AUSGABE 4

cm magazin

01010000110101011001010101010101010110

Digitale Transformation – innovativ und sicher

IT SERVICE

IT SECURITY

DATENSCHUTZ

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?
- Welches 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

Cyberwehr

Teilnehmer der Allianz für Cyber-Sicherheit

IT-BESTENLISTE BEST OF 2021 mittelstand BEST OF

IST IHRE IT SICHER?

Sind Sie sicher, dass Ihre IT sicher ist? Die neuesten Branchenzahlen und Meldungen gängiger Nachrichtendienste sprechen da eine ganz klare Sprache. IT- und Cyber-Angriffe nehmen zu und zwar massiv. Es vergeht nahezu keine Woche in dem es keine erfolgreichen Angriffe gibt. Vor keiner Branche und Unternehmensgröße wird Halt gemacht. Alle sind potenziell gefährdet.

Mein klarer Appell: Das Bewusstsein und Handeln zu mehr IT Security muss steigen, um gegen die digitalen Gefahren jetzt und in Zukunft gewappnet zu sein!

Das klingt komplex – und das ist es auch! Doch mit den richtigen Bausteinen ist auch diese Aufgabe erfolgreich und vor allem so sicher wie möglich zu meistern.

WO BEGINNEN?

Ein guter Start ist immer am Anfang. Passend hierzu finden Sie auf den ersten Seiten dieser Ausgabe (ab S. 5) unseren Leitfaden ‚Ihr Weg zu (mehr) IT Security im Unternehmen'. Mit diesem Wissen im Gepäck legen Sie die Basis um die weiteren Schritte in die richtige Richtung zu gehen, den weiteren Weg gehen wir zusammen. An welchen Stellschrauben bei Ihnen gedreht werden muss, zeigen wir Ihnen auf mit unserem Security Audit (S. 20). Und welche Werkzeuge und Lösungen dafür passend für Sie und Ihr Unternehmen sind erfahren Sie ab S. 26.

CONNECTING MEDIA

Als IT-Lösungsanbieter aus dem Raum Karlsruhe haben wir uns sichere Digitalisierung auf die Fahne geschrieben mit der klaren Bekenntnis zu IT Security. Gemeinsam mit unseren Lösungspartnern machen wir IT-Systeme sicherer, dabei fokussieren wir uns auf Lösungsansätze ‚made in Germany'. Vom Stecker bis hin 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.

Ihr Andreas Kunz
CEO & Gründer, Connecting Media

P.S.: Schnappen Sie sich gleich unsere IT-Notfallkarte (links zum Raustrennen) für Ihre Pinnwand und seien Sie immer sicher aufgestellt!

Inhaltsverzeichnis

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

Der Weg zur IT Security in Ihrem Unternehmen

ZUM EINSTIEG

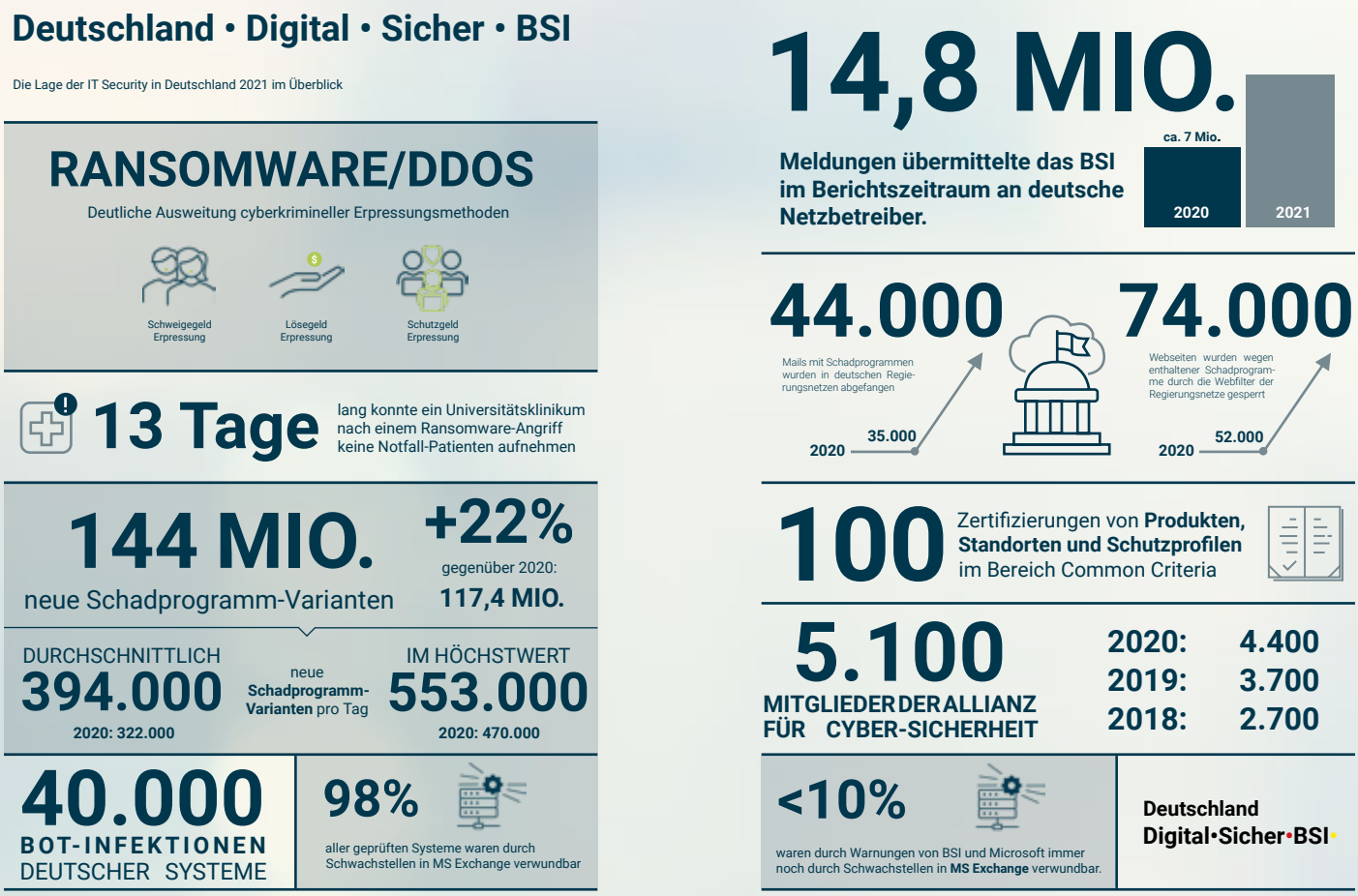
Sichere Rahmenbedingungen sind die Basis aller Digitalisierungsvorhaben Ihres Unternehmens. Durch den intensiv erlebten Digitalisierungsboom der letzten Jahre nehmen nicht nur die völlig neuen Möglichkeiten exponentiell zu, sondern geradezu im Gleichschritt auch die Gefahren. Das Thema IT Security ist mittlerweile 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 2021, ist nun umso mehr bewusst geworden, dass hier dringender Nachholbedarf besteht.

Keine Sorge, mit dem nun folgenden Leitfaden möchten wir aus Ihnen keinen Security Experten machen, sondern unsere Erfahrung der letzten 20 Jahre aus nationalen und internationalen IT Security Projekten teilen. Der Leitfaden ist 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. Denn IT Security bleibt nicht stehen, sie ändert sich täglich.

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 des Tages derjenige der die Verantwortung für dieses Thema übernehmen muss.

Wir haben Ihnen dieses Thema so zugänglich wie möglich aufbereitet, damit Sie umgehend mit den ersten Schritten in die Umsetzung starten können.



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

Bausteine einer Sicherheitskultur

Wie bei vielen unternehmerischen Entscheidungen und Tätigkeiten ist es auch in Bezug auf IT und Cybersicherheit wichtig sich auf gewisse Grundbausteine vorab zu einigen mit einer klaren Definition. Auf diese sollten Sie keineswegs verzichten, da diese über Erfolg oder Misserfolg Ihrer Sicherheitskultur entscheiden wird. 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 Webshop 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***

Auch branchenspezifische Richtlinien dürfen nicht außer Acht gelassen werden, 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.

Das heißt u.a. den Kompetenzerwerb zu fördern, etwa durch Motivationsmittel, Schulungen und Informationsveranstaltungen. Wer Commitment zeigt und mit gutem Vorbild vorangeht, ist glaubwürdig und darf auch Commitment erwarten.

Definition Informationssicherheit

Kommen wir nun zum spannenden Punkt: Was ist überhaupt diese Informationssicherheit und wie ist diese charakterisiert?

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

- ***Vertraulichkeit: Informationen sind nur berechtigten Personen zugänglich***
- ***Integrität: Informationen sind vor unrechtmäßiger oder außerplanmäßiger Veränderung gesichert***
- ***Verfügbarkeit: 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 bewusst, 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***

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 hinein – also 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***

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***

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 der neuesten Erhebung des Branchenverbandes Bitkom e.V. entstanden im Jahr 2020/2021 deutschen Unternehmen Schäden in Höhe von 223 Milliarden Euro durch Diebstahl, Spionage oder Sabotage. 2018/2019 waren es noch 103 Milliarden Euro. Neun von zehn Unternehmen waren nach Angaben der Bitkom direkt von Cyber-Angriffen betroffen.

Informationen werden nicht ausschließlich von digitalen Angreifern mit böswilligen Absichten bedroht. Auch die eigenen Mitarbeiter können – mutwillig oder versehentlich – eine 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 definitiv 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.

Gefahren durch Cyberkriminalität

Der Branchenverband Bitkom e.V. spricht von Rekordschäden durch Cyberangriffe, das Bundesamt für Informationstechnik (BSI) bewertet im Lagebericht 2021 die IT Security Lage als angespannt bis kritisch: Noch nie waren Cyberattacken so gefährlich für Unternehmen in Deutschland wie heute!

Beide Organisationen untermauern ihre Aussagen mit konkreten Zahlen. Die Bitkom beziffert die Schadenssumme, die die Cyberkriminalität der deutschen Wirtschaft kostet, auf 220 Milliarden Euro pro Jahr. Diese Summe ist mehr als doppelt so hoch wie im Vergleichszeitraum 2018/2019. Hauptverantwortlich für diese Entwicklung seien Erpressungsvorfälle, die durch Ransomware-Angriffe ausgelöst wurden.

Das BSI wiederum verzeichneten im Februar 2021 den höchsten jemals gemessenen Wert an neuen Schadprogramm-Varianten. Über den kompletten Berichtszeitraum gesehen (Juni 2020 bis Mai 2021), seien 144 Millionen neue Schadprogramm-Varianten aufgetaucht – ein Plus von 22 % gegenüber dem Vorjahreszeitraum. Erschwerend komme hinzu, dass Cyberkriminelle ihre Angriffe stetig weiterentwickelten. Bei Ransomware-Attacken etwa, wird, neben Lösegeldforderungen, immer häufiger mit der Veröffentlichung der gestohlenen Daten gedroht.

