AUSGABE 3

cm magazin

0101000011010101100101 1010101010101110

DIGITALISIERUNGSFIEBER – JETZT, ABER SICHER!

IT-SECURITY

IT-SERVICE

DATENSCHUTZ

www.connectingmedia.de

NEWSLETTER!

Registrieren Sie sich für die ‚CM News' und bleiben Sie am Puls der Zeit in Sachen IT-Sicherheit, Digitalisierung & Datenschutz:

Connecting Media

www.connectingmedia.de/kontakt

Ein herzliches Hallo!

Die letzten beiden Ausgaben des CM Magazin, ja richtig, wir sind schon bei der 3. Auflage, wurden anlässig der SecurityCruise veröffentlicht, nun entkoppeln wir es und geben dem Magazin ganzjährig die Aufmerksamkeit, die es verdient. Ein bisschen finetuning haben wir wieder betrieben, denn zu optimieren gibt es immer etwas. So finden Sie in der Übersicht auf Seite 4 eine komplette Auflistung der Vielzahl unserer engeren Lösungspartner mit Themenschwerpunkt um einen noch besseren Überblick zu bekommen. Sie vermissen eine Technologie oder gar Ihre eigene? Dann sprechen Sie uns dazu an.

WER WIR SIND?

Wir sind Connecting Media, ein junger **IT-Dienstleister** aus Ettlingen bei Karlsruhe und wir haben uns Digitalisierung auf die Fahne geschrieben. Wir lieben und leben Digitalisierung und Technik, wenn möglich ‚made in Germany' oder sogar lokal aus der Ideenschmiede und Technologieregion Karlsruhe, dem Silicon Valley Deutschlands.

Mit über 20 Jahren Erfahrung in der nationalen und internationalen IT-Security Branche unterstützen wir bei den Themen **IT-Sicherheit, IT-Service, Datenschutz und Managementsysteme nach ISO**. Mehr Informationen zu unseren ausgewählten Lösungspartnern mit denen wir die Digitaliserung weiter vorantreiben finden Sie in dieser Ausgabe des CM Magazin.

Mit unserem Podcast **‚Digitalisierungsfieber'** verfügbar auf Apple Podcast, spotify Podcast und Youtube, vertiefen und informieren wir regelmäßig über spannende Themenfelder rundum IT-Sicherheit, Datenschutz und die Digitalisierung.

Viel Spaß beim Lesen, Reinhören und Nachfragen

Ihr Andreas Kunz
CEO & Gründer, Connecting Media

Wir haben für Sie immer die richtige Lösung zu Ihrem Problem!

LÖSUNG	LÖSUNGSPARTNER	
Authentifizierung	OneLogin, Inc.	
Backup	BUSYMOUSE Business Systems GmbH	
Berechtigungsmanagement	**Makrofactory GmbH & Co.KG**	**Seite 6-7**
Cloud	Azure by Microsoft Corp.	
Cloud Access Security Broker (CASB)	Bitglass, Inc.	
Cloud Hosting	BUSYMOUSE Business Systems GmbH	
Cloud Proxy	Menlo Security, Inc.	
Compliance	**Securepoint GmbH**	**Seite 8-9**
Datensicherheit	**Varonis Systems GmbH**	**Seite 10-11**
Digitale Zusammenarbeit	**Inylse GmbH**	**Seite 12-13**
Digitale Zusammenarbeit	Microsoft Teams	
DNS Security	**Blue Shield Security GmbH**	**Seite 17**
DSGVO	Andreas Kunz	
Datenschutz Managementsystem (DSMS)	Intervalid GmbH	
E-Mail Security	Hornetsecurity GmbH	
E-Mail-Archivierung	Hornetsecurity GmbH	
E-Mail-Verschlüsselung	**Seclous GmbH**	**Seite 14-15**
Endpoint Management	Riverbird GmbH	
Endpoint Security	**SentinelOne, Inc.**	**Seite 36-37**
Fernwartung	**solarwinds**	**Seite 17**
Fernzugriff (VPN)	**Safe-T**	**Seite 17**
Firewall/UTM	LANCOM Systems GmbH	
Healthcare	MEDIGATE	
Industrie 4.0	Otorio Ltd.	
Informationssicherheitsmanagementsystem (ISMS)	**Makrofactory GmbH & Co.KG**	**Seite 6-7**
IT-Sicherheitsgutachten	Andreas Kunz	
Managementsysteme (ISO, VdS)	**ISOSchmiede by Connecting Media**	**Seite 48-49**
Microsoft 365	Microsoft Corp.	
Mobile Security	**Securepoint GmbH**	**Seite 8-9**
Mobile Security	Virtual Solution AG	
Network Access Control (NAC)	**Soliton Systems Europe N.V.**	**Seite 18-19**
Netzwerkperformance	**Enginsight GmbH**	**Seite 20-21**
Netzwerkperformance	**Orion Platform by solarwinds**	**Seite 17**
Passwortmanagement	Lastpass by LogMeIn, Inc.	
Patchmanagement	**solarwinds**	**Seite 17**
Pentesting	**Enginsight GmbH**	**Seite 20-21**
Performance	**LoginVSI**	**Seite 22-23**
Scaling	**LoginVSI**	**Seite 22-23**
Schulungen	**Connecting Media**	**Seite 5**
Schwachstellenscanning	**A1 Digital Deutschland GmbH**	**Seite 17**
Schwachstellenscanning	**Enginsight GmbH**	**Seite 20-21**
SD-WAN	LANCOM Systems GmbH	
Server Security	**SentinelOne, Inc.**	**Seite 36-37**
SIEM & Monitoring	**Connecting Media Service Cockpit**	**Seite 26-27**
Simulation	**LoginVSI**	**Seite 22-23**
SOAR	**Enginsight GmbH**	**Seite 20-21**
SOAR	Otorio Ltd.	
Switche	LANCOM Systems GmbH	
Telefonanlage	GoToConnect by LogMeIn, Inc.	
Testing	**LoginVSI**	**Seite 22-23**
Versicherungen	**Dr. Hörtkorn München GmbH**	**Seite 24-25**
Videokonferenz	Starleaf GmbH	
WLAN	LANCOM Systems GmbH	
WLAN	Socialwave GmbH	

Connecting Media

Haben Sie noch genug Zeit für Ihr Kerngeschäft?

