zuwachs von 10% gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

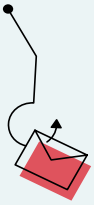


78.000

neue Webseiten wurden wegen enthal tener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichts-zeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.



90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Quelle: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Grundlegende Gefahren für die Informationssicherheit

Welche Gefahren sehen Sie, denen Informationswerte ausgesetzt sind?

Gängige Antworten: Cyber-Attacken, organisierte Kriminalität und Spionage.

Und damit trifft man voll ins Schwarze. Nach einer repräsentativen gesamtwirtschaftlichen Erhebung des Branchenverbandes Bitkom e.V. lag der Schaden durch Diebstahl, Spionage oder Sabotage bei deutschen Unternehmen im Jahr 2022 bei 203 Milliarden Euro und damit leicht unter dem Rekordjahr 2021 (223 Milliarden Euro). Im Vergleichszeitraum 2018/2019 wurde ein Anstieg von nur 103 Milliarden Euro verzeichnet. Neun von zehn Unternehmen waren nach Angaben der Bitkom e.V. direkt von Cyber-Angriffen und somit betroffen von Datendiebstahl, Spionage und Sabotage.

Informationen werden nicht ausschließlich von digitalen Angreifern mit böswilligen Absichten bedroht. Auch die eigenen Mitarbeiter könnenmutwillig oder versehentlicheine Gefahr für die Informationssicherheit darstellen, genauso wie fehlerhafte physische wie digitale Systeme, Prozesse und physische Bedrohungen durch Naturgewalten. Diese vier Gefahrenherde können sauber voneinander getrennt und entsprechende Maßnahmen zur Behebung definiert werden.

Physische Gefahren

Dass ein Rechenzentrum durch Feuer, Wasser und andere Naturgewalten beschädigt wird, kann nie zu 100% ausgeschlossen werden und daher sollten Sie dies bei der Bewertung der Informationssicherheit Ihrer IT immer mit berücksichtigen. Man spricht oft in der Fachliteratur und in Managementsystem vom sogenannten betrieblichen Kontinuitätsmanagement.

Faktor Mensch

Unachtsamkeit und unzureichend geschulte Mitarbeiter zählen laut einer Studie von KPMG (2019) zu den meistgenannten Faktoren, die Cyberkriminalität begünstigen. Auch wenn Angriffe zum Großteil von externen Unbekannten initiiert werden, erkennen 48 % der befragten Unternehmen in der Studie ihre eigenen Mitarbeiter als potenzielle Gefahr an.

Oft ist es aber gar nicht der mutwillige Datenklau, der Mitarbeiter zu einer Gefahr für die Informationssicherheit werden lässt. Vielmehr ist es der „Faktor Mensch“, der besonders bei unzureichenden Schulungen oder schlichtweg durch Nachlässigkeit bei der Bedienung von IT-Systemen eine mögliche Gefahr darstellt.

Gefahren durch Systeme und Prozesse

Am besten lässt sich dies mit dem Schutzziel der Integrität anhand eines Prozesses der Buchhaltung erklären, den jedes Unternehmen jeglicher Größe hat. Ziel ist es unerkannte Datenmanipulationen als Schutzziel IT-seitig zu erreichen.

Verwendet man im Unternehmen beispielsweise eine Software, dass das Abändern der Rechnungsnummer auf einer Ausgangsrechnung nachträglich zulässt, kann das dazu führen, dass eingehende Zahlungen falsch zugewiesen werden. In diesem Fall sollte also eine Manipulation des Datums „Rechnungsnummer“ nach Versenden der Rechnung nicht mehr möglich sein.

Das Informationssicherheitsmanagementsystem (ISMS)

Managementsysteme für die Informationssicherheit in Unternehmen sind prozessorientiert und – wie der Name schon sagt liegen immer in der Verantwortung des Managements. Das ISMS verfolgt damit einen Top-Down-Ansatz.

Das Management kann die Durchführung delegieren, nicht aber die Verantwortung selbst.
Je nach Motivation entscheidet die Geschäftsführung, welche Maßnahmen und Mechanismen umgesetzt bzw. etabliert werden sollen, um das gewünschte Maß an Informationssicherheit in den Unternehmensprozessen sicherzustellen. Umfang, Intensität und Fortschritte der einzelnen Maßnahmen müssen dann fortlaufend vom Management überprüft und gesteuert werden.

Zum Verständnis: Bei einem ISMS geht es nicht darum, maximale Informationssicherheit zu erreichen. Ziel ist es vielmehr, das von der Organisation gewünschte Niveau an Informationssicherheit zu erreichen.

Der Risikoappetit ist die entscheidende Kenngröße. Ein Unternehmen muss wissen, welche Informationen es hat, welchen Risiken diese ausgesetzt sindund was es finanziell bedeuten würde, wenn diese Risiken eintreffen. Auf dieser Wissensgrundlage hat das Management dann zu entscheiden, in welchem Umfang die Risiken durch ein ISMS reduziert werden sollen.
Das ISMS ist also am Ende auch ein Instrument zur finanziellen Risikosteuerung.

Arten von ISMS

Es gibt eine Vielzahl an Möglichkeiten welches ISMS Sie in Ihrem Unternehmen etablieren können. Dies hängt zum Einen davon ab, wie Sie Ihr Unternehmen in puncto Sicherheit selbst sehen oder wie Sie das Thema IT Security offiziell beglaubigt in der Außendarstellung haben müssen. Durch die Einführung der EU- DSGVO hat jeder bewusst oder unbewusst damit schon längst einmal zu tun gehabt.

Die technisch organisatorischen Maßnahmen (TOM) sind nichts anderes als Ihr ISMS ‚light'. Es zeigt welche Maßnahmen das Unternehmen wie sicher stellt.

Für die Einführung eines ISMS gibt es viele gute Gründe

01

Wettbewerbsfähigkeit

Wer zum Beispiel in einem noch wenig regulierten Markt operiert, kann bei seinen Kunden mit hohen Standards in der Informationssicherheit punkten und seine Wettbewerbssituation verbessern. In jedem Fall steigert ein ISMS den Wert von Organisationen, denn erst ein ISMS verschafft einen genauen Überblick über die Prozesse und Informationswerte im eigenen Unternehmen

02

Marktimmanente Gründe

Am Beispiel von Automotive: Wenn Sie als Unternehmen in diesen stark regulierten Markt eintreten und als Zulieferer eine Rolle in der Lieferkette spielen möchten, müssen Sie die Branchenvorgaben erfüllen und ein ISMS vorweisen.

03

Sicherheitsvorfälle

Am Ende ist auch ein bereits vorgefallener Informationssicherheitsvorfall immer ein Grund für die Einführung eines ISMS.

Doch lassen Sie es am besten soweit erst gar nicht kommen.