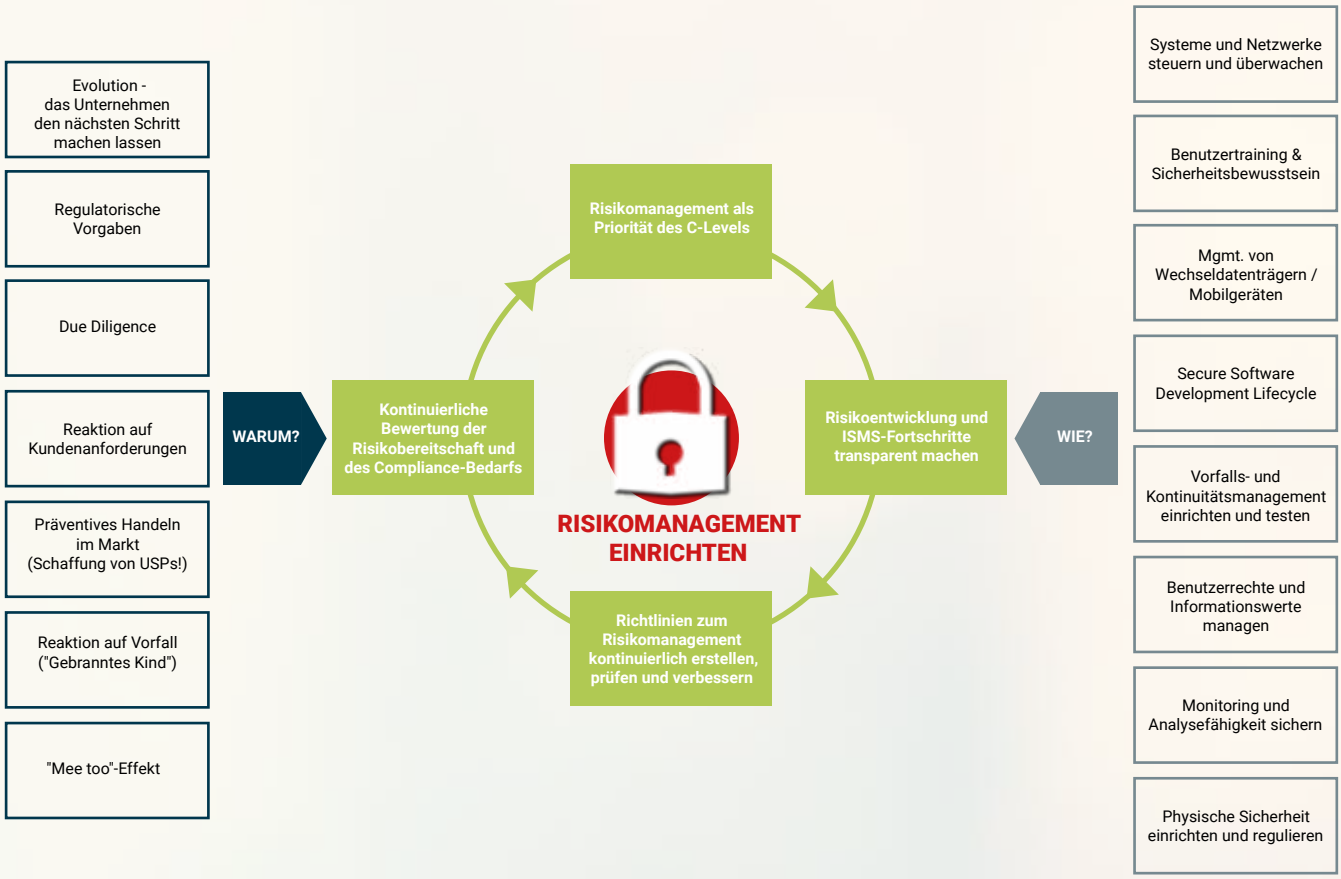
Auch auf geistiges Eigentum haben Hacker es laut der Bitkom-Studie abgesehen. So heißt es in einem Pressebericht: *„Geistiges Eigentum wie Patente oder Forschungsinformationen wurden bei 18 % gestohlen – ein Plus von 11 Prozentpunkten gegenüber den Jahren 2018/2019."* Für den innovationsgetriebenen deutschen Markt führt der Verlust geistigen Eigentums zu potenziell besonders hohen Schäden.

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 sind – und 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.



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

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. Denn die technisch organisatorischen Maßnahmen (TOM) sind nichts anderes als Ihr ISMS ‚light'. Nämlich welche Maßnahmen das Unternehmen wie sicher stellt.

Für die Einführung eines ISMS gibt es viele gute Gründe. 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.

Hinzu kommen 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. 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.

Name	Umfang	Außenwirkung
TOM (EU-DSGVO)	Recht überschaubar und nicht zeitaufwändig. Auch gibt es hier kein klares Regelwerk in puncto must have und Umsetzung	Man wird als „macht“ nur das nötigste wahrgenommen, keine „richtige“ Vergleichbarkeit
VdS 10005	Speziell auf die Bedürfnis- und Ressourcenstruktur von KKU sowie von Handwerksbetrieben mit bis zu 20 Mitarbeitern ausgelegt	Mindestanforderungen an die Informationssicherheit für KKU
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+	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
VdS 10000	Definiert Mindestanforderungen an ein Managementsystem für die Informationssicherheit für KMU	Testat über implementierte technische und organisatorische Massnahmen auf Wirkung der wichtigsten Angriffsszenarien
VDA-ISA TISAX	Je nach Grad der TISAX 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 (35 Maßnahmenziele (Controls) mit 114 konkreten Maßnahmen zu verschiedensten Sicherheitsaspekten)	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 48-50).*

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.*

Quellen:

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

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

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

Die passenden Lösungsbausteine für Ihre Herausforderungen!

LÖSUNG	LÖSUNGSPARTNER	SEITE
Authentifizierung	SAYTEC AG	
Backup	Acronis International GmbH	
Berechtigungsmanagement	Makro Factory GmbH & Co. KG	
Cloud	Azure by Microsoft Corp.	
Cloud Service	**Connecting Media**	**21**
Compliance	Varonis Systems GmbH	
Cyberpolice	Dr. Hörtkorn München GmbH	
Datensicherheit	Varonis Systems GmbH	
Datenschutz & Cookie Consent	**comply**	**42-43**
Digitale Zusammenarbeit	Microsoft Teams	
DNS Security	**Blue Shield Security GmbH**	**38-39**
DSGVO	Andreas Kunz	
Datenschutz Managementsystem (DSMS)	Intervalid GmbH	
Edge Computing	**Scale Computing**	**40-41**
E-Mail Security	Hornetsecurity GmbH	
E-Mail-Archivierung	Hornetsecurity GmbH	
E-Mail-Verschlüsselung	Seclous GmbH	
Endpoint Management	Riverbird GmbH	
Endpoint Security	BlackFog, Inc.	
Endpoint Security	Inlyse GmbH	
Fernwartung	Supremo | Nanosystems Srl	
Fernzugriff	**Soliton Systems Europe N.V.**	**30-31**
Firewall/UTM	**Securepoint GmbH**	**44-45**
Firewall/UTM	LANCOM Systems GmbH	
Healthcare	MEDIGATE	
Industrie 4.0	DataOS GmbH	
Inudstriepolice	Dr. Hörtkorn München GmbH	
Informationssicherheitsmanagementsystem	Confluence	
IT Sicherheitsgutachten	Andreas Kunz	
Managementsysteme (ISO, VdS, TISAX...)	**ISOSchmiede by Connecting Media**	**52-53**
Microsoft 365	Microsoft Corp.	
Mobile Security	BlackFog, Inc.	
Mobile Security	**Securepoint GmbH**	**44-45**
Monitoring	**Connecting Media Control Center (CMCC)**	**18-19**
Network Access Control (NAC)	**Soliton Systems Europe N.V.**	**30-31**
Netzwerkperformance	Enginsight GmbH	
OT-Sicherheit	DataOS GmbH	
Passwortmanagement	LastPass	
Patchmanagement	**Connecting Media Control Center (CMCC)**	**18-19**
Pentesting	**Security Audit by Connecting Media**	**20**
Schulungen	**Connecting Media**	**12-13**
Schwachstellenscanning	A1 Digital Deutschland GmbH	
Schwachstellenscanning	Enginsight GmbH	
SD-WAN	LANCOM Systems GmbH	
Server Security	BlackFog, Inc.	
SIEM	**Connecting Media Service Cockpit (CMSC)**	**28-29**
SOAR	Enginsight GmbH	
Switche	LANCOM Systems GmbH	
Telefonanlage	**GoTo Connect**	**32-34**
Training (IT Security)	**Securepoint GmbH**	**44-45**
Videokonferenz	**GoTo Meeting & GoTo Webinar**	**32-34**
Videokonferenz	Starleaf GmbH	
Virtualisierung	**Scale Computing**	**40-41**
Virtual Private Network (VPN)	SAYTEC AG	
WLAN	LANCOM Systems GmbH	

Erleben Sie uns 24/7 in unserem digitalen Ausstellungsraum.
Erleben statt nur sehen!

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.

Als Start-up sind wir 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.

SECURITY AUDIT

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 Analyse Ihres IT Security Zustandes. (S. 20)

WEB-CHECK

Die Webpräsenz ist das Aushängeschild Ihres Unternehmens. Um so wichtiger ist es daher einen professionellen und gesetzeskonformen Auftritt zu haben. Mit unseren teilautomatisierten Web-Checks decken wir sämtliche Angriffspunkte und Gesetzesabweichungen Ihres Webauftritts oder Online-Shops auf.

Connecting Media

COMPLIANCE-CHECK

Sicherheit gibt es nicht nur in der IT - es gibt gesetzliche Anforderungen wie die DSGVO sowie organisatorische Optimierungsmöglichkeiten um die Angriffsfläche zu minimieren. Mit unserem detaillierten Compliance-Check schaffen wir für Sie eine optimale und verständliche Entscheidungsgrundlage um Maßnahmen gezielt und kostenoptimiert ergreifen zu können.

IT SERVICE

Organisieren Sie Ihren 1st & 2nd Level Support effektiv, oder vertrauen Sie uns diesen gleich ganz an, um sich wichtigeren Dingen in Ihrer IT zu widmen. Eine Lösung Made in Germany, die dafür sorgt, dass Ihre Daten auch sicher in Deutschland bleiben. Lokal gehostet in Ihrem System, sichere Verarbeitung der Daten in unserer Private Cloud. Versuchen Sie nicht zu managen was Sie nicht kontrollieren können!

Unser komplettes Lösungs-Portfolio finden Sie unter www.connectingmedia.de

CMCC

CONNECTING MEDIA CONTROL CENTER

Mehr Transparenz in Ihrem Netzwerk - Mehr Zeit für Wichtigeres

Verschaffen Sie sich einen Überblick über alle Systeme Ihres Netzwerkes, überprüfen Sie jedes einzelne Endgerät auf mögliche Sicherheitslücken und beheben Sie diese ohne Umwege. **Und das alles mit nur wenigen Klicks!**

Organisieren Sie Ihren 1st & 2nd Level Support effektiv, oder vertrauen Sie uns diesen gleich ganz an. Eine Lösung made in Germany, die dafür sorgt, dass Ihre Daten auch sicher in Deutschland bleiben. Lokal gehostet in Ihrem System und sichere Verarbeitung Ihrer Daten in unserer Private Cloud.

Unser Baukasten für Ihre einfache, zuverlässige und umfassende Kontrolle über Ihr Netzwerk

NETZWERKKONTROLLE

RiverSuite Monitoring überwacht Ihr Netzwerk rund um die Uhr und macht Sie auf Probleme aufmerksam, bevor diese zu Notfällen werden.