Oder frisst die Digitalisierung Ihre Ressourcen?

Unternehmer werden heute durch den technologischen Wandel mit immer komplexer werdenden IT-Systemen und völlig neuartigen Fragestellungen konfrontiert. 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.

Profitieren Sie von über 20 Jahren Erfahrung in der nationalen und internationalen IT-Branche und unserem 360°-Lösungsportfolio: 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. In jedem Fachgebiet stehen Ihnen zertifizierte Experten zur Seite. Wir betreuen unsere Kunden ganzheitlich – von der ersten Idee bis zum fertigen Projekt.

Das Portfolio von Connecting Media

IT-SECURITY
- Informationssicherheitsbeauftragter (ISB)
- Managementsystem für Informationssicherheit (ISMS)
- IT-Security Consulting & Schwachstellen-Analyse
- Awarenessschulungen & Workshops
- Software & Hardware

IT-SERVICE
- Hosting und Cloudservices
- Managed Service Provider (MSP)
- Installation, Wartung & Workshops
- Auftragsbezogene Programmierung
- Software und Hardware

DATENSCHUTZ
- Datenschutzbeauftragter (DSB)
- Datenschutzmanager (DSM)
- Datenschutzmanagementsystem (DSMS)
- DSGVO-Consulting
- Awarenessschulungen & Workshops

Profitieren Sie von unserem ausgezeichneten Service!