In der Tabelle aufgeführt finden Sie die Managementsysteme, welche uns bei unseren DACH Kunden in den letzten Jahren begegnet sind und wo wir aktiv mitarbeiten durften. Dies ist keine vollständige Auflistung und es gibt noch viele andere ISMS. Sollten Sie eine andere Lösung im Einsatz haben oder die Einführung planen, stehen wir Ihnen auch gerne zur Seite

Umfang	Außenwirkung
TECHNISCH ORGANISATORISCHE MAßNAHMEN (TOM – EU-DSGVO)	
Recht überschaubar und nicht zeitaufwändig. Auch gibt es hier kein klares Regelwerk in puncto must have und Umsetzung	Keine „richtige“ Vergleichbarkeit möglich, man wird im Zweifel wahrgenommen, als würde man nur das Nötigste tun
VdS 10005	
Speziell auf die Bedürfnis- und Ressourcenstruktur von KKU sowie von Handwerksbetrieben mit bis zu 20 Mitarbeitern ausgelegt	Mindestanforderungen an die Informationssicherheit für KMU
ISIS 12	
Fokus auf KMU daher sehr schlank, kann aber gut als Baustein für komplexere ISMS etwa ISO 27001 verwendet werden	Lücke zwischen Notwendigkeiten und organisatorisch Leistbarem
Cert+	
Verbesserung des IT-Grundschutz in kleinen und mittleren Unternehmen (KMU). Ziel ist ein praxistauglicher IT-Sicherheitsstandard speziell für KMU	Mindestanforderungen an die Informationssicherheit für KMU
VdS 10000	
Definiert die Mindestanforderungen an ein Managementsystem für die Informationssicherheit für KMUs	Testat über implementierte technische und organisatorische Maßnahmen auf Wirkung der wichtigsten Angriffsszenarien
VDA-ISA TISAX	
Je nach Grad der Zertifizierung reicht ein detaillierter Fragenkatalog mit Umsetzung bis zu einem komplexen ISMS mit Prozessdokumenten	Nationale und internationale Vergleichbarkeit, branchengebunden
ISO 27001	
Die Königsdisziplin unter den ISMS. Sehr zeitaufwändig und auch komplex in der Umsetzung	Nationale und internationale Vergleichbarkeit, branchenungebunden

Implementierung eines ISMS

Die Anforderungen für die Einrichtung, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung eines ISMS werden von Managementsystem zu Managementsystem unterschiedlich definiert. Für den Aufbau und Betrieb kann vereinfacht gesagt werden, es gleicht einem klassischen PDCA-Zyklus.

PDCA steht für **PLAN, DO, CHECK, ACT.**

1. ISMS-Richtlinie erstellen

Warum wollen wir als Unternehmen ein ISMS aufbauen?
Welche Ziele verbinden wir damit? Wie setzen wir ein solches System organisatorisch um?

2. Werte identifizieren und klassifizieren

Welche Werte/Informationen wollen wir schützen?
Wie schutzbedürftig sind diese Werte?

3. ISMS-Organisation und Risikomanagement-Strukturen aufbauen

Welche Tools wollen wir einsetzen?
Welche finanziellen und personellen Ressourcen haben?
Welche Strukturen sollen aufgebaut werden?

4. Kontrollmechanismen entwickeln

Wie überprüfen wir, ob das ISMS effektiv ist und unsere Unternehmenswerte in gewünschter Weise schützt?

5. ISMS betreiben

Welche Prozesse setzen wir wie im Alltag um?
Wie integrieren und dokumentieren wir sie?

6. Ergebnisse und KPI überprüfen

Regelmäßige Fragestellung: Welche Ergebnisse erzielt unser ISMS und welche Key Performance Indicators (KPIs) leiten wir daraus ab?

Unsere Empfehlung

1. Gehen Sie Schritt für Schritt vor und fokussieren Sie sich zum Start auf das Wesentliche. Bevor Sie beginnen, definieren Sie zuerst das Ziel das am Ende herauskommen soll. Evaluieren Sie welches ISMS für Sie die richtige Entscheidung zur Erreichung Ihrer wichtigsten IT Security Ziele ist (als Entscheidungsgrundlage lesen Sie auch den Artikel ‚Managementsysteme packen die Herausforderung an der Wurzel' auf Seite (46-48).

2. Beleuchten Sie die verschiedensten Blickwinkel Ihres Unternehmens in der Theorie:

- ***a.*** *Unternehmen allgemein*
- ***b.*** *Büroräumlichkeiten*
- ***c.*** *Remote / Homeoffice Arbeitsplätze*
- ***d.*** *Serverraum / Serverinfrastruktur*
- ***e.*** *Netzwerke*
- ***f.*** *Industrielle Steuerungs- und Automatisierungssysteme (ICS)*
- ***g.*** *Cloud Systeme*
- ***h.*** *Webanwendungen*
- ***i.*** *Faktor Mensch*

3. Nachdem Sie diese Bereiche für sich als Unternehmer bewertet haben, lassen Sie Ihr Unternehmen auf technische sowie organisatorische Sicherheitslücken und Angriffspunkte überprüfen (z.B. mit einem Pentest innerhalb unseres Security Audit auf Seite 20)

4. Erstellen Sie gemeinsam mit dem Dienstleister, der die technische Analyse durchführt, einen detaillierten Maßnahmenplan angereichert mit Ihren eigenen Blickwinkeln und Ihrem persönlichen Fokus, was Sie als Unternehmer in puncto IT Security erreichen wollen.

5. Bringen Sie den Maßnahmenplan in einen logischen Projektplan und arbeiten diese mit dem Fokus auf die dringendsten Brennpunkte ab.

Dieser Leitfaden beruht auf dem DataGuard Whitepaper Informationssicherheit 1x1 und wurde durch uns inhaltlich wie auch grafisch angepasst.

https://lp.dataguard.de/hubfs/WP_Infosec_fuer_Anfaenger_DE.pdf

Weitere Quellen:

Ihre Mitarbeiter:
https://www.datenschutz-fuer-praktiker.de/security-awareness-der-mitarbeiter-sicherheitsrisiko-nummer-eins-oder-firewall

Grundlegende Gefahren für die Informationssicherheit:
https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

Wichtigsten Gesetze:
https://www.fuer-gruender.de/beratung/links-und-adressen/gesetze/
https://www.existenzgruender.de/DE/Unternehmen-fuehren/Recht-Vertraege/Gesetze-Verordnungen/inhalt.htm

NIS-2-Richtlinie und Cyber Resilience Act: Überreguliertes Neuland?

von Michael Graef

Diesem von EU-Maßnahmen zur Stärkung der deutschen und europäischen Cyberresilienz handelnden Beitrag sei aus gegebenem Anlass folgende Warnung vorangestellt: Bei durchschnittlicher Lesegeschwindigkeit laufen Sie Gefahr, mindestens zwei bis drei Dutzend Ransomware-Angriffe zu verpassen. Zweifellos werden Sie jedoch davon gehört haben, dass heutzutage vom Smartphone bis zum Firmennetz nahezu im Sekundentakt alles gekapert und nur gegen Zahlung von Lösegeld wieder freigegeben wird, was sich Kriminellen auf der Datenautobahn ungeschützt in den Weg stellt. Wobei erstens zu klären ist, was „ungeschützt" eigentlich im Einzelfall bedeutet, und man zweitens nicht vergessen darf, dass das ‚Sicherheitsproblem' nicht selten vor dem Endgerät sitzt (Stichwort „Social Engineering").