- *Vermeiden Sie Leistungsengpässe und liefern Sie eine bessere Service-Qualität durch proaktives Handeln*
- *Reduzieren Sie Kosten durch bedarfsgerechte Anschaffungen und erhöhen Sie Ihren Gewinn, indem Sie Ausfallzeiten minimieren*
- *Beruhigt zurück lehnen: Solange Sie keine Warnungen von RiverSuite Monitoring erhalten, wissen Sie, dass alle Komponenten wie erwartet funktionieren*

INVENTARISIERUNG

Endlich werden Dokumentationen Ihres Netzwerks einfach. Erhalten Sie sowohl eine optimale Dokumentation als auch das integrierte Monitoring aus einer Hand.

Alle Daten an einer zentralen Stelle. Prüfen Sie beliebig viele Systeme, und halten Sie mit der RiverSuite Inventory Ihre IT-Infrastruktur sowie die Ihrer Kunden und Partner auf dem aktuellen Stand.

Mit Lösungen zur Sicherheitsanalyse des Netzwerkes, dem integrierten Compliance-Management, einer ausgefeilten Berechtigungsanalyse auf Dateisystem-Ebene und vielen weiteren Funktionen erhalten Sie die optimale Lösung für Ihre IT.

PATCHMANAGEMENT

Halten Sie die Endgeräte (Clients & Server)

Ihrer Kunden mit dem Patchmanagement von Riverbird stets aktuell. Über den Paketmanager werden im RiverSuite Inventory immer die neusten 3rd Party Updates mit Ihrem System synchronisiert. Anschließend können Sie Software komfortabel neu verteilen oder auch updaten.

SECURITY

Bekannte Sicherheitslücken schließen:

RiverSuite Inventory gleicht die verwendete Software Ihrer inventarisierten Kunden mit einer CVE Datenbank ab und hilft Ihnen Schwachstellen in den Systemen zu finden. Alle wichtigen Informationen werden dabei übersichtlich im Security Dashboard dargestellt.

REPORTING

Problemlose Dokumentation:

RiverSuite bietet Ihnen umfangreiche und einfache Möglichkeiten Berichte zu erzeugen. Somit kommen Sie Ihren Nachweispflichten problemlos nach und sichern sich belastbar ab.

BENUTZER CONTROL CENTER

Selbsterklärendes Informationsportal für Endbenutzer:

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

BERECHTIGUNGSANALYSE

Komplexe Informationen verständlich aufbereitet:

Jederzeit aussagekräftige und aktuelle Berichte über die effektive Berechtigungssituation im Unternehmensnetzwerk. Korrekte IT-Dokumentation für Führungskräfte, Datenschutzbeauftragte und IT-Administratoren.

UND NOCH MEHR

Kundenportal:

Übersicht aller Tickets und Aufträge, Ansprechpartner und Bearbeitungsstati.

Weitere Tools für Ihren Werkzeugkasten:

RiverSuite stellt zahlreiche zusätzliche Funktionen und Features bereit, die Ihnen die Betreuung Ihres Netzwerkes und der Benutzer weiter vereinfacht.

Kontakt
+49 7243 99 167-10
vertrieb@connectingmedia.de

SECURITY AUDIT

Sicherheit durch Sichtbarkeit

Für die meisten Unternehmen stellt die IT-Infrastruktur einen zentralen Schaffungsort Ihrer Produkte und Dienstleistungen dar. Egal, ob es sich hierbei um Computerarbeitsplätze für Mitarbeiter, Netzwerkfreigaben, Drucker oder andere Komponenten handelt. Dabei liegen unserer Erfahrung nach viele sensitive Informationen, wie Kundendaten oder Geschäftsgeheimnisse nahezu ungeschützt und teilweise frei zugänglich im Unternehmensnetzwerk.

Jede Entscheidung ist eine Investition, ob in Sicherheit und Stabilität oder in Risiko.

"Unternehmen können nicht nicht investieren"

Geld und Zeit das man bewusst nicht in die Prävention, also in die IT-Stabilität (Ausfallsicherheit) oder die Reduzierung von möglichen Datenschutzverstößen und IT Security Vorfällen investiert sind Dark-Side-Investments.

Um eine fundierte Entscheidung treffen zu können bedarf es einer ebenso soliden Grundlage. Für die meisten Entscheidungsträger ist es jedoch schwer eine objektive Entscheidungsgrundlage zu erhalten, da nicht jeder tief in technischen und organisatorischen Themen zuhause ist.

Wir versetzen Sie mit unserem IT-Security Audit in die Lage fundierte Entscheidungen für Ihr Unternehmen zu treffen und es somit aktiv zu schützen. Der hier vorgestellte Pentest beinhaltet eine Sicherheitsanalyse Ihrer internen IT-Infrastruktur aus der Perspektive eines internen Angreifers (Blackbox). Wir simulieren einen Angreifer mit Zugriff auf das interne Netzwerk und versuchen, Schwachstellen wie bspw. veraltete Softwareversionen, schwache Zugriffskontrollen oder Fehlkonfigurationen, zu identifizieren.

Interne Netzwerke bieten Angreifern viele interessante und lukrative Angriffsziele, welche in der Regel weniger stark abgesichert sind als die öffentlich erreichbaren Systeme eines Unternehmens. Unsere Tests beinhalten einen automatisierten Schwachstellenscan sowie eine manuelle Analyse und Auswertung durch unsere IT Security Spezialisten. Als zertifizierte Datenschützer achten wir hierbei besonders auf die Einhaltung der DSGVO-Richtlinien.

Erkennen Sie Schwachstellen, bevor es ein anderer tut!

Weitere Informationen und die Terminvereinbarung finden Sie unter www.secaud.it

CLOUD SERVICES

Cloud mit höchsten Standards

Alle Cloud Services betreiben wir für Sie im Hochverfügbarkeitsrechenzentrum der Telemaxx Telekommunikations GmbH in Karlsruhe. Es verfügt über Zertifizierungen nach ISO 27001 und TÜVIT EN50600 Verfügbarkeitsklasse 3.

Pentest as a Service (PaaS):
-Schwachstellen erkennen, bevor es ein anderer tut-

Sie erhalten Zugriff auf unsere Engine und können mit uns zusammen jederzeit die Sicherheit Ihrer Umgebung prüfen. Mit dem passenden Team aus Security Spezialisten werden auch komplexe Sachverhalte verständlich aufgedeckt.

Backup (BaaS):
- Ihre Daten sind bei uns sicher-

Mit unserer Lösung sparen Sie den Kauf und die Wartung von Backup-Servern, das tägliche Aufbewahren der Sicherungsbänder und gehen dem Risiko aus dem Wege, dass ein Backup-Vorgang vergessen wird.

Reporting (RaaS):
- Jederzeit Transparenz –

Unsere Services und Dienstleistungen sind keine Blackbox. Durch unseren Reporting Service wissen Sie jederzeit wo Sie IT technisch stehen. Egal ob es um das Nachvollziehen von Tätigkeiten geht oder als Planungsgrundlage für Neuanschaffungen bzw. strategischen Ausrichtungen. Mit unserem Reporting Service sind Sie jederzeit proaktiv handlungsfähig zum Betrieb Ihrer IT.

Infrastruktur (IaaS):
-Leistung auf Knopfdruck-

Sie erhalten flexiblen Zugriff auf hochleistungsstarke Infrastruktur, ohne weitere administrative Aufwände zu erzeugen. Wartung und Pflege übernehmen wir. Dabei kann die Leistung jederzeit flexibel angepasst werden.

Monitoring (MaaS):
-Behalten Sie alles im Blick-

Mit unserem Monitoring haben Sie jederzeit einen Überblick über Ihre Umgebung. Unser Team kann jederzeit unterstützen und frühzeitig auf Herausforderungen reagieren, bevor es zu Problemen kommt.

Security Operation Center (SOCaaS):
-Vorsicht ist besser als Nachsicht-

Warten Sie nicht, bis die Infiltration bereits stattgefunden hat! Lassen Sie Ihre Systeme durch ein SOC rund um die Uhr überwachen und seien Sie in der Lage, schnellstmöglich auf Anomalien zu reagieren. Gemeinsam mit unserem Security Team, sind Sie stets den entschiedenen Schritt voraus.

KUNDENSTIMMEN

Unsere Projekte und Aufgabengebiete sind so vielseitig wie unsere Kunden. Das sagen unsere Auftraggeber über unsere vergangene Zusammenarbeit.

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. Herrn Radovic und Herrn Pusch gilt noch ein besonderer Dank für Ihre Geduld mit uns. Es gab kein Problem bzw. Anliegen was nicht in kürzester Zeit gelöst wurde. Wir bedanken uns herzlichst für diese großartige Arbeit und empfehlen Connecting Media jederzeit weiter.

KM TGA
HAUSTECHNIK VON MORGEN
HEUTE GEPLANT.

Gemeinschaftspraxis Claudia Obert & Patrick Näher

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.

Autohaus Müller GmbH
persönlich · kompetent · zuverlässig

fintag Finanzdienstleistungs- und Treuhand AG

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.

cosack
DRUCK + VERPACKUNG SEIT 1833

Nagel Kunststoffe
Thermoplastische Kunststoffe

Katja Nagel
Geschäftsführerin
KN Nagel Kunststoffe e. K.

Am Anfang der Zusammenarbeit mit Connecting Media war ein großes Anliegen, unsere IT auf den neuesten Stand zu bringen. Dies betraf sowohl die Hardware als auch digitale Fragestellungen wie Backup und Schutzkonzepte oder auch unsere Webseite. Kombiniert war dies mit dem Wechsel unseres Standorts, den Connecting Media mit begleiten konnte. Nachdem wir intensiv mit Connecting Media zusammenarbeitet, können wir uns nun ganz auf unsere Kerngebiete konzentrieren und wissen unsere IT in den besten Händen gestellt.

Fachtagung IT Security & Datenschutz

01.+ 02. Juni 2022

Hotel 47°, Konstanz

Lassen Sie als Unternehmen keinen Raum für digitale Gefahren

- » Treffpunkt für Entscheider des Mittelstandes auf Augenhöhe mit IT Security Experten
- » hochaktuelle Themen hautnah an der Praxis diskutieren
- » Lösungsansätze und Fragestellungen verständlich und übersichtlich aufbereitet

Wir freuen uns Sie an Bord begrüßen zu dürfen!