Cyberwehr Baden-Württemberg PARTNER 2021

Allianz für Cyber-Sicherheit Teilnehmer

IT-BESTENLISTE BEST OF 2021 initiative mittelstand BEST OF

SIEGER DES USER-VOTINGS IT-Bestenliste ★★★★★ 2019

makroaudit

Edition 2020

Intuitive Ergebnisse

Rechtzeitige Warnungen

Blitzschnelle Kontrolle

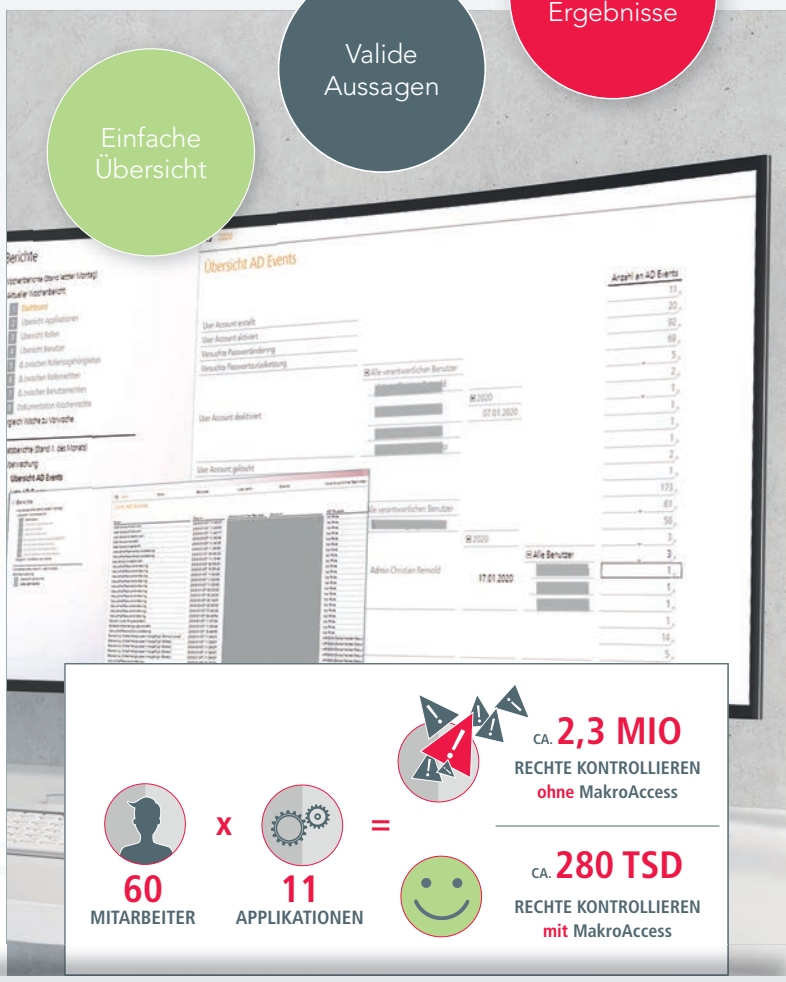
makroaccess

Edition 2020

Einfache Übersicht

Valide Aussagen

Blitzschnelle Ergebnisse



60 MITARBEITER x 11 APPLIKATIONEN =

CA. 2,3 MIO RECHTE KONTROLLIEREN ohne MakroAccess

CA. 280 TSD RECHTE KONTROLLIEREN mit MakroAccess

Über Makro Factory

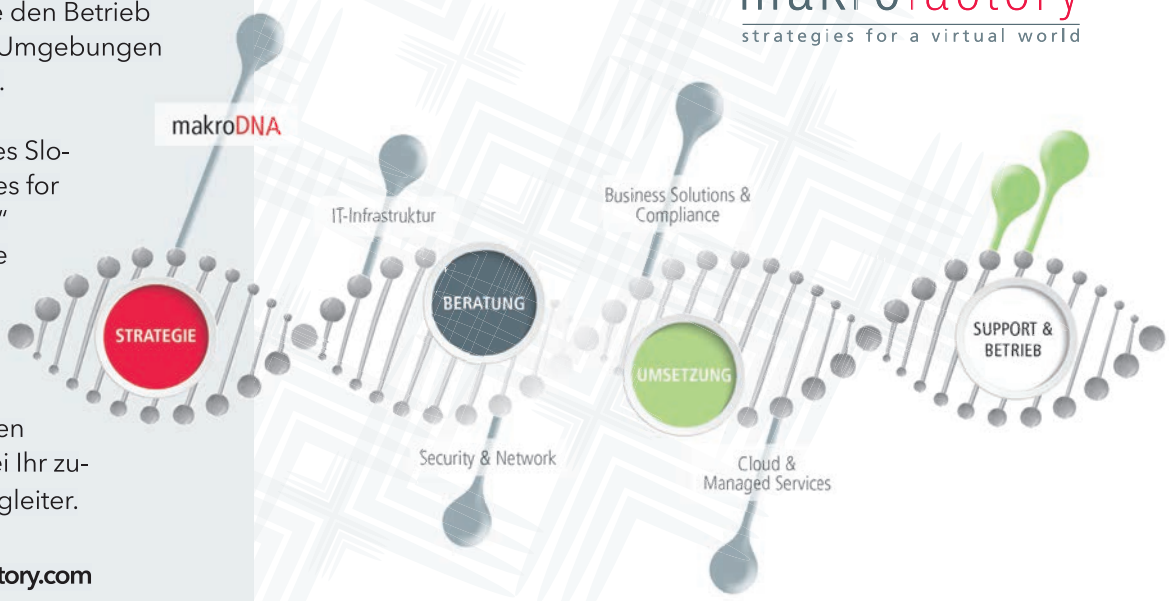
Als eines von Deutschlands führenden IT-Beratungsunternehmen verfügen wir über erprobte Erfolgsrezepte und die entsprechende Umsetzungskompetenz rund um Ihre IT-Projekte. Wir beraten, planen, realisieren und steuern gemeinsam mit Ihnen Ihre Vorhaben. Dabei setzen wir die IT-Analyse, IT-Strategie und IT-Compliance als Fundament aller Entscheidungen ein. Darüber hinaus stehen wir Ihnen für Cloud-, Support- und Wartungs-Services sowie den Betrieb kompletter IT-Umgebungen zur Verfügung.

Gemäß unseres Slogans „strategies for a virtual world" beraten wir Sie bei Ihrer Entscheidung die digitale Transformation umzusetzen und sind dabei Ihr zuverlässiger Begleiter.

www.makrofactory.com

makrofactory

strategies for a virtual world



EFFIZIENZ-BOOSTER BUSINESS INTELLIGENCE

ISO-Zertifizierungsmanagement mit MakroAudit

Eine ISO-Zertifizierung ist für kleine und mittelständische Unternehmen oftmals mit hohem zeitlichen Aufwand verbunden, da ISO-relevante Dokumente zyklisch betrachtet und überarbeitet werden müssen. Während in großen Firmen die kontinuierliche Überwachung von extra dafür zuständigen Teams übernommen wird, fällt diese Aufgabe in kleineren Betrieben meist Mitarbeitern unterschiedlicher Abteilungen erst kurz vor einem Audit zusätzlich zum Tagesgeschäft in den Schoß.

Die Vorbereitung einer Rezertifizierung ist in diesem Fall enorm zeitaufwändig, da den Beteiligten der Überblick fehlt, an welcher Stelle sie im ISO-Prozess gerade stehen, welcher Arbeitsschritt als nächstes sinnvoll abgearbeitet werden muss und wer überhaupt für was zuständig ist.

Wie MakroAudit den ISO-Prozess unterstützt
Der Einsatz einer Business Intelligence-Lösung wie MakroAudit kann den ISO-Prozess deutlich vereinfachen und beschleunigen, da das Tool jederzeit Informationen darüber liefert, welche Aufgaben gerade anstehen und rechtzeitig warnt, wenn gesetzte Deadlines ablaufen. Die Verantwortlichen werden kontinuierlich bei der Überwachung der Einhaltung von Standards und Normen unterstützt.

Dank MakroAudit wird der ISO-Prozess für alle Beteiligten übersichtlich, verständlich und nachvollziehbar. Bei einer Rezertifizierung kann der Auditor zudem ohne Mühe prüfen, ob die Vorgaben korrekt abgearbeitet und alle Richtlinien eingehalten wurden.

MakroAudit basiert auf dem DeltaMaster des Herstellers Bissantz & Company GmbH. Das Unternehmen arbeitet seit Jahren erfolgreich auf Basis neuester wissenschaftlicher Erkenntnisse an der optimalen Datenvisualisierung. Typische Hürden wie eine schlechte Lesbarkeit aufgrund von Farbfehlsichtigkeit oder optischer Reizüberflutung wurden stark minimiert. Die Interpretation der Zahlen ist einfach und intuitiv.

Berechtigungsmanagement mit MakroAccess

Den Überblick über die vergebenen Zugriffsberechtigungen von Mitarbeitern auf Applikationen zu behalten und zu kontrollieren, kann selbst in kleinen Unternehmen sehr schnell mühselig werden. Dabei ist es sowohl aufgrund der aktuellen DSGVO-Richtlinien, als auch aus Gründen der IT-Sicherheit heutzutage unerlässlich, genau zu wissen, wer auf was Zugriff hat, da natürlich mit jeder unnötig vergebenen Berechtigung auch das Risiko des Datenmissbrauchs steigt.