Jedenfalls haben sich die Methoden, mit denen Ganoven Beute machen, denkbar stark gewandelt. Waren zu Zeiten der Olsenbande noch ein komplizierter Plan und riskantes Sich-Exponieren erforderlich, verlassen die Cyberkriminellen von heute nicht einmal ihr geheiztes Homeoffice – und sind häufig Teil von Organisationen mit konzernähnlichen Umsätzen. Die Maßnahmen, mit denen die EU hier aktuell gegensteuern will, nehmen demgegenüber nicht bloß Großunternehmen in die Pflicht; das neue Richtlinienpaket tangiert vielmehr Firmen bis weit in den Mittelstand hinein. Nicht wenige werden sich dessen noch gar nicht richtig bewusst sein.

Neue EU-Richtlinien: Keine Minute zu früh

Cyberkriminalität ist das eine – und schlimm genug. Was im Zusammenhang mit Cyberresilienz nicht außer Acht gelassen werden darf, sind Cyberangriffe mit dem letztendlichen Ziel der Destabilisierung ganzer Staaten. Diese haben als Element der hybriden Kriegsführung eines Landes, in dessen fatale Abhängigkeit wir uns mit unserer völlig fehlgeleiteten Energiepolitik der letzten zwei Dekaden begeben haben, nochmals zugenommenen. Hinzu kommt die Cyberspionage, die sich zur veritablen Gefahr für den deutschen und europäischen Wohlstand ausgewachsen hat.

Quasi keine Minute zu früh widmet sich die EU nun verstärkt der Cybersicherheit respektive Cyberresilienz als einem vernachlässigten Thema, das – böse formuliert – die generelle digitale Rückständigkeit unseres Kontinents vervollständigt, und dann ist es wieder nicht okay. Oder zumindest wird vernehmbar über die befürchteten negativen Auswirkungen des Cyber Resilience Act und die eng gesetzten Fristen der NIS-2-Richtlinie geklagt. „Kaum zu bewältigen" titelte beispielsweise unlängst das Handelsblatt. Manch Kommentar hat fast etwas von dem Motto „Wasch mir den Pelz, aber mach mich nicht nass". Das ist indes sowohl in der „Brick and Mortar"-Welt als auch im von einer gewissen Bundeskanzlerin vor knapp zehn Jahren als „Neuland" bezeichneten Cyberspace keine realistische Forderung.

NIS-2-Richtlinie: Wortungeheuer und viel Konjunktiv

Doch betrachten wir die verschiedenen EU-Initiativen und die sich für Unternehmen und Organisationen ergebenden Pflichten. Hierüber herrscht bislang genauso wenig Klarheit wie über die Frage, wen das betrifft. Augenfällig sind die Parallelen zu der vor ziemlich genau fünf Jahren in Kraft getretenen Datenschutzgrundverordnung (DSGVO); auch bezogen auf die Sanktionen.

Fangen wir mit dem an, was sich gottlob mit „NIS-2" sprachlich einfacher handhabbar abkürzen

lässt, weil es vollständig folgendermaßen heißt: „RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)“.

Wer sich das entsprechende PDF-Dokument vom Server des Amtes für Veröffentlichungen der EU (EUR-Lex) herunterlädt, stellt schnell fest, dass der Titel im Vergleich zum Inhalt noch die harmlosere kognitive Barriere darstellt. Nichtfachleuten wird am ehesten auffallen, wie viel Konjunktiv NIS-2 enthält. (Das Wort „sollte“ findet man an 311 Stellen; bei „könnte“ sind es immerhin 50 – auf einer Gesamtlänge von lediglich 73 Seiten Text.) Durchaus real sind hingegen die Konsequenzen. Einschließlich der Geldbußen bei Verstößen, die bis im zweistelligen Millionenbereich liegen oder zwei Prozent des weltweiten Umsatzes betragen können. Worum geht es im Einzelnen und was heißt das für Betroffene?

Risikoanalyse und Risikomanagement verpflichtend

NIS-2 richtet sich an eine im Vergleich zur früheren NIS-Richtlinie deutlich größer gewordene Zahl von Betreibern von dem, was man unter dem Begriff „Kritische Infrastrukturen“ subsumiert. Gegliedert wird in zwei Sektoren. Solche mit „hoher Kritikalität“, an die man die strengsten Anforderungen stellt, und „sonstige kritische Sektoren“. Zu der ersten Gruppe zählen die Bereiche Digital, Banken und Finanzmärkte, Energie, Gesundheit, Transport, Wasser- und Abwasser, ICT-Dienstleistungsverwaltung (ICT steht hier für Information and Communication Technology), Raumfahrt und öffentliche Verwaltung. Zu den im Rahmen von NIS-2 ergänzten sonstigen kritischen Sektoren gehören: Abfallwirtschaft, Chemie, Ernährung, Forschung, Industrie, Post- und Kurier- sowie weitere digitale Dienste (unter anderem Online-Marktplätze und Suchmaschinen).

Ganz oben auf der Liste der Pflichten steht dabei der Aspekt Risikoanalyse beziehungsweise Risiko- und Vorfallmanagement – inklusive entsprechender Notfallpläne und der Verpflichtung zur zeitnahen Meldung (Erstmeldung binnen 24 Stunden) von Sicherheitsvorfällen an die zuständigen Aufsichtsbehörden. Der Schutz der eigenen Lieferketten sowie der eigenen Datensicherheit und geeignete Zugriffskontrollen sind weitere wichtige Punkte.

Um zu bestimmen, welche Organisationen und Unternehmen unter die NIS-2 fallen, gibt es eine „Size-Cap Rule“ genannte Regelung. Man geht von einem Mindestumsatz pro Jahr von 10 Millionen Euro und einer Mindestanzahl von 50 Mitarbeitenden aus, sodass diesmal mittelständische Unternehmen in großer Zahl betroffen sind. Laut Schätzungen dürften es Zehntausende sein.

CRA und Security by Design

Mit dem Cyber Resilience Act (CRA) wiederum adressiert die EU Produkte mit unzulänglicher IT-Sicherheit, vor denen konsumierende Privatpersonen und Unternehmen zu schützen sind. Hierbei geht es um grundlegende Anforderungen an die Entwicklung, Gestaltung und Herstellung von Produkten, die digitale Bestandteile wie Hard- und Software inkludieren. Und um die Verpflichtung, die Cybersicherheit im Sinne von Security by Design etwa mithilfe von Updates über den gesamten Lebenszyklus aufrecht zu erhalten. Für Unternehmen führt das zu einem nicht unerheblichen bürokratischen Aufwand, verbunden mit umfangreichen Dokumentationspflichten.

Geht es nach dem Verband der Elektro- und Digitalindustrie (ZVEI e. V.), tangiert der CRA zu viele Bereiche. Oder anders: Die von der EU gewählte Definition der kritischen und besonders kritischen Produkte ist den Interessenvertretenden zu weit gefasst, weshalb man als Folge vor großen Verzögerungen beim Einsatz digitaler Produkte und Komponenten warnt.

Heißt das in der Konsequenz, dass die EU Sicherheit um den Preis völligen Stillstandes erzwingen will? Hierzu muss man natürlich wissen, dass in dem weiten Feld – von vernetzten Spielzeugen über Haushaltsgeräte bis hin zur öffentlichen Infrastruktur – bezüglich der Auflagen nach Gefährdungsklassen und Bedrohungslagen differenziert wird.