Sponsored by

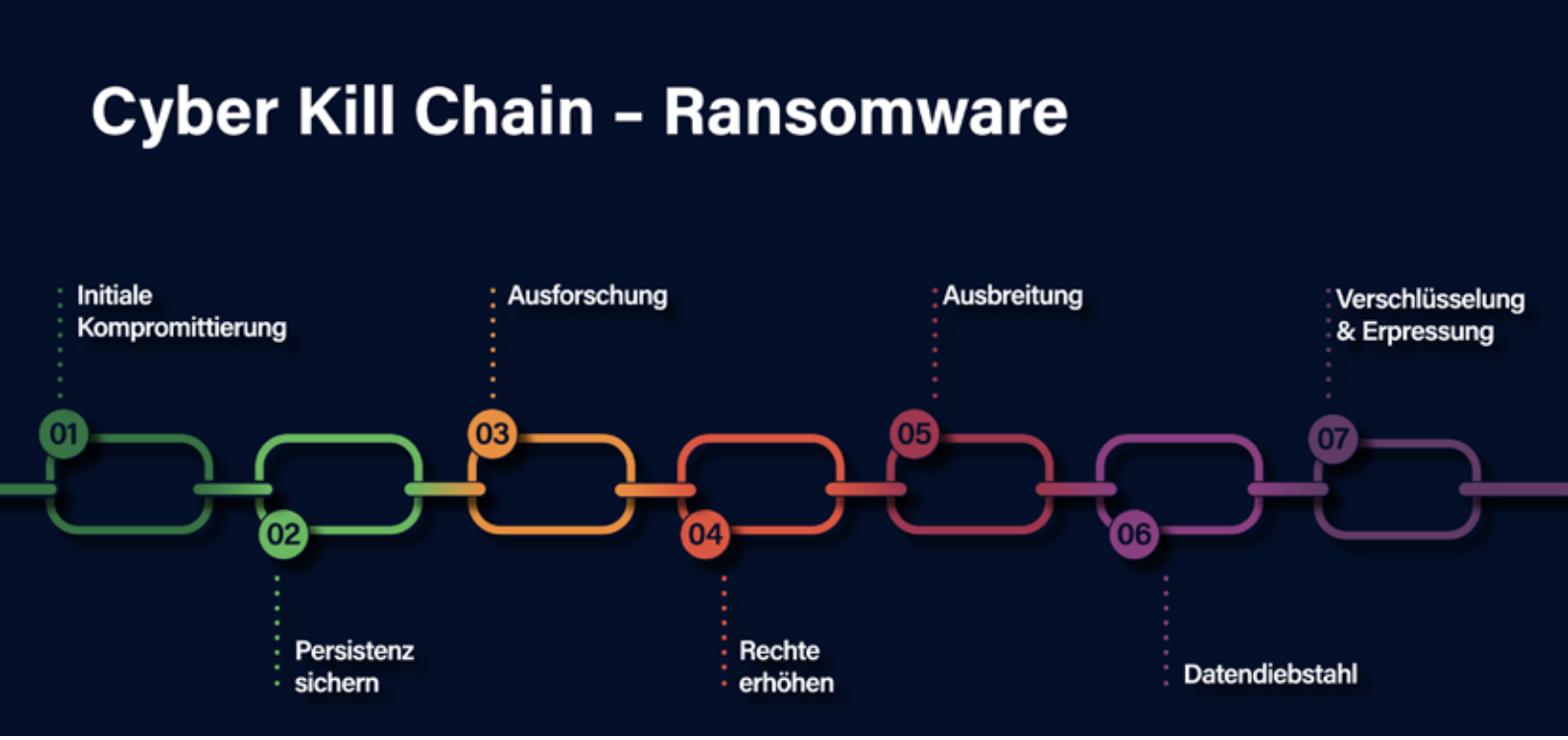
GoTo

»CYBERSENSE

LANCOM SYSTEMS

SECURITYCRUISE.DE · SECURITYCRUISE.DE

SecurityCruise



»CYBERSENSE

ADVANCED DECEPTION

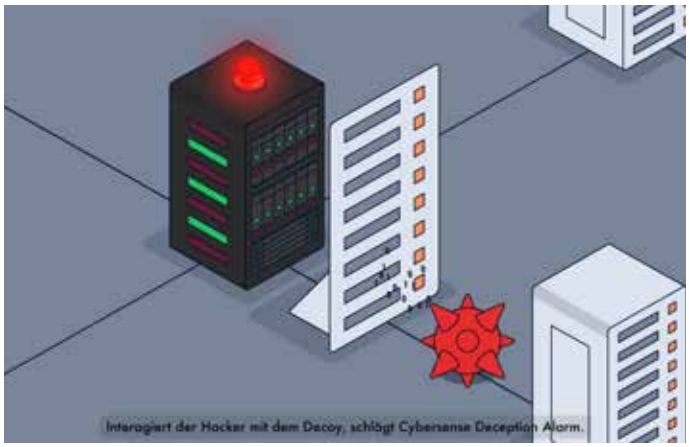
Für jedes Unternehmen und jede Einrichtung ist es heute selbstverständlich, dass man eine mehr oder weniger leistungsfähige Firewall am Internetzugang und einen Virenschutz am Endgerät einsetzt, um sich vor bösartigen Angriffen zu schützen.
Dieser rudimentäre „Grundschutz“ reicht aber bei den heutigen Angriffsszenarien nicht mehr aus. Angreifer schaffen es immer häufiger den Perimeter zu überwinden und/oder den Virenschutz zu umgehen und in Netzwerke einzudringen.

EINBRUCHSERKENNUNG EINFACH UND WIRKSAM

Der CYBERSENSE MANAGED SERVICE erkennt Einbrüche in Ihr Unternehmensnetzwerk einfach und wirksam. Cybersense basiert auf einem komplementären Ansatz, der unabhängig von vorhandenen Sicherheitssystemen funktioniert. Während seiner Erkundungsphase nutzt der Angreifer präparierte Informationen, deren Nutzung sofortigen Alarm auslöst. Der Angreifer hat keine Chance zu erkennen, ob er echte, wertvolle Daten oder von Cybersense vorgetäuschte Informationen erbeutet hat.

EINBRÜCHE ERKENNEN BEVOR SCHADEN ENTSTEHT

Schaden entsteht, weil erfolgreiche Angriffe nicht oder zu spät entdeckt werden. Im Durchschnitt bewegen sich Angreifer > 6 Monate unbemerkt in Unternehmensnetzwerken. Mit viel Kreativität und Einfallsreichtum überwinden sie immer wieder innovative und intelligente Sicherheitssysteme. Die Zahl erfolgreicher Angriffe steigt trotz aller Gegenmaßnahmen.



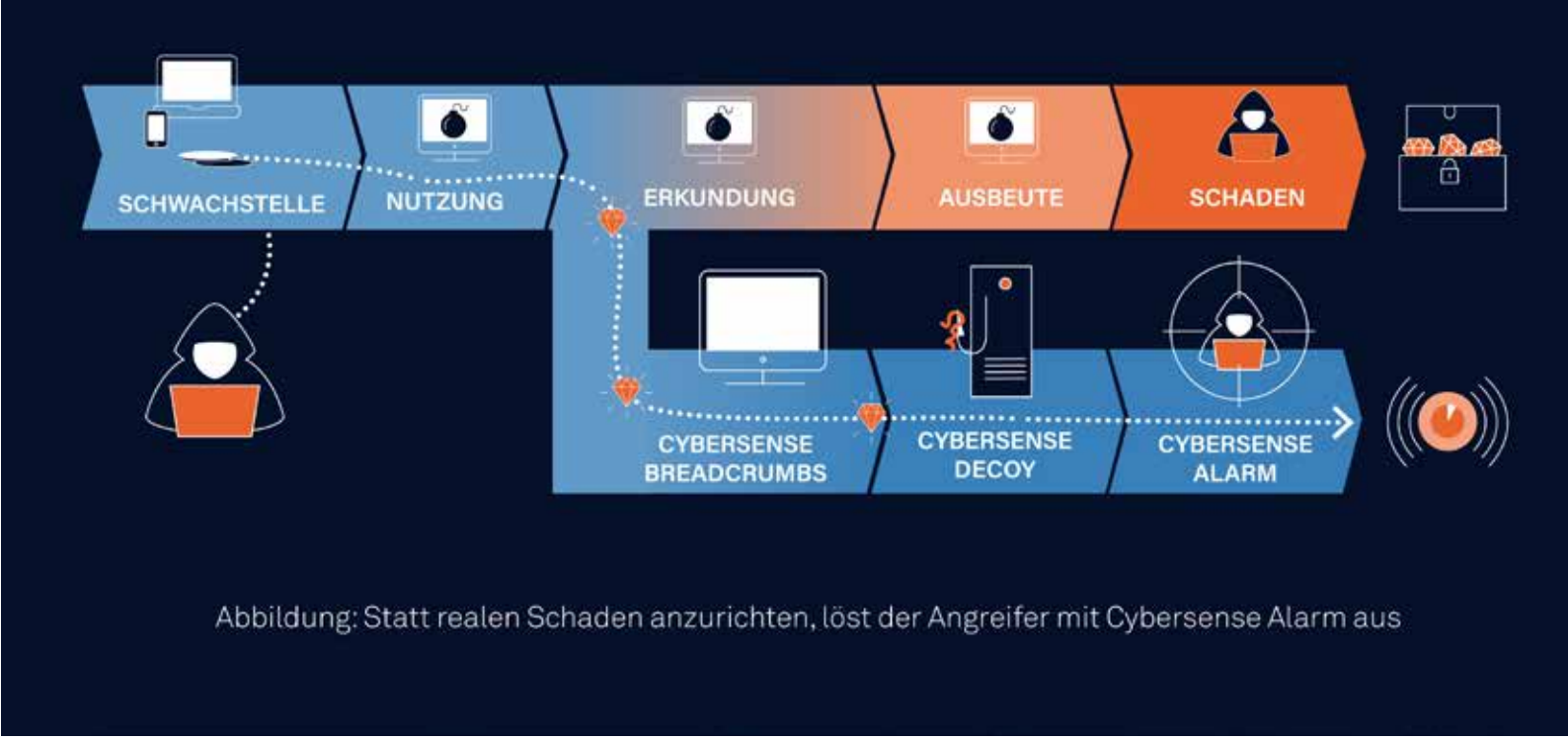


Abbildung: Statt realen Schaden anzurichten, löst der Angreifer mit Cybersense Alarm aus

DAS VORGEHEN VON ANGREIFERN

Die meisten Einbrüche basieren nicht auf den berüchtigten, hochkomplexen Angriffen. Vielmehr stehen dem Angreifer alle digitalen, sozialen oder physischen Methoden zur Verfügung, um sich einen ersten Eintrittspunkt zu verschaffen. Hier ist der Angreifer klar im Vorteil. Hat er erst einmal Zugang bekommen - meist mit geringen Nutzerrechten - versucht er, unter Nutzung einschlägiger Angriffstools, seine Befugnisse im Unternehmensnetz zu erweitern und seine Spuren zu verwischen. Hier ist die Schwachstelle des Angreifers, die sich Cybersense zunutze macht. Er befindet sich in einem ihm vollkommen unbekannten Netzwerk und muss diese Umgebung zuerst erkunden. Zwar wird der Angreifer sehr vorsichtig vorgehen, aber letztlich muss er die wenigen erbeuteten Informationen nutzen, um mehr Informationen zu bekommen. Cybersense infiltriert diesen Erkundungsprozess und bietet vorgetäuschte Informationen, die sofortigen Alarm auslösen.

DIE VORTEILE VON CYBERSENSE ADVANCED DECEPTION AUF EINEN BLICK

» FRÜHZEITIGE ANGRIFFSERKENNUNG
Alarmierung in der Erkundungsphase des Angreifers

» AGENTENLOS
Keine zusätzliche Software auf Clients oder Servern notwendig

» KOMPLEMENTÄR
Unabhängig von der vorhandenen Sicherheitsinfrastruktur

» BETRIEBSSICHER
Stört vorhandene IT nicht, ideal auch in KRITIS-Umgebungen

» KEINE FEHLALARME
Nur die absichtliche Nutzung von Breadcrumbs löst Alarm aus

» SCHONT PERSONALRESSOURCEN
Bindet keine Personalressourcen im täglichen Betrieb

CMSC

Connecting Media 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 Connecting Media 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.

Ein Schweizer Taschenmesser

Für jeden Use Case das passende Konzept: Als Hardwareappliance mit integrierter USV, virtueller Umgebung wie Hyper V und VMWare oder als Managed Service über eine private Cloudinfrastruktur (nach ISO 27001) gehostet in einem deutschen Rechenzentrum.