Was leistet MakroAccess?
MakroAccess liest in Sekundenschnelle alle vergebenen Rechte der in Ihrem Unternehmen eingesetzten Applikationen aus und stellt sie in einer einfach zu lesenden Übersicht dar. Dies ermöglicht es Ihnen, in kürzester Zeit valide Aussagen über alle vergebenen Rechte Ihrer Applikationen zu machen: sei es beispielsweise gegenüber Ihrem Geschäftsführer, dem Betriebsrat oder einem Auditor im Rahmen einer Rezertifizierung.

Welch wertvollen Beitrag der Einsatz einer BI-Lösung im Berechtigungsmanagement leisten kann, zeigt ein Beispiel aus der Praxis. Eine Recherche der Makro Factory im eigenen Unternehmen ergab, dass bei ca. 60 Mitarbeitern und 11 Applikationen rund 2,3 Mio. Rechte vergeben wurden. Mit MakroAccess konnte die Anzahl der zu kontrollierenden Rechte auf 280 Tsd. reduziert werden! Der Clou: Für eine übersichtliche Darstellung all dieser Rechte benötigt MakroAccess weniger als 5 Minuten! Wie lange brauchen Sie derzeit in Ihrem Unternehmen?

Neben MakroAudit und Makro Access bietet die Makro Factory noch weitere BI-Lösungen an, z. B. für das IT-Reporting oder Marketing- & Vertriebscontrolling. Sprechen Sie uns bei Bedarf gerne an.

Tel: +49 721 97 003 861
E-Mail: sales@makrofactory.com

SECUREPOINT

- Als deutscher Anbieter von IT-Sicherheitslösungen setzt Securepoint auf das mehrschichtige Konzept der Unified Security, also der umfassenden und ganzheitlichen IT-Sicherheit.
- Securepoint sichert weltweit bereits mehr als 80.000 Netzwerke ab.
- Der Hersteller steht für das Vertrauenszeichen „IT Security made in Germany“. Selbstentwickelte Lösungen sind garantiert frei von Backdoors.

Mehr Informationen unter:
www.securepoint.de

Machbare IT-Sicherheit für Unternehmen

Die schiere Anzahl von Schadsoftware und Malware sorgt für eine ständige Gefahr der Unternehmensnetzwerke und der damit verbundenen webfähigen Geräte. Dahinter steckt ein enormes Schadensrisiko, z. B. bei einem totalen Ausfall eines Rechnernetzes oder der Verschlüsselung von Daten. Die Bedrohungslage ist hoch. Welche Maßnahmen und Schritte aber bieten kleinen und mittleren Unternehmen (KMU) Schutz? Mit welchen Lösungen lässt sich gute IT-Sicherheit schnell und machbar erreichen?

Angreifer versuchen regelmäßig Verschlüsselungsprogramme oder andere Schadsoftware zu installieren. Das funktioniert z. B. über kompromittierte Remote-Zugänge auf Systemen oder ganzen Netzwerken. Gezielte Angriffe auf Unternehmen passieren täglich. Bei Erfolg erhalten die Opfer eine Lösegeldforderung, um die verschlüsselten Daten freischalten zu lassen. Hinter einer digitalen Attacke auf einzelne Unternehmen steht meist noch mehr. Die Angreifer haben die Infrastruktur des Unternehmensnetzes längst kompromittiert. Dieses Vorgehen ermöglicht ihnen das Kopieren wichtiger Daten und den Weiterverkauf. Oft werden Daten in so einem Fall gelöscht oder manipuliert, um die Unternehmen zu schädigen. Die Kombination aus Spionage, Sabotage und Erpressung ist eine große Herausforderung, gegen die es sich zu schützen gilt.

Die Umsetzung entsprechender Schutzmaßnahmen bedeutet aus wirtschaftlicher Perspektive ein präventives Krisenmanagement. Beim Blick auf die Investition sollten die möglichen hohen Folgekosten berücksichtigt werden, die im Falle einer erfolgreichen Cyberattacke für ein Unternehmen entstehen. Denn klar ist: Von einer funktionierenden IT hängt langfristig der Erfolg und das Vertrauen Ihrer Kunden ab. Viele kleine und mittlere Unternehmen fragen sich, wie sie IT-Sicherheit einfach und effizient umsetzen können. Während große Unternehmen dafür eine eigene Abteilung und Fachleute im Haus haben, suchen KMU nach bezahlbaren Lösungen und anwendbaren Maßnahmen.

Unified Security Cert+ zeigt Ihnen den Weg

Orientierung und konkrete notwendige Schritte finden sich beim IT-Sicherheitsstandard „Unified Security Cert+“ wieder. Das Konzept wurde vom deutschen IT-Sicherheitshersteller Securepoint entwickelt. Ziel des unabhängigen Standards ist es, dass IT-Security für KMU in der Praxis machbar ist, um schnell ein besseres IT-Sicherheitsniveau zu erreichen. Für Ihr Unternehmen bedeutet Cert+ eine übersichtliche Planung von Investitionen in IT-Sicherheit. Das schützt die Daten Ihrer Kunden. Die wichtigen Schritte zu mehr Sicherheit gehen Sie als Unternehmen gemeinsam mit Ihrem für Cert+ zertifizierten IT-Dienstleister – der Connecting Media. So kann auf neue Herausforderungen gemeinsam schnell reagiert werden.

Und auch wenn Sie bereits IT-Sicherheitsmaßnahmen im Einsatz haben, ein Problem mit Ihrer IT aufgetreten ist oder sie unsicher sind, ob die eingesetzte Lösung die richtige für Ihr Unternehmen ist, können Sie auf den Service der Connecting Media zurückgreifen. Der ausgebildete und zertifizierte „Sachverständiger nach Cert+“ auditiert, bewertet und analysiert die Schwachstellen

Your Data.

Our Mission.