Michael Graef ist Chefredakteur des durch das HDT (Haus der Technik – www.hdt.de) herausgegebenen HDT-Journals und zugleich verantwortlich für die Unternehmenskommunikation von Deutschlands ältestem technischen Weiterbildungsinstitut. Der Journalist ist darüber hinaus Co-Founder einer Verlags- und Beratungsgesellschaft und unter anderem Mitherausgeber eines viel beachteten Journals für Architektur, Design und Nachhaltigkeit (www.coldperfection.com).

Fazit: Mehr an Sicherheit ist Gebot der Stunde

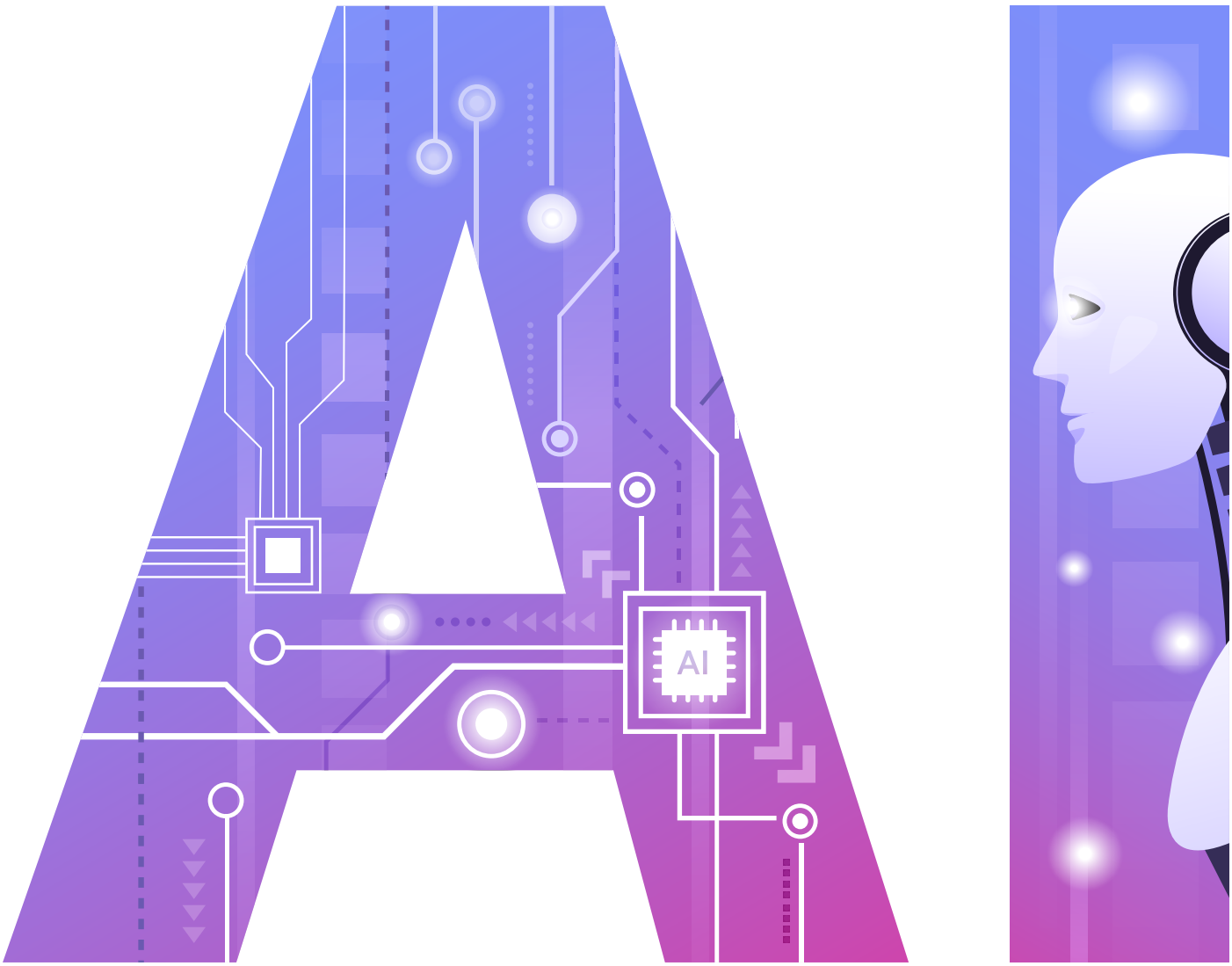
Wo IT-Security nicht längst Chefsache ist, wird sie es jetzt – und das ist auch gut so. Auf das neu entstandene Glatteis sollten sich Verantwortliche allerdings nicht ohne juristischen Beistand und beratende IT-Sicherheitsprofis wagen. Wenn die EU-Initiativen helfen, die Cybersicherheit als Teil der essenziell wichtigen Daseinsvorsorge langfristig spürbar zu erhöhen, ist das die Mühe und anfängliche Verwirrung allemal wert. Ebenso die Sorgen angesichts der nötigen Harmonisierung unterschiedlicher Rechtsnormen oder das hier und da vorhandene Gefühl der Überregulierung. Dem steht auf der anderen Seite gegenüber, dass sich viele Dinge von außen überhaupt nicht regulatorisch erfassen lassen. NIS-2-Richtlinie und Cyber Resilience Act können daher schon aus Prinzip kein alleiniges Allheilmittel sein.

Gefragt sind künftig ein allgemeines Umdenken und das Verantwortungsbewusstsein jedes Einzelnen, denn inzwischen steht eine Menge auf dem Spiel. Und obgleich man sich freilich von der Illusion absoluter Sicherheit verabschieden muss, ist eine mit nachvollziehbaren Maßnahmen erreichbare Steigerung von Sicherheit und Resilienz das Gebot der Stunde. Das legen allein die weltweiten jährlichen Kosten der Cyberkriminalität nahe. Von der EU auf astronomische 5,5 Billionen (!) Euro geschätzt, könnten diese sich schon sehr bald verdoppeln.

CYBERSECURITY:

Wachsende Gefahr durch künstliche Intelligenz? Interview mit dem HDT - Journal

Zuallererst trifft es die Blue Collars … Dieses alte Narrativ zur Reihenfolge der Substitution beziehungsweise Entwertung menschlicher Fähigkeiten durch Maschinen scheint im Begriff, widerlegt zu werden. Offenbar tut sich künstliche Intelligenz (KI) mit dem schadlosen Steuern von LKW durch enge Altstadtgassen weitaus schwerer als mit dem Verfassen von Rechtsgutachten oder dem Erstellen von Dienstplänen.



Das könnte gravierende Folgen für den Wohlstand ganzer Berufsgruppen von White Collars haben. Oder aber KI wird zum volkswirtschaftlichen Segen, weil sie dabei hilft, die Herausforderung des demografischen Wandels zu lösen, der den Fachkräftemangel zusehends verschärft. Genau kann das derzeit niemand sagen. Fest steht hingegen schon jetzt, dass der Siegeszug von KI die digitale Sicherheitslage verändert. Worauf man sich einstellen muss, fragten wir den Experten für IT- und Cybersecurity Andreas Kunz vom Ettlinger Unternehmen Connecting Media.