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

Lückenlose Überwachung und einfache System-Inventarisierung

Das CMSC 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 ServiceCockpit 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 | A³ 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.

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

All-in-One NAC für jedermann

Hand aufs Herz: Gehören Sie zu einem der vielen Unternehmen, die immer noch versuchen, ohne Netzwerkzugangskontrolle über die Runden zu kommen?

NetAttest EPS ist eine Enterprise taugliche NAC-Lösung, die bereits bei zahlreichen führenden Unternehmen zum Einsatz kommt. Wir haben die Lösung für KMU erschwinglich gemacht – jetzt können auch Sie davon profitieren.

Heutzutage ist eine effektive Netzwerkzugangskontrolle unverzichtbar für jeden Betrieb, der ein Netzwerk betreibt. NAC-Systeme sorgen dafür, dass sich nur die richtigen Benutzer mit der richtigen Authentifizierung im Netzwerk anmelden können. Sobald sie Zugriff darauf haben, regelt das NAC-System innerhalb des Netzwerks die Bereiche, auf die Benutzer zugreifen können, und überwacht und protokolliert deren Aktivitäten.

Der fortschreitende Trend zu hybriden Arbeitsmodellen und die kontinuierliche Weiterentwicklung von Angriffsvektoren sorgt bei IT Security Experten immer wieder für unliebsame Überraschungen. Mehr denn je wird eine effektive NAC benötigt, um heute und auch in Zukunft sicher arbeiten zu können.

Allerdings benötigen die IT-Teams eine moderne NAC, die sich mühelos und unkompliziert einführen und verwalten lässt. Möchten Sie mehr darüber erfahren?

Netzwerksicherheit von der Stange für jedermann

Soliton ist seit 2001 Marktführer im Bereich der Netzwerkzugangskontrolle und unsere NetAttest EPS kommt heute bei zahlreichen weltweit führenden Unternehmen zum Einsatz.

Wir haben in enger Zusammenarbeit mit unseren Kunden eine All-in-One NAC-Lösung entworfen, dank der die Komplexität und der enorme Aufwand, den eine gängige Netzwerkzugangskontrolle in der Regel mit sich bringt, ab heute Vergangenheit ist.

Soliton liefert eine All in One Lösung – alle nötigen Features sind bereits in NetAttest EPS integriert und in den erschwinglichen Pro-Benutzer-Lizenzgebühren enthalten. Es gibt keine versteckten Zusatzkosten und es wird auch kein hochqualifiziertes Personal für den Betrieb benötigt – das heißt, Sie werden künftig auch davon profitieren, dass Ihre Benutzer nicht mehr andauernd den IT-Support um Rat fragen müssen.

High-End-Security mit zertifikatsbasierter Authentifizierung

Mithilfe der zertifikatsbasierten Authentifizierung können Sie überprüfen, ob alle mit einem Netzwerk verbundenen Geräte autorisiert sind – auch wenn sie nicht von Ihnen administriert werden. Digitale Zertifikate ermöglichen es den Benutzern, gleich von Beginn an auf die richtigen Bereiche des Netzwerks zuzugreifen, was die Anfragen an die IT-Support-Teams reduziert.

Mit den Zertifikaten lassen sich auch Authentifizierungszyklen automatisieren – man muss also nicht mehr selbst daran denken, Benutzerberechtigungen zu verlängern oder zu löschen.

»Wir müssen unsere Benutzer authentifizieren, um sicherzustellen, dass nur autorisierte Benutzer Zugriff erhalten. Mit der zertifikatsbasierten Authentifizierung können wir den Benutzerzugriff und unseren Onboarding- und Offboarding-Prozess automatisieren.«

Sie behalten vom Anfang bis zum Ende die volle Kontrolle über den gesamten Authentifizierungsprozess, da Sie das Ende bereits zu Beginn Ihrer Authentifizierung festlegen. Sobald das Zertifikat abläuft, können die betreffenden Benutzer nicht mehr auf Ihre Ressourcen zugreifen.

Müheloser Einstieg in nur 5 Minuten

Der Lösungsansatz von Soliton besteht darin, die Komplexität zu verringern und eine einfache Kontrolle und Verwaltung durch die IT-Abteilung zu ermöglichen. Dank der assistentengestützten Installation von NetAttest EPS ist ein einfacher Einstieg ohne spezielle Fachkenntnisse möglich.

NAC ist mehr als nur eine Sicherheitslösung – sie hilft Ihnen, ein produktives Arbeitsumfeld für Ihr Team und ein beeindruckendes, nahtloses Erlebnis für Ihre Gäste zu schaffen.

Um Funktionalität in den vernetzten Umgebungen von heute zu gewährleisten und diversen Personen Zugriff zu Ihrem Netzwerk gewähren zu können, benötigen Sie für Ihr Unternehmen das beste auf dem Markt verfügbare NAC-System. Ihre Daten sind zu wertvoll, um sie irgendeinem Anbieter anzuvertrauen.

Sichere Geschäftskommunikation mit GoTo Connect

HERAUSFORDERUNG

Connecting Media ist zwar ein Kleinunternehmen, betreut aber Kunden vom Friseurladen nebenan bis in zum Dax-Unternehmen. Außerdem ist man nicht nur regional, sondern auch überregional in der DACH-Region vertreten. Und genau hier lag laut Andreas Kunz, Gründer und Geschäftsführer von Connecting Media, die große Herausforderung. „Wir standen also vor der Aufgabe, einen Anbieter für Cloud-Telefonanlagen zu finden, der nicht nur unseren Anspruch an IT-Security und Datenschutz erfüllt, sondern auch den unserer Kunden. Darüber hinaus suchten wir nach einer Telefonlösung, die uns auch beim Thema Teamintegration Arbeit abnimmt“, erklärt Kunz gleich zu Beginn.

„Mit dem Thema Cloud-Telefonie beschäftigen wir uns zwar schon ziemlich lange, doch seit unserer Gründung im Jahr 2017 hatten wir nie den einen Anbieter an der Hand, der uns voll und ganz überzeugen konnte“, berichtet der Connecting Media Gründer. Doch das sollte sich schon bald ändern.

Ein Glück, dass Connecting Media seinerzeit vom GoTo Channel Team kontaktiert wurde: „Ich muss gestehen, bis dato war mir GoTo kein Begriff, ich war aber sehr gespannt, was dieser für mich neue Anbieter zu zeigen hatte“, erinnert sich Kunz an dieser Stelle. Und das war so einiges. Kurze Zeit später lernte der Connecting Media Geschäftsführer einen Vertriebsmitarbeiter kennen, der einen technischen Pitch zu der Telefonielösung von **GoTo Connect, der Voice-over-IP-Telefonanlage, machte und damit beim Gründer voll ins Schwarze traf.** Dabei handelt es sich um eine Telefonanlage, bei der alles digital abläuft– ein herkömmlicher Telefonanschluss ist nicht erforderlich.

Alle Gespräche werden über eine Internetverbindung geführt „Ich saß also beim Pitch und fragte mich, warum wir diese geniale Lösung eigentlich nicht anbieten. Von GoTo Connect war ich von Tag eins so begeistert, dass ich gleich Nägel mit Köpfen machte und die Telefonanlage in unser Produktportfolio mit aufnahm“, bringt Kunz das Szenario auf den Punkt und fügt hinzu: „Mein Credo lautet hier, dass wir unseren Kunden nur das verkaufen, was wir auch selbst im Einsatz haben.“ Mit GoTo vertraut und mit GoTo Connect gut aufgestellt, war die Suche nach einer professionellen Telefonanlage für Connecting Media also abgeschlossen.

LÖSUNG

Die Integration und Einbindung von GoTo Connect machte für Connecting Media vieles einfacher: „Hier hat wirklich von Beginn an alles gestimmt – so auch der Preis, wenn man sich mal vor Augen führt, was die Anlage alles kann“, erklärt der Gründer und berichtet weiter: „Meine Begeisterung geht schon soweit, dass ich fast nur noch GoTo Connect pitche.“ Besonders überzeugt haben Kunz aber die einfache Bedienbarkeit und die Benutzeroberfläche: Gerade im Vergleich mit anderen Anbietern ist die Bedienbarkeit keine Raketenwissenschaft. Bei GoTo Connect muss ich nicht erst mal zwei Tage in Schulungscentern sitzen, damit ich wirklich verstehe, wo die einzelnen Häkchen zu setzen sind“, erklärt der Connecting Media Inhaber und fügt noch hinzu: „Ich bin übrigens ein Riesenfan vom Drag-&-Drop-Editor– den lieb ich ja.“

Weiter stellt der Vollbluttechniker klar, dass die Aufnahme eines neuen Produkts ins Portfolio alles andere als ein Selbstläufer ist. „Ich bin besonders skeptisch, wenn ich einen neuen Hersteller mit ins Boothole, weil ich hier Schulungsaufwand habe. Heißt im Klartext: Ich muss meine Techniker briefen“, betont Kunz an dieser Stelle und lobt: „Bei GoTo Connect ist das nicht der Fall. **Alles läuft sehr intuitiv – ich verschwende hier keine Zeit im Meetingraum, sondern bekomme das Produkt direkt auf die Straße.“**

Auch in Sachen Kundenservice und Professionalität hat das Unternehmen große Schritte nach vorne gemacht. Mit der Integration von GoToConnect hatte man nicht mehr „nur“ eine gefühlte Erreichbarkeit, sondern eine gelebte. „Wir hatten jetzt die Möglichkeit, unterschiedliche Sprachnachrichten aufzunehmen. Innerhalb der Geschäftszeiten hat der Kunde die Möglichkeit, per Knopfdruck zu entscheiden, ob er beispielsweise mit dem Vertrieb, der Buchhaltung oder dem Support verbunden werden möchte. Außerhalb der Geschäftszeiten werden dem Kunden weitere Ansagen ausgespielt. Es ist hier ganz einfach, Kunden richtig abzuholen. **Das hat nicht nur unser Auftreten nach außen, sondern auch unsere Flexibilität enorm verbessert“**, lobt Kunz.

„Mit GoTo Connect wollten wir uns breiter und professioneller aufstellen – diese Ziele haben wir übertroffen. Bei unseren Kunden punkten wir mit gelebter Erreichbarkeit und absoluter Sicherheit, bei unseren Mitarbeitern mit einfacher Bedienbarkeit und Integration.”

Andreas Kunz,
Geschäftsführer
und Gründer,
Connecting Media

Wichtig für den Technikexperten war außerdem, dass man die Telefonanlage auf mehrere PCs und Endgeräte ausrollen kann: „Und das ist bei GoTo Connect problemlos möglich. Der Übergang zwischen mehreren Endgeräten läuft immer gut und flüssig“ betont Kunz an dieser Stelle.

Außerdem konnte Connecting Media über GoTo Connect sicherstellen, dass neue Mitarbeiter einfach und schnell ins Unternehmen integriert werden: „Das Anlegen neuer Mitarbeiter ist wirklich ein Kinderspiel. Wenn ich da an andere Tools denke, musste ich von einem Untermenü zum nächsten springen, um einen Mitarbeiter einer Rufgruppe hinzuzufügen. Das hat mich dann immer nicht nur viel Zeit, sondern auch Nerven gekostet. Bei GoTo Connect sind das jetzt zwei Klicks und der User ist im Profil“ sagt der Gründer mit einem zufriedenen Lächeln. Auf das Thema Implementierung angesprochen muss Kunz kurz auflachen „Ganz ehrlich, das Onboarding war nach zwei Stunden abgehakt. Anschließend hat dann auch alles funktioniert – das war zwar tough, aber auch richtig cool“, erzählt der Inhaber von Connecting Media rückblickend.