VARONIS, *DER* PIONIER BEI DATENSICHERHEIT UND ANALYTIK.

- Wir konzentrieren uns auf den Schutz von Unternehmensdaten: sensible Dateien und E-Mails; vertrauliche Kunden-, Patienten- und Mitarbeiterdaten; Finanz- oder Produktunterlagen sowie geistiges Eigentum.
- Die Varonis Data Security Plattform erkennt Insider-Threats und Cyberangriffe durch die Analyse von Daten, Konto- oder Benutzeraktivität: Die Plattform verhindert und begrenzt so einen möglichen Ernstfall - sensible und veraltete Daten werden für den Zugriff gesperrt und Datenschutz wird automatisiert.
- Mit dem klarem Fokus auf Datensicherheit bildet Varonis eine Vielzahl von Anforderungsfällen, einschließlich Governance, Compliance, Klassifizierung und Bedrohungsanalysen ab. Varonis unterstützt seit 2005 weltweit mehr als 6000 Kunden in den Bereichen High-Tech, Retail, Finance, Fertigung oder Energie.

VARONIS

Gefahren & Hintertüren in der digitalen Welt

Und warum lernende, datenzentrierte Systeme der Schlüssel zu Sicherheit und Compliance sind

Immer mehr Unternehmen sind von Sicherheitsverletzungen betroffen und die Flut gefährdeter Daten steigt weiter an. Es ist leider auch zu erkennen, dass Unternehmen immer noch nicht ausreichend auf diese Gefahren vorbereitet sind, obwohl diese immer häufiger auftreten.

Was ist eine Datenschutzverletzung?

Eine Datenschutzverletzung bzw. ein Datenleck ist jeder Vorfall, bei dem unbefugt auf vertrauliche oder sensible Informationen zugegriffen wurde. Datenschutzverletzungen können das Ergebnis eines Cyberangriffs sein, bei dem sich Kriminelle unbefugten Zugang zu einem Computersystem oder Netzwerk verschaffen und die darin enthaltenen privaten und vertraulichen, personenbezogenen Daten stehlen. Häufige Cyberangriffe, die zu Datenschutzverletzungen führen sind: Ransomware, Malware, Phishing oder Denial-Of-Service.

Wie kommt es zu Datenschutzverletzungen?

Während die meisten Datenschutzverletzungen auf Hacker- oder Malware-Angriffe zurückgeführt werden gibt es auch andere Methoden. Dazu gehören etwa Insider-Leaks, Verlust oder Diebstahl von physischen Festplatten mit Dateien sowie menschliches Versagen.

Was bedeutet der Verlust unternehmenskritischer Informationen?

Jedes Unternehmen besitzt unternehmenskritische Daten. Die Spanne dieser Informationen reichen von Kunden- und Projektdaten über Rezepte, Patente bis hin zu Entwicklungsdaten. Gemeinsam haben all diese Informationen das die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen unternehmenskritisch sind! Hierdurch gelangen Sie in den Fokus Cyberkrimineller die dem Unternehmen schaden wollen. Durch Verlust der Verfügbarkeit z.B. kann dem Unternehmen ein großer finanzieller Schaden entstehen, Vertraulichkeit bedeutet ein Reputationsverlust.

Identifizierung und Klassifizierung als Voraussetzung für Datenschutz Informationssicherheit und Compliance

Ziel ist die Entdeckung und Klassifizierung regulierter Daten: und das Wissen (und Beweisen!), dass nur die richtigen Personen Zugriff auf die Daten haben. So lassen sich z.B. Datenschutz- und Aufbewahrungsrichtlinien durchsetzen und Benachrichtigungen bei verdächtigen Aktivitäten und Richtlinienverstößen erhalten. Varonis gibt die nötige unternehmensweite Transparenz, die für effektives Erkennen und Prüfen sowie für Compliance-Audits für eine Vielzahl aufsichtsrechtlicher Standards nötig ist. So lassen sich auch Cyberangriffe schneller erkennen und man kann schneller darauf reagieren: Es werden Bedrohungen identifiziert, die herkömmliche Cyber-Security Lösungen meistens übersehen. Durch eine Kombination aus Transparenz und Kontext, sowie durch sofort einsatzbereite Bedrohungsmodelle (MITRE) ermöglicht Varonis statistisch um 90 % reduzierte Reaktionszeiten – sowohl in der Cloud, als auch in der lokalen Infrastruktur.

Varonis sammelt Metadaten aus verschiedensten Quellen im Unternehmen und Netzwerk und korreliert diese, um eine Rundum-Sicht mit Künstlicher Intelligenz zu gewähren. Durch die gesammelten Metadaten lernt es, die Unterschiede eines normalen Nutzers (und des damit verbundenen Zugriffsverhalten auf Daten) und eines kompromittierten Accounts kennen und kann so sehr schnell bei einem ungewöhnlichen Verhalten Alarme generieren und automatisch bzw. autonom Aktionen bei IT-Security-Systemen triggern.