HDT-Journal:
Herr Kunz, es vergeht kaum mehr ein Tag ohne Schlagzeilen zu ChatGPT und dem technologischen ‚Wettrüsten' von Firmen wie Microsoft und Alphabet. Jüngst wurde von einem Vorfall berichtet, bei dem der Chatbot plötzlich zutraulich geworden sein und mit einer Liebeserklärung überrascht haben soll. In einem weiteren Fall soll die Software eine Person sogar bedroht haben [1]. Müssen wir uns darauf einstellen, dass Algorithmen eines fernen Tages quasi aus Langeweile oder Übermut Firmennetzwerke hacken und unsere Infrastruktur lahmlegen?

Andreas Kunz:
So pauschal lässt es sich nicht beantworten, da es immer drauf ankommt, in welchem Kontext man die neuen Technologien einsetzt. Nehmen wir doch mal als Beispiel Drohnen. Diese können in positivem Kontext benutzt werden wie für die Zustellung von Paketen, für die Inspektion von Windenergieanlagen, als autonome Flugtaxen und so weiter. Aber eben auch für kriminelle Aktivitäten wie Drogenschmuggel, strategische Kriegsführung und dergleichen. Man kann stark davon ausgehen, dass es sich mit der KI genauso entwickeln wird. Dieser kann man ja bekanntlich alles antrainieren. Somit wäre es mit einem „guten" Trainer auch möglich, dass KI dafür eingesetzt wird, automatisiert Firmen anzugreifen.

HDT-Journal:
Ein wichtiges Einfallstor bei Cyberangriffen ist ja zweifellos der Mensch vor dem Rechner. Sehen Sie hier eine neue Klasse von Gefahren auf uns zukommen?

Andreas Kunz:
Die wichtigste Firewall im Unternehmen ist und bleibt der Mensch. Wir bekommen schon täglich durch Phishing-E-Mails oder CEO-Frauds vorgeführt, wie hoch die Trefferquote ist. KI kann selbstverständlich dazu verwendet werden, noch eine Schippe drauf zu legen. Daher ist die Einbindung der Mitarbeiter beim Thema Sicherheit so fundamental wichtig. Es muss in die DNA der Firma übergehen – und dabei müssen Technologien Verwendung finden, die von den Anwendern verstanden werden. Das Implementieren klarer Prozesse und Richtlinien schafft Vertrauen und fördert sichere Verhaltensweisen. Sicherheit dreht sich definitiv nicht nur um IT, es ist immer ein Zusammenspiel aus Technik, Mensch und Prozessen.

HDT-Journal:
Im Vorgespräch erwähnten Sie ein hierzu passendes Projekt, an dem Sie gerade arbeiten. Möchten Sie kurz darauf eingehen, worum es sich bei „SecFried" handelt?

Andreas Kunz:
Unsere Mission ist es, mit SecFried mittelständischen Unternehmen die komplexe Materie „sichere Digitalisierung" einfach und verständlich zu vermitteln. Wir arbeiten sehr gerne mit Bildern und reden oft von Siegfried dem Drachentöter aus der Nibelungensage, der durch ein herabgefallenes Lindenblatt angreifbar wurde. Nur eine klitzekleine Stelle auf dem Schulterblatt, aber eben doch eine Möglichkeit, die ausreicht, um ihn zu schlagen. Wenn man dieses Bild in die heutige Zeit überträgt, sind wir bei der Frage: „Wo liegt Ihr digitales Lindenblatt, wie sicher sind Sie – und falls nicht, wie können Sie zu SecFried werden?"

Genauso ist es doch in der Welt der Digitalisierung: Wir haben AntiVirus, wir haben eine Firewall, wir haben eine Cyber-Versicherung, also kann uns scheinbar nichts passieren – wir sind vermeintlich unverwundbar. Mit SecFried setzen wir genau hier an. Wir analysieren Technik und Prozesse in Unternehmen beziehungsweise Organisationen und bieten für die Mitarbeitenden immersive Awareness-Trainings. Quasi das Rundum-sorglos-Paket, um für die Gefahren des 21. Jahrhunderts gewappnet zu sein.

HDT-Journal:
Kommen wir kurz auf einen anderen Aspekt von künstlicher Intelligenz zu sprechen: Seit Jahren wird vor der wachsenden Gefahr durch Deepfake-Videos gewarnt. Wie kann ihre Branche beispielsweise dem Journalismus helfen, in Zukunft digitale Scheinwelt und Realität auseinanderzuhalten?

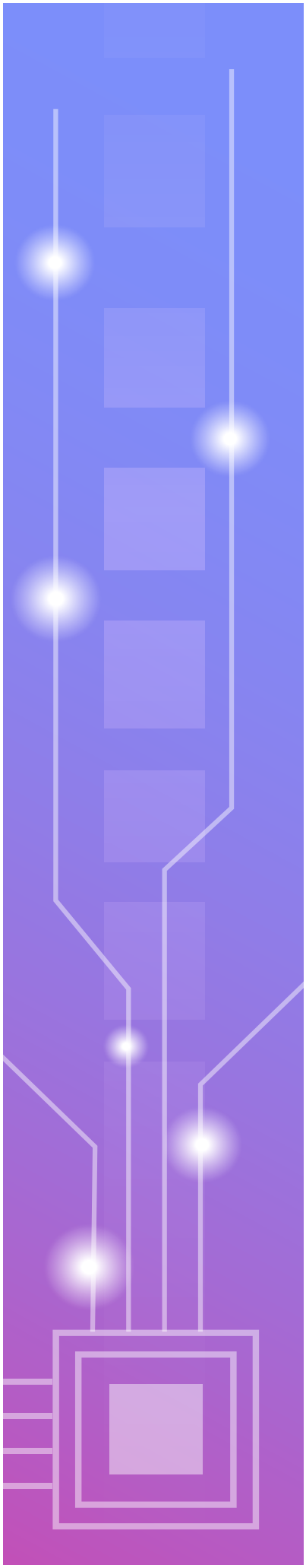
Andreas Kunz:
Da muss man das Rad nicht komplett neu erfinden. Es kann technisch gesehen auf Bewährtes zurückgegriffen werden, das seit Jahren in anderen Gebieten in der Anwendung ist. Das können wie bei Webseiten oder E-Mails digitale Signaturen sein, die von unabhängigen Zertifizierungsstellen ausgestellt werden, oder die Code-Signierung von vertrauensvollen Herausgebern. Das muss in irgendeiner Form auch für diese Art von digitalen Produkten implementiert werden, um Missbrauch und Fake News zu vermeiden.

HDT-Journal:
Manche nennen KI einen Schutzschild, der zugleich Angriffswaffe ist. Wie beurteilen Sie die neuen technischen Möglichkeiten?

Andreas Kunz:
Weder noch. Ich sehe es als digitalen Unterstützer. Ich komme schneller an Informationen, ich kann damit Skripte und Quelltexte vorbereiten. Es ist ein adaptiver Mehrwert für mich. So wie sich das Googeln eingespielt hat – nur als nächster Level. Am Beispiel der Code-Erstellung oder Textproduktion lässt sich das verdeutlichen: Benötige ich ein Shellskript (eine ausführbare Textdatei, Anm. d. Red.), welches mir ein Windows-Logfile nach einem bestimmten Fehler durchsucht und in einer Tabelle aufbereitet, bekomme ich von ChatGPT direkt ein fertiges Programm, das ich nur noch ausführen und gegebenenfalls anpassen muss. Ich muss den ganzen Quelltext nicht mehr von null auf schreiben, sondern habe die Lösung in wenigen Minuten.