ERGEBNIS

Mit GoToConnect hat Connecting Media nicht nur das Produktportfolio weiter ausgebaut, sondern auch viele Arbeitsprozesse erleichtert – intern, aber auch extern. „Aufgrund der Einfachheit und des breiten Feature-Sets bei GoToConnect arbeiten wir viel effizienter. Wenn wir den Service beim User übernehmen, haben wir vor allem in der Technik wenig Aufwand und können so mehr Kunden betreuen“, macht Kunz deutlich.

Auch den Faktor Sicherheit, der bei Connecting Media großgeschrieben wird, konnte man mithilfe von GoToConnect perfekt abdecken. Das Unternehmen wollte eine Telefonanlage integrieren, die es ihm erlaubt, auch mit Großunternehmen zusammenzuarbeiten. Und das ist Connecting Media als Ziel gelungen. „Da wir auch Dax-Konzerne betreuen und im Security-Umfeld tätig sind, haben wir hohe Anforderungen an die Verschlüsselungstechnik. **GoToConnect hat uns hier von Anfang an überzeugt – und das bis heute“**, lobt der Gründer.

#Unternehmenssicherheit

ZOOM MEETING | VOR ORT | IM STREAM

FRÜHLING 04. - 07. APRIL 2022
HERBST 14. - 17. NOVEMBER 2022

SECURITY WEEK

EINE WOCHE KNOW-HOW, KONTAKTE UND INSPIRATION!

04. APRIL - KEINE CLOUD IST KEINE OPTION
05. APRIL - TAUZIEHEN UM TALENTE
06. APRIL - KRITIS & CYBER WAR
07. APRIL - IT SECURITY IST MARKTVORTEIL

ANMELDUNG

WWW.SECURITY-WEEK.DE

Sichere Passwörter mit LastPass

LastPass •••|

Die Zahlen sprechen eine deutliche Sprache: Laut Statista haben 46% aller deutschen Unternehmen im Jahr 2021 mindestens einen Hackerangriff erlebt. Dabei sind 80 % aller Datenschutzverletzungen auf schwache, wiederverwendete oder gestohlene Passwörter zurückzuführen.

Fakt ist: Ohne tadellose Passwortgewohnheiten sind solche Datenschutzverletzungen unvermeidlich. Aber herkömmliche Passwortverwaltungsmethoden können sowohl für Mitarbeitende als auch Administratoren eine Überforderung darstellen.

Die interessante Frage ist hier also, wie Unternehmen die Passworthygiene und Sicherheitsverhalten Ihrer Teams verbessern können, ohne dadurch an Benutzerfreundlichkeit für Mitarbeitende und Administratoren einzubüßen.

LastPass bietet Sicherheit und erstklassige User Experience

LastPass unterstützt Mitarbeitende, indem es die Belastungen sowohl für AnwenderInnen als auch für IT-Teams reduziert. Sie sparen Zeit mit einer einfachen, zentralen Passwortverwaltung und Administratoren profitieren von einer umsetzbaren Überwachung durch erweiterte Berichterstattung und über 100 konfigurierbare Sicherheitsrichtlinien.

-Keine Wiederverwendung von Passwörtern mehr: Der integrierte Passwortgenerator von LastPass sorgt für eine gute Passworthygiene der Mitarbeitenden.

-Zentrale Passwortverwaltung: Mitarbeitende erhalten einen eigenen personalisierten Passwort-Vault, während Admins mit einem robusten Admin-Dashboard den Überblick behalten.

-Der Schutz sensibler Daten: Mit dem Sicherheitsmodell nach dem Zero-Knowledge-Prinzip von LastPass werden Zugangsdaten, Notizen und Informationen sicher aufbewahrt.

-Einfache und sichere Passwortfreigabe: Sichere Freigabe von Zugangsdaten an Teammitglieder und Verwaltung freigegebener Zugangsdaten über Gruppen.

Weltweit überzeugende IT Security

LastPass überzeugt: Bereits mehr als 25 Millionen User und 70.000 Unternehmen weltweit arbeiten mit LastPass für mehr IT Security und eine erstklassige User Experience.
Das wird regelmäßig honoriert: 2021 mit dem „Global-InfoSecAward“ und dem „CyberSecurity Breakthrough Award“, 2022 mit dem „Trust Radius Award“ und einem „Sehr gut“ beim CHIP Test „Die besten Passwort-Manager 2022“.

Gewappnet sein im Cyberkrieg: Blue Shield hat KI-Defensivwaffe

Der SolarWinds-Hack im Dezember des Vorjahres ist der größte Hackerangriff der US-Geschichte „und definitiv ein Game-Changer, dessen Folgen sich noch nicht abschätzen lassen“, sagt der Cyber-Security-Spezialist Avi Kravitz, seit Anfang 2020 im Expertenbeirat der Blue Shield Security GmbH mit Sitz in Linz-Leonding.
Mit dem Beginn des Ukrainekriegs haben sich die Cyberangriffe potenziert. Es bedarf einer Defensivwaffe, die neuartige Cyberbedrohungen erkennen und abwehren kann. Blue Shield hat mit dem Blue Shield Umbrella eine derartige Defensivwaffe entwickelt und ständig weiterentwickelt, sodass mit den neuesten Methoden der Künstlichen Intelligenz ein System auf White List Basis entwickelt wurde, das vollkommen neue Bedrohungen in Echtzeit erkennen kann. Eine Weltneuheit im Bereich der DNS Threat Intelligence. Made in Austria.

Der SolarWinds-Hack im Dezember wurde bereits ausführlich erforscht: Betroffen waren mehr als 18.000 Unternehmen und Organisationen weltweit, welche die Software des texanischen Netzwerkmanagement-Spezialisten SolarWinds verwenden. Hinter dieser raffinierten Attacke wird eine geballte Macht von 1.000 Programmierern vermutet – eine Attacke, die in mehreren Stufen abgelaufen ist. Motto: Wer SolarWinds hackt, hackt auch seine Kunden. Und die Kunden der Kunden. Einem Bericht des „Wall Street Journal“ zufolge, hatten 30 Prozent der angegriffenen Unternehmen keine direkte Verbindung zu SolarWinds. Alles begann Monate vorher mit einem präparierten Update der SolarWinds-Software namens „Orion“. Mit dieser Installation schufen sich die Hacker eine Hintertür ins jeweilige System.

Die betroffenen Unternehmen sind teilweise das Who‘s Who der Technologie-Giganten mit fortgeschrittenem Sicherheitsbewusstsein. Und dieses Beispiel veranschaulicht hier deutlich: Wir benötigen bessere Schutz- und Detektionsmöglichkeiten. Die Angreifer waren etwa neun Monate aktiv, bevor es irgendjemand (durch Zufall!) gemerkt hat! Die Angreifer seien mindestens zwei Schritte voraus.

Warum Zero Day Prävention

Es bedarf daher neuer Lösungen und Konzepte, um solche Cyberattacken systematisch erkennen zu können. Und es wird ein IT Security-System benötigt, das schlauer ist als die Angreifer – oder eines, das ein Eindringen von Schadsoftware von vornherein verhindert. Wie es geht, zeigte der heimische Anbieter Blue Shield Security, der mit dem auf künstliche Intelligenz basierten IT Security-System „Blue Shield Umbrella“ alle seine Kunden vor diesem Angriff schützen konnte.

Warum Blue Shield Umbrella sicher ist

„Während andere IT Security Lösungen meist mit einem Blacklist-basierten Ansatz arbeiten, der aber voraussetzt, dass der Schädling bereits bekannt ist, verfolgen wir einen gänzlich anderen Ansatz. Blue Shield Umbrella ist der erste auf KI basierte WhiteList- bzw. AllowList-DNS-Filter der Welt, der die Schadsoftware erst gar nicht ins System lässt und somit ein Infektionsrisiko von Anfang an ausschließt“, sagt Avi Kravitz. Der Cyber-Security-Experte ist davon überzeugt, dass dieser Angriff durch Blue Shield Umbrella hätte verhindert werden können – weltweit.

Über Blue-Shield

Das Blue-Shield-Headquarter mit mehr als 30 Beschäftigten im Bereich Forschung und Entwicklung befindet sich in Leonding bei Linz. Der seit 2015 in Österreich entwickelte Blue Shield Umbrella ist ein cloudbasiertes System und der weltweit einzige Whitelist-/Allowlist-Filter auf Basis künstlicher Intelligenz.

BlueShield

Digitale Souveränität bewahren!

Services und Dienste outzusourcen oder in die Cloud zu bringen muss nicht für jedes Unternehmen der richtige Ansatz sein. Diese Verantwortung auszulagern oder gar abzutreten kann personelle, finanzielle und materielle Ressourcen einsparen, aber seien Sie sich bewusst, dass Ihre digitale Souveränität darunter leidet.

Dahingegen behalten Sie bei Betrieb Ihrer eigenen Cloud, einer sogenannten private Cloud, Ihre digitale Souveränität und sind weiterhin Herr Ihrer Daten.

IT so einfach wie ein Smartphone

Mit der HC3 All-in-One-HCI Plattform von Scale Computing erhalten Sie einfachste und effizienteste IT-Infrastruktur der Welt.

Ein dezentraler Standort, so klein oder groß er auch sein kann, muss ebenso hohe Sicherheitsstandards erfüllen, wie das Rechenzentrum, daher bringt die HC3-Lösung grundlegenden Features der HCI-Architektur mit, dazu zählen:

- Absolute Einfachheit und Hochverfügbarkeit
- Redundanz, Ausfallsicherheit und selbstheilende Architektur
- Belastbarkeit und Notfallwiederherstellung auch as a Service

Einsatzgebiete

•Als klassisches Data Center on prem beim Kunden oder für Partner mit Manages Service Provider Ansatz, um Kunden Services bereitzustellen

•Außerhalb des Data Centers als Edge Computing Lösung in Außenstandorten, Produktionslokationen, Retailstores, Windkraftanlagen oder auch auf Handelsschiffen

•Als Business Resiliance System, um Backup und Disaster Recovery abzubilden

•Sowie Sicherheit im Unternehmen aufzugreifen, als Video Surveillance Plattform zum Managen tausender Kameras und Auswertung oder Speichern des Bildmaterials.

Die HC3-Plattform ist als Appliance konzipiert und integriert, als speziell gehärtetes System, besondere Merkmale, die die Sicherheit erhöhen:

•Ein Update ist getestet und validiert, schließt sämtlich Hardwarekomponenten wie z. B. BIOS oder Firmware mit ein, so dass mit einem Klick ohne Unterbrechung des Betriebs, das Hard- und Softwareupdate durchgeführt wird

•Ein Zugriff auf den Cluster bzw. Knoten, seitens des Supports, kann nur nach Freigabe erfolgen, es besteht kein Zugriff des Scale Computing HC3 Systems direkt auf die virtuellen Maschinen und das System „telefoniert“ nicht nach Hause, hieraus entstehen keine versehentlichen Sicherheitslücken

•Die Einfachheit des Systems ermöglicht eine Bedienung ohne spezielle Kenntnisse oder eine Notwendigkeit von fortlaufenden, zeit- und kostenintensiven Schulungen

Die Scale Computing HC3 Plattform stellt insofern eine besondere Infrastruktur Lösung dar, als das Szenarien auf kleinsten Raum abgebildet werden können und somit sehr niedrige Anschaffungskosten entstehen. Nebst geringem Platzbedarf wird dadurch auch der Energiebedarf für Strom und Klima massiv gesenkt und der CO2 Ausstoß sinkt rapide.