INLYSE
_01. IDENTIFY
EVERY SECOND THE GLOBAL IT-INFRASTRUCTURE IS HARMED BY CYBER-ATTACKS.
_02. FOCUS
INLYSE. IT-SECURITY POWERED BY ARTIFICIAL INTELLIGENCE. STOPS MORE THAN 99% OF ALL CYBER-ATTACKS WITHIN SECONDS.
_03. INVEST
TRY OUT THE FUTURE FOR FREE AND CONTACT US. NOTICE THE DIFFERENCE.
INLYSE
PROTECT YOURSELF NOW
INLYSE.COM

Virenerkennung mit Künstlicher Intelligenz

Mit der zunehmenden Relevanz von Cloud Anwendungen werden die IT-Umgebungen von Unternehmen komplexer als je zuvor. Deshalb setzen Unternehmen komplizierte regel- und signaturbasierte Sicherheitstechnologien ein, um ihre Unternehmensdaten und Netzwerkteilnehmer gegen Angriffe zu schützen. Diese Methoden schützen Unternehmen jedoch nur gegen bereits bekannte Angriffsmethoden und Schadsoftware. Heutzutage mutiert Schadsoftware täglich, sogar stündlich, um diese Systeme zu umgehen. Zugleich steigt die Anzahl an Targeted Zero-Day Angriffen weiter rasant an. Diese Angriffsmethoden machen die eingesetzten Technologien obsolet und erfordern neue Methoden um diese zu erkennen.

inlyse ist ein in 2018 gegründetes Karlsruher Unternehmen, das genau daran arbeitet unbekannte Computerviren mittels Künstlicher Intelligenz zu erkennen.

Ein Teilbereich der Künstlichen Intelligenz ist „Computer Vision". Dabei handelt es sich um ein Technologiefeld, das mit Hilfe von tiefen neuronalen Netzen Bilder, Fotos und Videos für Computer interpretierbar machen soll. Dieses Technologiefeld hat in den vergangenen Jahren einen Siegeszug in den verschiedensten Domänen hingelegt. Diese umfassen unter anderem die Gesichtserkennung, autonomes Fahren oder das Erkennen von Krankheiten auf Röntgenbildern. Weltweit arbeiten Forscher an Computer Vision Architekturen um die Erkennungsraten stets weiter zu verbessern. Diese Architekturen stellen sich ein um das andere Mal in den Schatten und dienen nur dem Zweck bereits minimalste Strukturen auf Bildern zu erkennen, die selbst dem menschlichen Auge verborgen bleiben.

inlyse macht sich genau diesen Ansatz zu Nutze und hat eine Methode entwickelt, Dateien so in Bilder umzuwandeln, dass diese von tiefen neuronalen Netzen interpretiert und selbst kleinste Hinweise auf Computerviren erkannt werden können. Damit ist inlyse in der Lage, selbst unbekannte Computerviren innerhalb weniger Sekunden zu 99% zu erkennen, ohne dass diese Dateien ausgeführt und deren Verhalten analysiert werden muss. Selbst regelmäßige Updates werden dadurch nicht mehr benötigt, da die Künstliche Intelligenz nicht versucht einzelne bestimmte Viren zu erkennen, sondern das Gelernte auf unbekanntes zu interpolieren. Diese Erkennungsraten können daher updatefrei über mehrere Monate hinweg gehalten werden.

inlyse stellt diese innovative Technologie jedem Interessenten über komplementäre Plugins bereit, die sich genau dort integrieren sollen, wo Sicherheitsmängel festgestellt werden. Diese umfassen momentan Browser Erweiterungen für alle gängigen Browser-Systeme, Outlook und Office365 Plugins oder Integrationen für Slack, die unkompliziert aus den entsprechenden Plugin-Stores installiert werden können.

Dieser Ansatz ermöglicht es somit auch kleinen und mittelständischen Unternehmen, sich gezielt dort gegen unbekannte Viren und Angriffe schützen zu können, wo IT-Sicherheitsdefizite bestehen, ohne dass dafür bereits vorhandene Systeme ersetzt werden müssen und ohne dass erweiterte IT-Kenntnisse gefordert werden.

seclous mail

Natürlich auf Basis unserer patentierten
Non-Visible-Data Technologie.

seclous

Per E-Mail über das Internet zu kommunizieren, das muss doch einfach, hochsicher und bei voller Kontrolle gehen. Ganz egal wo, wie, mit wem und unabhängig von der Konfiguration. IT-Sicherheit ist aber heute meist umständlich und teuer. Hat Deutschland hier bereits den Anschluss verloren? Oft werden neue Regeln (Stichwort Datenschutzverordnung) geschaffen, aber der fehlende Schutz vor Datenmissbrauch wird dabei nicht gelöst. Wir von SECLOUS sorgen dafür, dass sich das ändert, indem wir für eine digitale Souveränität bei den Daten sorgen, ohne dass der Nutzer viel dazu tun muss. SECLOUS arbeitet mit neuartigen Lösungen daran, dass Ihre Daten immer sicher sind.

Einfach
durch unsere 1-Click Aktivierung!

Sicher
auf militärischem Niveau!

Unsichtbar
und dadurch nicht angreifbar!

seclous

Wir machen Ihre Daten unsichtbar!

**Hybride Arbeitsformen –
neue Chancen, neue Risiken**

Sind Sie noch Herr über Ihre Daten? Die Corona-Pandemie zwingt Millionen von Beschäftigten zur Arbeit von zu Hause. Ein Wachstumsmarkt wie das Home Office bringt Vorteile, aber auch neue Risiken. Always on, Use Your Own Device oder ein selbst eingerichtetes Heimnetzwerk sind Gefahren im Netz ausgesetzt. Andererseits werden Unternehmen in diesen Zeiten „virtuell" geführt. Gesetzliche Anforderungen, wie Datenschutz, wollen da weiter erfüllt werden. Und wie setzt man das in der Praxis um? Wie schützt man bei den ganzen Begebenheiten grundsätzlich die Unternehmenswerte? Das sind alles neue Herausforderungen, mit denen sich IT-Abteilungen auseinandersetzen müssen. Und nicht selten wird hier mal ein Auge zugedrückt, um den Geschäftsbetrieb, in einer mental wie auch wirtschaftlich angespannten Zeit, nicht noch weiter zu behindern. Im Kontext von stark zunehmender Cyberkriminalität kann das aber schnell zum großen Problem werden.