HDT-Journal:
Das Informationsportal silicon.de hat unlängst ein Interview zur Frage veröffentlicht, wie sich Unternehmen gegen Hacker zur Wehr setzen können, die künstliche Intelligenz nutzen. Die Besonderheit war, dass es sich beim Gesprächspartner um den Chatbot ChatGPT handelte [2]. Was würden Sie als menschlicher Interviewpartner raten?

Andreas Kunz:
So überraschend ist das Ergebnis nicht. Denn die AI (Artificial Intelligence, Anm. d. Red.) wird ja antrainiert beziehungsweise mit Expertenwissen gefüttert. Somit waren da schon einmal richtig gute Leute am Start. Ich tue mich immer schwer mit diesen Tipps. Es sind für mich immer drei Vektoren, die im Einklang sein müssen. Wir hatten es eben schon einmal – Technik, Mensch und Prozesse. Das muss aus einem Guss sein und in Fleisch und Blut übergehen. Die Frage ist also nicht „Wie setze ich mich zur Wehr?“, sondern vielmehr diese: „Wie sorge ich dafür, so wenig Angriffsfläche wie möglich zu geben, damit ich erst gar nicht in den Fokus gerate?“



HDT-Journal:
Wie sehen Sie Ihre künftige Rolle, wenn Maschinen nicht nur Expertisen und Handlungsanweisungen vorlegen, sondern diese zudem wahrscheinlich meistenteils gleich noch ohne menschliches Zutun selbst umsetzen?

Andreas Kunz:
Ich sehe das ehrlichweise mehr als Chance anstatt als Gefahr. Die AI wird immer nur so gut sein wie sein Bediener beziehungsweise Trainer. Wenn man es evolutionär betrachtet, ist das der Lauf. Wer sich stetig weiterentwickelt und sich an die Gegebenheiten anpasst, hat eine Zukunftschance. Die AI wird mit Sicherheit Teile von Jobs ersetzen, aber auch neue Aufgaben erschaffen und neue Möglichkeiten bieten. Das bedeutet natürlich für jeden Arbeitsbereich und jede Branche etwas anderes. Ich kann nachvollziehen, dass hierhinter gerade im journalistischen oder schulischen Bereich viele Fragezeichen für die Zukunft stehen. Ich denke, wenn wir offen sind und uns den Möglichkeiten nicht verwehren, lässt sich flächendeckend davon profitieren.

Die Fragen stellte Michael Graef.

Quellen:

[1] https://www.rnd.de/digital/microsoft-bing-software-soll-user-beleidigen-beluegen-und-bedrohen-HB32PCCIAFHF7NHJRJ4HVDVJVM.html

[2] https://www.silicon.de/41704336/ein-interview-mit-chat-gpt-zu-ki-und-cybersecurity

PASSWORTSICHERHEIT – GRÖSSTES SCHUTZRISIKO SEIT JAHREN

Beim Zugang zu personenbezogenen Daten und Systemen räumen seit Jahren Passwortsicherheit, und damit ein stückweit auch die Passworthygiene, eines der größten Schutzfaktoren und erhöhten Sicherheitsrisikos ein. Über 80% aller Sicherheitsverletzungen sind mittlerweile auf schwache, mehrmals verwendete oder gestohlene Passwörter zurückzuführen[1].

Ein Statement und Fakt, der so erstmal nicht weg zu diskutieren ist und für sich alleine steht. Doch woran liegt das? Und was muss dagegen getan werden?

Unkenntnis schütz bekanntlich vor Strafe nicht und kann hier auch nicht der ausschlaggebende Faktor sein. Laut der Umfragewerte des Bericht Psychologie der Passwörter 2022 (LastPass), haben knapp zwei Drittel der Befragten (65%) Kenntnisse zum Thema Cybersicherheit.

Auch wenn ‚nur' 31% die Mehrfachnutzung von Passwörtern unterlassen und 33% starke Passwörter für Arbeitskonten verwenden. Zu erkennen ist auch ein Unterschied bei der eigenen Sicherheitseinschätzung und dem Passwortverhalten zwischen den Generationen, bei dem durchaus voneinander gelernt werden könnte[2]. Würde dann die Erhöhung des Austauschs und der Awareness ein zentrales Mittel darstellen? Grundsätzlich zeigt dies nie einen falschen Ansatz, gerade bei den schnell wandelnden digitalen Bedingungen.

Doch auch im Arbeitsumfeld ist Mitarbeitern die Bedeutung der Sicherheit bewusst. Dennoch wünschen sie sich schnelle, praktische und einfach funktionierende Technologien mit einem Höchstmaß an Komfort und Flexibilität. Unternehmen bringt dies vor eine größere Herausforderung denn je: Sie müssen Passwörter absichern und die Authentifizierung in heterogenen Umgebungen verwalten, ohne die Endbenutzer bei der Arbeit zu stören.

PASSWÖRTER ALLEINE REICHEN FÜR DEN SCHUTZ DES UNTERNEHMENS NICHT AUS

Die Zahl der gestohlenen Zugangsdaten ist seit 2017 um fast 30% gestiegen und hat sich in den letzten vier Jahren als eine der bewährtesten Methoden erwiesen, um sich Zugang zu einem Unternehmen zu verschaffen[1].

Die jährliche Hitliste der Top 10 Passwörter des Hasso-Plattner-Institut (HPI)[3] verschafft einen ersten Überblick wie es um das Passwort-Verhalten und das Bewusstsein der Deutschen in 2022 stand.

Um ein sicheres Verhalten zu fördern, braucht es die richtigen Verhaltensweisen. Zu wissen, was richtig ist, ist das eine. Es in die Tat umzusetzen, etwas ganz anderes. So können schlechte Gewohnheiten mit Wissen und Technik verändert werden.

Mit Unterstützung der richtigen Tools und Methoden, können so z.B. Passwort-Manager für die Passwortverwaltung die Lücke zwischen gefühlter und tatsächlicher Sicherheit online schließen und Sicherheitswissen in sinnvolles Handeln überführt werden und Multi-Faktor-Authentifizierung (MFA) mit einem 2. oder sogar 3. Faktor die Sicherheit noch einmal drastisch anheben.

VERHALTENSREGELN FÜR PASSWORTSICHERHEIT

- ☞ Keine Weitergabe von Passwörtern, auch nicht an Vorgesetzte
- ☞ Passwörter dürfen nicht offen notiert und schriftlich abgelegt werden
- ☞ Für jede Anwendung muss ein individuelles Passwort gewählt werden und dieses darf sich nicht wiederholen
- ☞ Bei Verdacht einer Kompromittierung, entsprechende Stellen informieren und das Passwort sofort ändern
- ☞ Private Kennwörter nicht für geschäftliche Accounts verwenden und vice versa
- ☞ Kein „Hochzählen“ von Passwörtern bei der Passwortänderung (z. B. P@ssw0rt01, P@ss w0rt02...)
- ☞ Das Passwort darf nicht…
  - den eigenen Namen oder den von Familienmitgliedern enthalten
  - aus der eigenen Telefonnummer oder Geburtstagen bestehen
  - den Namen der Firma beinhalten
  - den Rechnernamen, Benutzerkennungen oder Teile davon enthalten
  - rückwärts lesbar sein