Die Möglichkeit unterschiedliche Knoten über „Mix & Match“ mit anderen Modellen zu mischen, z. B. auch Knoten mit unterschiedlichen CPU-(Generationen), führt zu transparenten Kosten, Planbarkeit und einer langen und flexiblen Einsatzdauer der Systeme. Mit all diesen Möglichkeiten ist ein Cloud-ähnlicher Einsatz ganz einfach möglich.

Scale Computing wurde gegründet, um den Bedarf von Unternehmen zu decken, die durch Komplexität, Zeit und Ressourcen behindert werden, die herkömmliche virtualisierte IT-Umgebungen zunehmend erfordern. Heute liefert Scale Computing IT-Infrastrukturlösungen für Edge-Computing, Virtualisierung und hyperconvergente Lösungen für Kunden weltweit. Die Scale Computing HC3®-Software macht herkömmliche Virtualisierungssoftware, Disaster Recovery Software, Server und gemeinsam genutzten Speicher überflüssig und ersetzt diese durch ein vollständig integriertes, hochverfügbares System zum Ausführen von Anwendungen.

Diese Auszeichnungen (Auszug) sprechen für unsere Lösungen:

THE CHANNEL CO. CRN ARC ANNUAL REPORT CARD WINNER 2021

Gartner peerinsights customers' choice 2021

STORAGE MAGAZINE PRODUCTS OF THE YEAR 2021 FINALIST 20TH ANNIVERSARY

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2021

Datenschutz erleichtern

Wie sagt man so schön: Vertrauen ist gut, Kontrolle ist besser!

Gerade in Bezug auf IT und Cyber Security trifft dieser Ansatz voll und ganz zu. Und das immer stärker. Zugegebenermaßen sind diese Themen komplex und zeitaufwendig. Wichtig ist umso mehr, den Einstieg so einfach wie möglich zu machen. Das schaffen wir mit unseren Sicherheits-Scans für das Einfallstor Webseite.

Einfallstor Webseite

In der heutigen Zeit ist die Webseite eines Unternehmens oftmals der erste Angriffspunkt - insbesondere, wenn Angreifer wissen, dass potentiell wertvolle und sensible Daten zu holen sind. Daher ist es wichtig, frühstmöglich über die zugrundeliegenden Sicherheitsrisiken, die einen solchen Vorfall ermöglichen, informiert zu sein.

Mit unserem Sicherheits-Scan auf Knopfdruck scannen Sie ab sofort Ihre Webseiten auf Sicherheitskriterien und -schwachstellen und minimieren so die Angriffsfläche. Positiver Nebeneffekt für Sie: Sie sagen auf Wiedersehen zu nervigen auszufüllenden Checklisten!

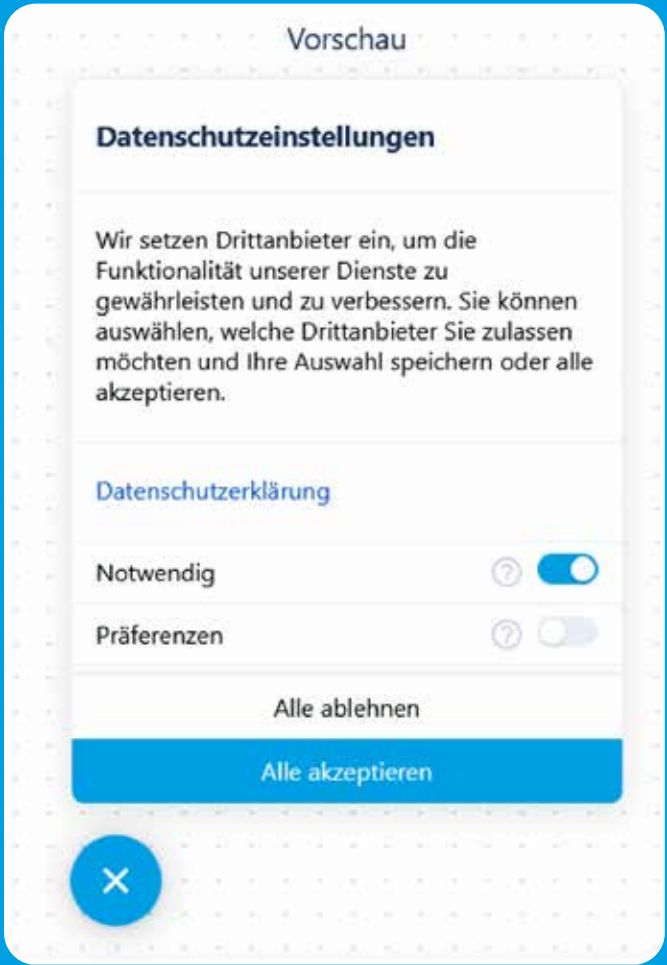
Zentrale Sicherstellung der digitalen DSGVO-Konformität

DSGVO Scan:
DSGVO-Cookie-Konformitätstest
Testen Sie, ob Ihre Website die DSGVO-Anforderungen zur Zustimmung von Cookies erfüllt.

Webseiten Monitoring:
Mit unserem Monitoring-System vollautomatisch Webseiten auf DSGVO-Konformität überprüfen. Dadurch werden Sie automatisch informiert, sobald sich etwas relevantes an Ihrer Website ändert, um proaktiv eingreifen zu können.

Consent Management:
Stellen Sie den Nutzern Ihrer Website einen transparenten und übersichtlichen Manager zur Verfügung, um wählen zu können welche Cookies genutzt werden. Durch einfache Anpassung an Ihr Firmenerscheinungsbild, fügt sich der Consentmanager optimal in Ihre bestehende Seite ein.

Datenschutzerklärung:
Durch vorgefertigte, rechtskonforme Textbausteine zu mehr als 1100 Webservices, ist Ihre Datenschutzerklärung immer aktuell und gepflegt.




comply

SECUREPOINT

IHR STÄRKSTER SCHUTZ: EIN HELLWACHES TEAM

SCHLAUER ALS JEDE K.I. ES SEIN KÖNNTE.

Geschärfte Aufmerksamkeit für versteckte Cyberangriffe schützt die IT-Sicherheit von Unternehmen nachhaltig. Etablieren Sie jetzt eine echte Sicherheitskultur durch interaktive Trainings.

Awareness PLUS

Cyber-Security-Trainings mit Wirkung

Jetzt entdecken: securepoint.de/ap

www.securepoint.de • Tel.: 04131 240 10 • info@securepoint.de

Cyber-Security-Training mit Wirkung

Unachtsamkeit oder mangelndes Verständnis von Angestellten ist eine der größten Bedrohungen für die Cybersicherheit von Unternehmen. Ihr stärkster Schutz vor Viren und Trojanern: Ein hellwaches Team. Mit Cybersecurity-Trainings etablieren Sie eine nachhaltige Sicherheitskultur, die Ihr Unternehmen und Ihre Mitarbeitenden gleichermaßen schützt.

Die aktuelle „WEKA Online-Studie Cyber Security 2021“ identifiziert ungeschulte Mitarbeitende als eine der größten Bedrohungen für die Cybersicherheit von Unternehmen. Der Einsatz von E-Mail, Smartphone und Laptop birgt Risiken, die ohne entsprechendes Training oft falsch eingeschätzt werden. Zugleich nimmt die Bedrohungslage für Unternehmen zu: Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden im Jahr 2021 pro Tag im Schnitt 394.000 neue Malware-Varianten veröffentlicht.

Gerade die zunehmende Verbreitung von Homeoffice und mobilem Arbeiten hat in vielen Unternehmen für neue Angriffspunkte gesorgt. Oft fehlen dann technische Maßnahmen, die richtigen Prozesse und das passende Wissen. Vor allem viele kleine und mittlere Unternehmen haben ihr eigenes Risiko in diesem Zusammenhang lange unterschätzt. Die Untersuchungsergebnisse der WEKA-Studie zeigen vor allem in kleinen und mittleren Unternehmen (KMU) eine eklatante Lücke bei der Analyse aktueller Cyber-Gefahren und den daraus resultierenden IT Security Maßnahmen auf.

Ihr Team als bester Schutz

„Mit Awareness PLUS steht nun erstmals eine umfassende E-Learning-Plattform mit realistischen Phishing-Simulationen und umfassenden Analysemöglichkeiten speziell für KMU zur Verfügung. Die Awareness-Schulungen haben das Ziel, jeden einzelnen User und Mitarbeitenden in KMU so auszubilden, dass er oder sie wissen, welches Verhalten bei bestimmten IT-Vorfällen richtig ist oder zum Risiko werden kann“, erläutert Eric Kaiser, Product Management Director bei Securepoint. Das Ergebnis des erfolgreichen Trainings: Das größte Risiko wird zum besten Schutz und aus einem ungeschulten Team eine „human firewall“.

Ihr Unternehmen erhält mit Awareness PLUS eine moderne E-Learning-Plattform mit multimedialen Lernmodulen und zahlreichen spielerischen Elementen. Der integrierte Gamification-Ansatz führt durch Punkte und Abzeichen zu erhöhter Lernmotivation. Inhaltlich bietet das Training elf multimediale und interaktive Lernmodule zum Thema IT Security. Mit regelmäßigen, branchenspezifisch zugeschnittenen Simulationen von Cyber-Attacken wird die Trainingsqualität weiter erhöht. Durch Analysen und Dashboards wird der weitere Fortbildungsbedarf visualisiert.

Dank anonymisierter Ergebnisse ist Awareness PLUS datenschutzkonform einsetzbar. Als deutscher Anbieter von IT Security Lösungen bietet Securepoint Cybersecurtiy-Trainings "made in Germany" mit Servern innerhalb Europas.

Bilden Sie Ihr Team zur „Human Firewall“ aus – stärker und schlauer als jede KI es sein könnte.

Der vielfältige Nutzen einer Zertifizierung

Ohne wirksames Managementsystem kein dauerhafter wirtschaftlicher Erfolg – diese Aussage würde wohl jeder CEO vorbehaltlos unterschreiben. Geht es aber um das Thema „Zertifizierung von Managementsystemen“, sieht das schon etwas anders aus. Eine häufig gestellte Frage lautet: Braucht man die Zertifizierung wirklich?

In Unternehmen herrscht oft die Meinung, dass es vollkommen ausreicht, ein Managementsystem zu implementieren und anzuwenden, schließlich könne man dessen Wirksamkeit selbst am besten beurteilen. Oberflächlich betrachtet mag das hier und da zutreffen. Berücksichtigt man jedoch den vielfältigen Nutzen einer Zertifizierung und setzt auf nachhaltiges Wirtschaften, wendet sich das Blatt.

Warum eine Zertifizierung?

Vorausschauend agierende Unternehmen lassen ihr Managementsystem zertifizieren. Einer der häufigsten externen Gründe: Auftraggeber, Geschäftspartner oder öffentliche Stellen fordern ein Zertifikat als Voraussetzung für eine Geschäftsverbindung. Ein wesentlicher Grund von intern: der Wille des Unternehmens, mit Blick auf die Wirksamkeit und die fortlaufende Verbesserung seines Managementsystems auf Nummer sicher zu gehen, um im Wettbewerb stets die Nase vorn zu haben. Denn eine Zertifizierung signalisiert Leistungsfähigkeit und schafft Vertrauen und Transparenz – nach innen und außen.