War der typische „Hacker" früher ein Computer-Enthusiast, rückt an diese Stelle zunehmend die organisierte Kriminalität. Gesellschaftlicher sowie digitaler Wandel und vor allem dessen Fallstricke, werden unter Gaunern als lukratives Geschäftsfeld begriffen. So sind E-Mails in Firmen zwischen Kollegen und Geschäftspartnern das häufigste Kommunikationsmedium. Fälschlicherweise werden E-Mails generell als sicher eingestuft und nicht selten mit hochsensiblen Inhalten belegt. Ein Umstand, der in Kombination mit vergleichsweise schlecht gesicherten oder falsch konfigurierten Heimnetzwerken und Endgeräten, auch Cyberkriminellen nicht entgangen ist. Ein beliebtes Medium, das für den Großteil der Cyberattacken verwendet wird, sind Verschlüsselungstrojaner, um sich mit deren Hilfe illegal zu bereichern.

Was ist dagegen zu tun, wenn man davon ausgeht, dass wir künftig verstärkt in der hybriden Form aus Präsenz und Digital zusammenarbeiten? Mehr digitale Mauern errichten, die von personell schwach besetzten IT-Abteilungen konfiguriert, überwacht und verwaltet werden? Und vor allem, wo soll da eine Grenze gezogen werden?

Entspannt daheim, unterwegs und in der IT zurücklehnen – ab sofort schützen Ihre E-Mails und Daten sich einfach selbst

Mit SECLOUS Mail* stellen wir Ihnen ein E-Mail-Produkt zur Verfügung, dass nicht nur kinderleicht zu bedienen ist, sondern vorkonfiguriert schon heute, zukünftige Sicherheitsanforderungen erfüllt. Weltweit einzigartig integrieren wir den Schutz direkt ab Entstehung Ihrer E-Mails und übertragen Ihre Nachrichten über das Internet unsichtbar, sodass keine Rückschlüsse auf die darin enthaltenden Informationen möglich sind. Und das Beste – wir schützen nicht nur Sie als Versender, sondern automatisch auch alle Empfänger Ihrer E-Mails und das wie gewohnt aus Outlook oder per Webmailer. Unabhängig davon wo, wie und in welcher Konfiguration Sie oder Ihre Geschäftspartner oder Freunde kommunizieren. Das schützt nicht nur effektiv gegen Cyberkriminelle, sondern entlastet auch die Kollegen aus der IT. Ein aufwendiges und komplexes Management entfällt vollständig. Mit SECLOUS Mail* macht es nun keinen Unterschied mehr, ob Sie im geschützten Umfeld der Unternehmens IT kommunizieren, im Home Office, Mobil, über private Endgeräte oder Ihr Heimnetzwerk unsicher konfiguriert ist.

Liest und fühlt sich spannend an?
Dann lassen Sie uns auch Ihre Mails unsichtbar machen! Testen Sie uns 14 Tage kostenlos auf www.seclous-mail.com.

* SECLOUS Mail – ein Produkt basierend auf der patentierten Non-Visible-Data (NVD) Technologie. Ausgezeichnet vom Bundesministerium der Verteidigung mit dem ersten Preis (https://bit.ly/3s0nSVT).

RamgeSoft
Europaweite Software Distribution

Die RamgeSoft ist der auf Monitoring- und Securitylösungen spezialisierte Value Added Distributor in EMEA.

Das Portfolio umfasst On-Premise- und Cloud-basierende Technologien sowie Produkte für Managed Service Provider.

Als VAD bietet RamgeSoft Beratung, Schulung und alle Dienstleistungen, die Systemhäuser benötigen, um die Lösungen bei ihren Kunden zu implementieren und zu betreiben. Mit Hauptsitz in Regensburg betreut RamgeSoft seit über 15 Jahren mehr als 1.500 Partner mit über 140.000 Endkunden.

Im Gewerbepark A10
93059 Regensburg

+49 941 58484001

sales@ramgesoft.de

www.ramgesoft.de

EIN REGELMÄSSIGER SCHWACHSTELLEN-SCAN SOLLTE KEIN LUXUS SEIN

A1 Offensity ist ein Produkt der A1 Digital und erblickte 2017 erstmals „das Licht der Erde". Was erst noch ein Produkt für eigene Bedürfnisse war ist heute eine Sicherheitslösung für die breite Masse. Offensity ist ein Schwachstellenscanner, der gerade für den KMU-Bereich, eine bezahlbare Lösung ist und mit Hilfe von Hackertools Schwachstellen bewertet und reportet.

Unternehmensweite Sicherheit – gehen Sie in die Offensive :

- Konkrete Handlungsempfehlungen: von den besten Hackern Europas
- Übersichtliches Reporting: schneller Probleme beheben
- Kontinuierliche Scans: Ihre gesamte IT-Systemlandschaft im Blick
- Datenleaks: gezielte Prüfung auf unfreiwillig veröffentlichte Datensätze im Deep Web

www.offensity.com

NEUE MASSSTÄBE IM BEREICH ZERODAY PRÄVENTION SETZEN

Mit knapp 22 Mitarbeitern ist die eigentümergeführte **Blue Shield Security GmbH**, unter Alois Kobler, federführend im Bereich der DNS-Sicherheit.

Wie funktioniert BlueShield Umbrella? Kurz gesagt: Jegliche Anfrage ins Internet benötigt einen DNS-Server. Diese Anfragen werden in Zukunft von BlueShield übernommen. BlueShield prüft und verifiziert Ihren DNS-Traffic und kann somit Anomalien sofort und in Echtzeit erkennen und Sie davor schützen. Auf einer sogenannten „WhiteList/AllowList" Root-Nameserver-Basis wird vorsortiert, bevor eine Domain in das eigene DNS-System aufgenommen wird. Zu dieser Bewertung kommen speziell entwickelte Algorithmen, eigene Crawler und Künstliche Intelligenz, welche seit 2013 analysiert und stetig mit weltweit öffentlichen Hybrid-Sandboxen erweitert wird.

www.blue-shield.at

ZERO TRUST ALS STRATEGIE FÜR DAS UNTERNEHMEN

Das Ziel von **Safe-T** ist es Ihr Unternehmen vor Angriffen und Datenlecks zu schützen. Die Sicherung der eigenen sensiblen Daten ist schwieriger als je zuvor. Modernste Hacking- und Scanningwerkzeuge machen es leicht in Unternehmen einzubrechen, egal aus welcher Branche Sie kommen.