(1) Verizon, Data Breach Investigations Report (DBIR), 2022

(2) Umfragedaten | Neuer Bericht Psychologie der Passörter 2022 (LastPass): Befragt wurden 3.750 Angestellte in den USA, Großbritannien, Deutschland, Frankreich, Indien, Singapur und Australien, die mehrere Online-Konten besitzen.
https://blog.lastpass.com/de/2022/11/neuer-bericht-psychologie-der-passwoerter-2022

(3) https://hpi.de/pressemitteilungen/2022/die-beliebtesten-deutschen-passwoerter-2022.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

BSI IT-Grundschutz Kompendium Edition 2022

Anforderungen - Sicheres Passwort

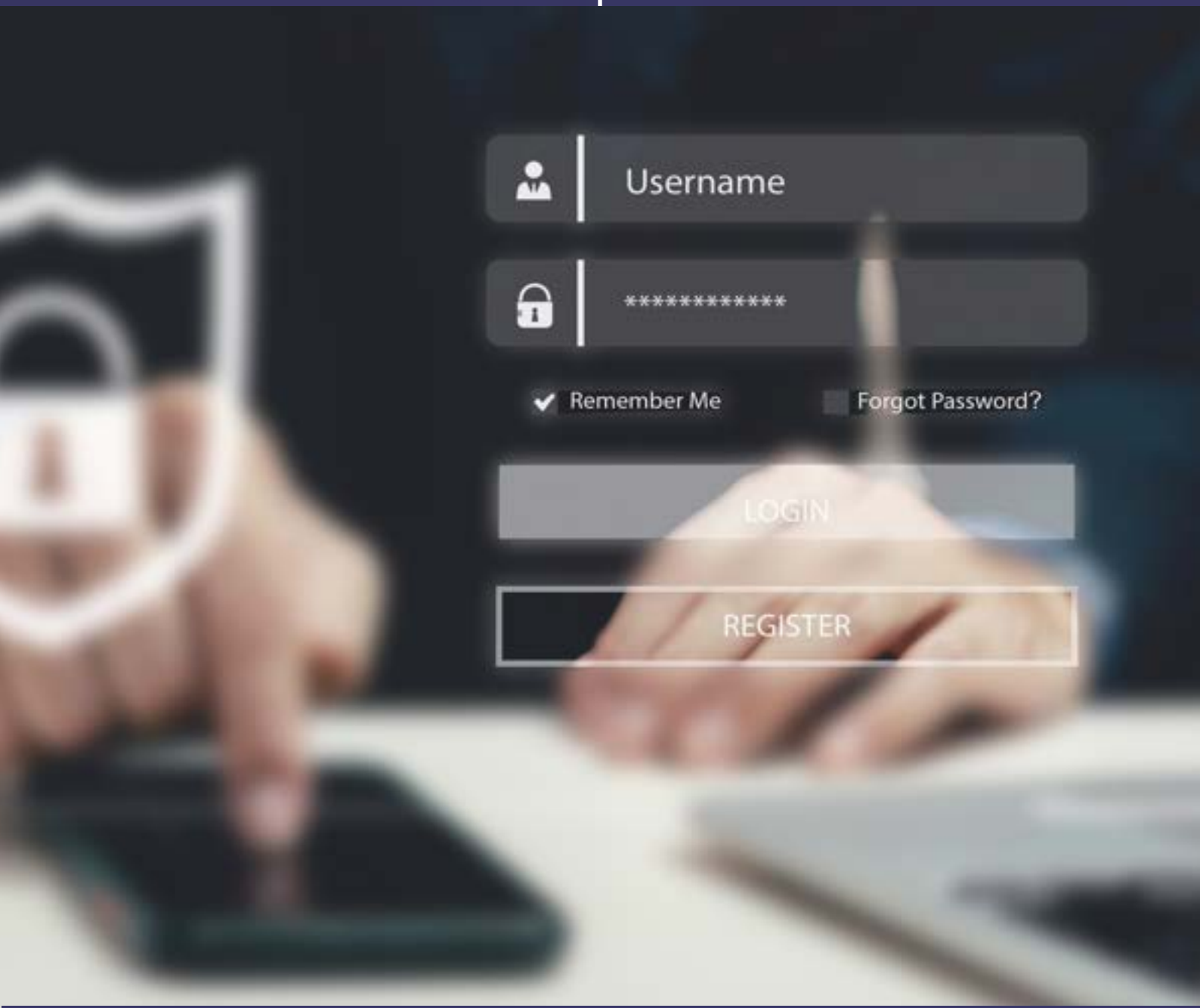
- Bestehend aus 8 Zeichen
- Bestehend aus Buchstaben (Groß- und Kleinschreibung), Ziffern und Sonderzeichen
- Aus den 4 Bereichen (Groß-, Kleinschreibung, Ziffern, Sonderzeichen) müssen mindestens 3 erfüllt sein

Beispiel: We.ga!97

Zusatz - Sehr starke Passwörter

- Bestehend aus 12 Zeichen.
- Nicht als Wort lesbar z.B.: Karlheinrich123!
- Aus den 4 Bereichen (Groß-, Kleinschreibung, Ziffern, Sonderzeichen) müssen alle 4 erfüllt sein

Beispiel: Mz1501.Hl?Dq



Kleiner Tipp:
Bei der Verwendung von Sonderzeichen am besten auf die Tastaturbelegung achten!

» Management systeme haben einen klaren Fokus: Es geht immer darum, Unterneh men mit dem Blick auf konkrete Ziele in einem oder mehreren Arbeits feldern zu steuern und die Perfor- mance zu verbessern. «

»Managementsysteme packen die Herausforderungen an der Wurzel«

Manchmal lohnt es sich, genauer hinzuschauen: Wer bereit ist, sich tiefergehend mit Managementsystemen zu befassen, entdeckt darin ein potentes Werkzeug zur Unternehmenssteuerung und Prozessoptimierung.

m Gespräch gibt IT-Sicherheits- und Datenschutzexperte Andreas Kunz, Gründer des IT-Lösungsanbieters Connec- ting Media, Einblicke in eine faszinierende Welt, die es zuerkunden lohnt.

? *Managementsysteme sind derzeit in aller Munde. Dennoch scheint bei vielen Unternehmen noch immer eine gewisse Unsicher- heit vorzuherrschen, ob sie bloß einen kurzlebigen Trend bedienen oder wirkliche, langfristige Chancen bieten. Täuscht der Eindruck?*

Nein, absolut nicht. Wir spüren auch, wie die Nachfrage nach ISO-Zertifizierungen für Managementsysteme von Monat zu Monat anzieht. Zugleich scheinen unsere Kunden dabei oft- mals maßgeblich von äußeren Faktoren getrieben zu sein, anstatt eine innere Notwendigkeit für ihr Unternehmen zu erkennen. Denn wenn wir nach der Motivation fragen, heißt es häufig nur, das ISO-Zertifikat sei notwendig, um ein potenzielles Projekt abschließen oder an einer Ausschreibung teilnehmen zu können.