Dabei kommt es auch auf die Reputation des Zertifizierers an: Seriöse Zertifizierungsstellen wie die DQS setzen auf „akkreditierte Zertifikate“ und bieten ihren Kunden impulsstarke Audits, Stichwort „Aufdecken von Verbesserungspotenzial“, ein höchst wertschöpfender Nutzen für das Unternehmen.

Akkreditierte Zertifikate schaffen Vertrauen

Für Zertifizierungen entlang der bekannten Managementsystemnormen wie ISO 9001 (Qualität) und einer Reihe weiterer Normen bietet die DAkkS (Deutsche Akkreditierungsstelle GmbH) Zertifizierungsstellen sog. Akkreditierungen an. Das sind Zulassungen auf der Basis einer Begutachtung, ob die Zertifizierungsstelle die Kompetenz für das Zertifizieren nach der jeweiligen Norm hat und ihrer Tätigkeit mit der gebotenen Neutralität nachgeht. Der Vorteil: An der Akkreditierung ist erkennbar, ob ein Zertifikat aussagekräftig ist oder nicht.

Der Nutzen einer Zertifizierung im Detail

Der wesentliche interne Nutzen einer Zertifizierung wird in den Zertifizierungs- und Überwachungsaudits generiert. Der Auditor wirft einen fachkundigen und neutralen Blick auf das Managementsystem und seine Prozesse. Dabei erkennt er Stärken und an welchen Stellen Handlungsbedarf besteht. Gerade in den Überwachungsaudits kann der Auditor feststellen, ob notwendige und empfohlene Maßnahmen umgesetzt wurden.

Der Zertifizierungsprozess fördert mit seinen Audits vor allem

- *die gezielte Umsetzung von Strategien*
- *das Erreichen gesetzter Ziele*
- *die fortlaufende Verbesserung des Managementsystems*
- *die Transparenz von Prozessen*
- *eine risikobasierte Herangehensweise*
- *das Unternehmensimage und damit den Zugang zu neuen Märkten*

Wie läuft eine Zertifizierung ab?

Der Ablauf einer Zertifizierung wird zu einem Gutteil von der Norm ISO/IEC 17021 vorgegeben, in Details unterscheidet sich der Vorgang jedoch nach zugrundeliegendem Regelwerk und von Zertifizierer zu Zertifizierer. Das oben aufgeführte Beispiel bezieht sich auf die Herangehensweise der DQS bei einer Zertifizierung nach ISO 9001. Der Zertifizierungsprozess durchläuft gemäß ISO/IEC 17021 unterschiedliche Phasen, vom Angebot über die Systemanalyse (Audit Stufe 1), das eigentliche Zertifizierungsaudit vor Ort und die Systembewertung bis zur Zertifikatserteilung. Das Zertifikat hat eine Gültigkeit von drei Jahren. Jährliche Überwachungsaudits vor Ort fokussieren auf wesentliche Komponenten des Managementsystems, vor allem aber auf die fortlaufende Verbesserung. Rechtzeitig vor Ablauf des Zertifikats erfolgt die Rezertifizierung.


MANAGEMENT SYSTEM
ISO
VDA-ISA TISAX
Cert+
AUDIT

„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. Im Gespräch gibt IT Security- und Datenschutzexperte Andreas Kunz, Gründer von IT-Lösungsanbieter Connecting Media, Einblicke in eine faszinierende Welt, die es zu erkunden lohnt.

Managementsysteme sind derzeit in aller Munde. Dennoch scheint bei vielen Unternehmen noch immer eine gewisse Unsicherheit 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 oftmals 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 nutzlose 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 selbstbewusst 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, Instrumente 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 Performance zu verbessern. Managementsysteme packen die Herausforderungen 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 Emissionen zu reduzieren.

Wo kommen Managementsysteme noch zum Einsatz?

Sie sind ein effektives Tool, um Abläufe und betriebliche Prozesse besser abzustimmen, zu strukturieren und zu dokumentieren, auch durch eine gesteigerte

Methodenkompetenz: 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 Arbeitsschutzes, unternehmensinterner Transparenz oder der Mitarbeitermotivation sowie die Minimierung von Fehlern und Haftungsrisiken sind weitere relevante Aspekte. Und schließlich gibt es eine Vielzahl von Managementsystemen, die sich der IT Security widmen, beispielsweise den BSI-Grundschutz, ISIS12, VdS10000 oder die ISO 27001.

Apropos Sicherheit: Sie haben Connecting Media 2017 als Systemhaus 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 nachhaltigen Sicherheitskonzepten zu versorgen. Dieser ganzheitliche Ansatz lässt sich auf andere Themenfelder übertragen. So war es für uns eine geradezu natürliche Entwicklung, auch unser Angebot und unsere Expertise in Sachen Managementsysteme 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 Managementsystem mit meinen individuellen Rahmenparametern abgleichen lässt: Das sind unter anderem die Größe des Unternehmens, die Ziele der Implementierung, deren angestrebte Durchdringungstiefe oder die Märkte, in denen ich aktiv bin: Agiere ich nur national oder muss ich auch internationalen Standards und Vergleichen standhalten? All das gilt es zu berücksichtigen. Denn nur ein passgenaues Managementsystem kann seine Wirkung voll entfalten.

Wie genau setze ich das Managementsystem dann praktisch genau 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 Betriebsblindheit 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?

Es hilft ungemein, sich zunächst einmal über die Möglichkeiten zu informieren und Orientierung zu verschaffen. Mit einer professionellen Beratung lässt sich dieser Schritt fokussiert angehen. Wir haben die Erfahrung gemacht, dass unsere kostenlosen einstündigen Erstgespräche bei unseren Kunden geradezu eine Impulswirkung entfalten, das Thema umgehend, umfänglich und fundiert anzugehen. Eine Entscheidung, 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 Managementsystem 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.

VEREINBAREN SIE UNVERBINDLICH IHREN PERSÖNLICHEN TERMIN!

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

Fachtagung IT Security & Datenschutz

01.+ 02. Juni 2022

Hotel 47°, Konstanz

Lassen Sie als Unternehmen keinen Raum für digitale Gefahren

» Treffpunkt für Entscheider des Mittelstandes auf Augenhöhe mit IT Security Experten

» hochaktuelle Themen hautnah an der Praxis diskutieren

» Lösungsansätze und Fragestellungen verständlich und übersichtlich aufbereitet

Wir freuen uns Sie an Bord begrüßen zu dürfen!

Sponsored by

GoTo

»CYBERSENSE

LANCOM SYSTEMS

SECURITYCRUISE.DE · SECURITYCRUISE.DE

SecurityCruise

MIT UNS DURCH DIE ZERTIFIZIERUNG

ANALYSE

Bestandsaufnahme der vorliegenden Dokumente und Strukturen

Erstellung Projektplan

Abschlussbericht

UMSETZUNG

Bereitstellung bewährter ISO Dokumentvorlagen

Anleitung zur Handhabung der Dokumente

Eine Korrekturschleife aller bereitgestellten ISO-relevanten Dokumente

INTERNES AUDIT

Durchführung eines internen Audits gemäß ISO-Norm

Detaillierter Auditbericht

Prozesssensibilisierung zertifizierungsverantwortlicher Mitarbeiter

ZERTIFIZIERUNG FÜR IHR UNTERNEHMEN

Wir haben für jedes Einsatzgebiet das passende Managementsystem:

- ✓ **ISO 9001**
  Qualitätsmanagement (QMS)
- ✓ **ISO 27001**
  Informationssicherheitsmanagement (ISMS)
- ✓ **ISO 14001**
  Umweltmanagement (UMS)
- ✓ **VDA-ISA TISAX**
- ✓ **Cert+**
- ✓ **VdS**

www.isoschmiede.de

UNSERE ISO BETREUUNGSPAKETE

GOLD (24 Monate Laufzeit nach Stufe 2)

- Leistungen Silber
- QMB (9001) / ISB (27001) Berater (Preis nur bei Unternehmen bis 25 Mitarbeiter)
- Beratung & Unterstützung bei folgenden Wiederholungsaudits
- Unterstützung bei Nachweiserstellungen
- 8 Arbeitsstunden inklusive für Erstellung / Update der Dokumente

SILBER (24 Monate Laufzeit nach Stufe 2)

- Leistungen Bronze
- monatliches Reviewgespräch
- Beratungsfunktion für kontinuierliche Verbesserungen
- Teilnahme am jährlichen Überwachungsaudit

BRONZE (24 Monate Laufzeit nach Stufe 2)

- jährliches internes Audit mit Auditbericht und Maßnahmenliste
- jährliches Reviewgespräch

VALIDIERUNG

Unterstützung erforderlicher Umsetzung von Haupt - und Nebenabweichungen basierend auf dem Bericht des internen Audits

Eine Korrekturschleife aller bereitgestellten ISO-relevanten Dokumente

STUFE 1

Begleitende Teilnahme am Stufe 1 Audit

Durchführung erfolgt durch externen Zertifizierungspartner
(DQS, TÜV Süd, Dekra)

FEINJUSTIERUNG

Unterstützung erforderlicher Umsetzung von Haupt - und Nebenabweichungen basierend auf dem Bericht des Stufe 1 Audits

Eine Korrekturschleife aller bereitgestellten ISO-relevanten Dokumente

STUFE 2

Begleitende Teilnahme am Stufe 2 Audit

Durchführung erfolgt durch externen Zertifizierungspartner
(DQS, TÜV Süd, Dekra)

„DIGITALISIERUNGSFIEBER“
IHR PODCAST FÜR IT SECURITY & DATENSCHUTZ!

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!

Präsentiert und moderiert von **Andreas Kunz**, Ihrem Experten in Sachen IT Security und Datenschutz!

Verfügbar auf allen gängigen Podcast-Plattformen.

Listen on Apple Podcasts

Listen on Libsyn Podcasts

Listen on Spotify Podcasts

IMPRESSUM

Connecting Media GmbH
Andreas Kunz, CEO & Founder

Am Hardtwald 7
76275 Ettlingen

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

Auflage 1.000

Die Wiedergabe von Firmennamen, Produktnamen und Logos berechtigt nicht zu der Annahme, dass diese Namen/Bezeichnungen ohne Zustimmung der jeweiligen Firmen von jedermann genutzt werden dürfen. Es handelt sich um gesetzlich oder vertraglich geschützte Namen/ Bezeichnungen, auch wenn sie im Einzelfall nicht als solche gekennzeichnet sind.

Alle Angaben sind unverbindlich, die technischen Angaben entsprechen Herstellerangaben. Keine Haftung oder Gewähr bei unzutreffenden Informationen, fehlerhaften und unterbliebenen Eintragungen. Sofern nicht anders vermerkt, stammen die Bilder von den Herstellern der abgebildeten Produkte oder wurden zur Verfügung gestellt.

Seite	Bildquelle
1	Alex;adobe.stock.com/ nuclear_lily;adobe.stock.com
5	Tierney; adobe.stock.com
15	denisismagilov; adobe.stock.com
16	natali_mis; adobe.stock.com
18	Viacheslav Lakobchuk; adobe.stock.com
20	ipopba; adobe.stock.com
25/51	Nuthawut; adobe.stock.com
38	lucadp; adobe.stock.com
46	NicoElNino; adobe.stock.com
48	Marco2811; adobe.stock.com
52	WrightStudio; adobe.stock.com