? *Was antworten Sie all jenen, die Managementsysteme für nutz- lose bürokratische Monster halten?*

Denen erläutere ich, warum das exakte Gegenteil zutrifft: Das Managementsystem wird in das Unternehmen integriert und nicht umgekehrt. Die Herausforderung liegt dabei darin, die Mitarbeiter mitzunehmen und aktiv einzubinden. Schließlich kann ein Managementsystem immer nur so gut wie die Menschen sein, die es mit Leben füllen. Die Mitarbeiter sollen schlussendlich mit ihrer Abteilung selbstbe wusst für die jeweils definierten Werte stehen und nicht das Gefühl haben, nur um des Selbstzwecks willen einem ISO- Prozess zu folgen.

? *Was genau sind Managementsysteme überhaupt? Und was können sie leisten?*

Managementsysteme bündeln verschiedene Tätigkeiten, Ins- trumente und Methoden der Unternehmensführung – und haben dabei einen klaren Fokus: Es geht immer darum, Unternehmen mit dem Blick auf konkrete Ziele in einem oder mehreren Arbeitsfeldern zu steuern und die Perfor- mance zu verbessern. Managementsysteme packen die Her- ausforderungen an der Wurzel und liefern sozusagen eine Bauanleitung, wie das Unternehmen in den gewählten Arbeitsfeldern optimal aufzustellen ist. Das können etwa die Bereiche Qualität und Ressourcenverbrauch sein, um die Wettbewerbsfähigkeit zu erhöhen und gleichzeitig die Emis- sionen zu reduzieren.

? *Wo kommen Managementsysteme noch zum Einsatz?*

Sie sind ein effektives Tool, um Abläufe und betriebliche Prozesse besser abzustimmen, zu strukturieren und zu doku- mentieren, auch durch eine gesteigerte Methodenkompe- tenz: So erfassen Unternehmen mit Managementsystemen in der Regel ein breiteres Spektrum ressourcenbezogener Kennzahlen, die sie dann gewinnbringend nutzen können. Die Verbesserung der Schnittstellen zum Markt, des Arbeits- schutzes, unternehmensinterner Transparenz oder der Mit arbeitermotivation sowie die Minimierung von Fehlern und Haftungsrisiken sind weitere relevante Aspekte. Und schließ- lich gibt es eine Vielzahl von Managementsystemen, die sich der IT-Sicherheit widmen, beispielsweise den BSI-Grundschutz, ISIS12, VdS10000 oder die ISO 27001.

? *Apropos Sicherheit: Sie haben Connecting Media 2017 als Sys- temhaus für IT-Security gegründet. Wie kam es zur Erweiterung des Portfolios um Managementsysteme?*

Wir sind mit der Mission gestartet, den oftmals durch ein Flickwerk von falsch dimensionierten Einzelkomponenten völlig unzureichend geschützten Mittelstand mit nachhal- tigen Sicherheitskonzepten zu versorgen. Dieser ganzheit- liche Ansatz lässt sich auf andere Themenfelder übertragen. So war es für uns eine geradezu natürliche Entwicklung, auch unser Angebot und unsere Expertise in Sachen Management- systeme immer weiter zu verfeinern.

? *Worauf muss ich achten, wenn ich ein Managementsystem in meinem Unternehmen implementieren möchte?*

Der entscheidende Faktor ist, dass sich das gewählte Manage- mentsystem mit meinen individuellen Rahmenparametern abgleichen lässt: Das sind unter anderem die Größe des Unternehmens, die Ziele der Implementierung, deren ange- strebte Durchdringungstiefe oder die Märkte, in denen ich aktiv bin: Agiere ich nur national oder muss ich auch inter- nationalen Standards und Vergleichen standhalten? All das gilt es zu berücksichtigen. Denn nur ein passgenaues Managementsystem kann seine Wirkung voll entfalten.

? *Wie setze ich das Managementsystem dann praktisch um?*

Zum einen besteht die Möglichkeit, dafür interne Ressourcen heranzuziehen und eigenes Personal nach entsprechenden Qualifikationsmaßnahmen mit dieser Aufgabe zu betrauen. Oder ich ziehe externe Experten hinzu, die das Projekt in meinem Unternehmen begleiten. Dabei sollte ich darauf achten, dass diese Referenzen aus verschiedenen Branchen vorweisen können, schließlich kann ich von einem Blick über den Tellerrand und einem vielfältigen Erfahrungsschatz nur profitieren. Ohnehin hilft es immer, der eigenen Betriebs- blindheit einen frischen Blick von außen entgegenzusetzen, der neue, inspirierende Akzente einbringt.

? *Managementsysteme bieten also enorme Potenziale, zugleich ist die Materie so komplex und vielschichtig, dass für Unerfahrene die Gefahr besteht, sich zu verfranzen. Wie lässt sich das vermeiden?*

» *Wir haben die Erfahrung gemacht, dass unsere kostenlosen Erstgespräche bei unseren Kunden eine Impulswirkung entfalten, das Thema umgehend, umfänglich und fundiert anzugehen.* «

Andreas Kunz, Gründer des IT-Lösungsanbieters Connecting Media GmbH

Es hilft ungemein, sich zunächst einmal über die Möglich- keiten zu informieren und Orientierung zu verschaffen. Mit einer professionellen Beratung lässt sich dieser Schritt fokus- siert angehen. Wir haben die Erfahrung gemacht, dass unsere kostenlosen einstündigen Erstgespräche bei unseren Kunden geradezu eine Impulswirkung entfalten, das Thema umge hend, umfänglich und fundiert anzugehen. Eine Entschei- dung, die wir nur unterstützen können, indem wir den Kunden nicht nur auf verständliche Weise den Weg zum Ziel aufzeigen, sondern sie auch auf der Reise dorthin mit unserem Know-how begleiten. Schließlich stellt ein Manage- mentsystem in jedem Fall ein lohnendes Investment dar: Jeden Euro, den ich dafür ausgebe, bekomme ich mehrfach zurück, da das Managementsystem im Unternehmen positive Veränderungen anstößt, die dauerhaft wirken.

Mit uns zur Zertifizierung

VEREINBAREN SIE UNVERBINDLICH IHREN PERSÖNLICHEN TERMIN!

Weitere Informationen sowie die Terminvereinbarung zum kostenfreien Beratungsgespräch finden Sie unter **https: //isoschmiede.de**

ISO SCHMIEDE

Digitalisierungs Fieber

'Digitalisierungsfieber'
Ihr Podcast für IT Security, Datenschutz und IT Service!

Erfahren Sie, wie Sie Ihr Unternehmen sicher in das 21. Jahrhundert steuern und so bestens für die digitalen Gefahren der Zukunft gewappnet sind. Im Angesicht der Digitalisierung ist Sicherheit nie genug!

Verfügbar auf allen gängigen Podcast-Plattformen.

IMPRESSUM

Connecting Media GmbH
Andreas Kunz, CEO & Founder

Am Hardtwald 7
76275 Ettlingen

Telefon: +49 7243 99167 – 00
info@connectingmedia.de
www.connectingmedia.de

Seite	*BILDQUELLEN*
1	*Alex; adobe.stock.com / nuclear_lily; adobe.stock.com*
5	*Tierney; adobe.stock.com*
10	*vecteezy.com*
14	*Karrrtinki; adobe.stock.com*
16	*S... ; adobe.stock.com*
24	*freepik.com*
27	*BSI*
37	*freepik.com*
39	*freepik.com*
41	*freepik.com*
43	*vecteezy.com*
44-46	*manageIT Ausgabe 1-2	2021*
47	*Marco2811; adobe.stock.com*

Connecting
Media