Und genau hier setzt Safe-t an. Die ZoneZero SDP von Safe-T verändert die Art und Weise, wie Organisationen sicheren externen Zugriff auf ihre Dienste gewähren. Dieses Produkt ist Teil der ZoneZero-Plattform für die Orchestrierung des Perimeterzugriffs, die eine zentrale Verwaltung aller sicheren Zugriffstechnologien bietet und Organisationen dabei unterstützt, Zero Trust Network Access (ZTNA) zu erreichen.

www.safe-t.com

LÖSEN SIE HEUTE IHRE SCHWIERIGSTEN IT-VERWALTUNGSPROBLEME

Getreu dem Motto, von Administratoren für Administratoren, entwickelt und kauft **SolarWinds** Software, die den Alltag des Admins enorm vereinfacht. Solarwindsprodukte zeichnen sich im Wesentlichen durch folgende Punkte aus:

- Herstellerunabhängigkeit
- Einfaches Ampelsystem
- Proaktives Management im Vordergrund
- Solarwindsprodukte haben nicht nur eine Monitoringoberfläche, sondern liefern auch das Werkzeug zum Management der Objekte
- Große Usercommmunity (Thwack)

Unter Berücksichtigung des Kunden-Feedbacks erstellt Solarwinds leistungsfähige und benutzerfreundliche Lösungen, die Ihnen helfen, Kosten und Aufwand zu reduzieren und sich den sich ständig verändernden IT-Bedürfnissen anzupassen.

www.solarwinds.com

Soliton®

- Soliton Systems ist ein seit 1979 führendes IT-Sicherheitsunternehmen aus Japan
- Innovative Technologien im Bereich Remote Access Control und Network Access Control
- Zertifikatsbasierte All-in-One NAC Lösungen, einfach zu skalieren und zu implementieren. Entwickelt auf Basis von 802.1X und Zero Trust.
- Mit Remote Access Control Produkten strikte Trennung von privaten sowie betrieblichen Daten. Ohne VPN oder hohen Installationskosten. Perfekt für unmanaged, COPE oder BYOD.

IT-Sicherheit auch auf nicht verwalteten Geräten

Erinnern Sie sich noch an die Zeit, als die IT eine einsame, abgeschiedene Abteilung war? Oft war sie in der dritten oder vierten Etage versteckt und agierte als selbsternannter Stadtstaat, weit weg von den Besprechungsräumen, in denen die „echte" Magie stattfand. Die IT-Manager wurden zu jener Zeit nicht regelmäßig zu Meetings leitender Angestellter eingeladen, ganz einfach, weil es keinen Grund dafür gab. Die Firma war ein Schiff und niemand konnte ohne Ihre Erlaubnis an Bord gehen. Aber das war einmal.

WLAN, BYOD und Freelancer

Heutzutage drehen sich die meisten organisatorischen Probleme um die IT. Die Geräte werden über Kabel, WLAN und VPN mit Ihrem Netzwerk verbunden und lassen sich so nur schwer kontrollieren. Immer mehr Unternehmen führen „Bring Your Own Device (BYOD)"-Konzepte ein, das heißt Sie müssen nicht nur die Firmencomputer überwachen, sondern auch unzählige Laptops, Telefone und Tablets. Und dann sind da noch die Gäste und Auftragnehmer, die Zugang zum Netzwerk anfordern: Menschen, von denen Sie noch nie zuvor gehört haben, aber die dennoch im Internet surfen wollen, wenn sie Ihr Unternehmen besuchen. Das bedeutet, dass viele Menschen kommen – aber auch viele Menschen wieder gehen.

NAC & das Konzept

Bereits 2001 konnte sich das Konzept der Netzwerkzugangskontrolle mit einem vielversprechenden Wertversprechen Zugang zum Markt verschaffen: „Die NAC kontrolliert den Zugang zu Unternehmensressourcen mittels Autorisierung und die Umsetzung von Richtlinien." Doch auch hier gibt es einige Punkte zu beachten.

NETTATEST EPS

Setzen Sie auf eine Komplettlösung – Eine Komplettlösung bietet buchstäblich alles, was Sie zum Schutz Ihres Unternehmensnetzwerks benötigen. Dazu gehören neben dem RADIUS-Server auch die Zertifizierungsstelle, welche die Sicherheitszertifikate erstellt oder der OTP-Server, welche die Zwei-Faktor-Authentifizierung ermöglicht.

Setzen Sie auf eine NAC-Lösung, die eine sichere Verteilung von Zertifikaten ermöglicht – Wenn Sie den Teil überspringen möchten, in dem jeder Mitarbeiter in Ihr Büro kommen muss, um sein Geräte einzeln authentifizieren zu lassen und Zertifikate zu verlängern, empfehlen wir Ihnen, nach einer benutzerzentrischen Vergabe der Zertifikate mittels Multi-Faktor-Authentifizierung zu fragen. Benutzerzentrisch bedeutet, dass Ihre Mitarbeiter die Zertifikate von ihrer eigenen Etage oder sogar von zu Hause aus herunterladen können. All das ist mit der Netattest EPS möglich.

Tasten Sie Ihre Dateninfrastruktur nicht an – Viele IT-Manager haben uns gefragt, ob sie ihre Dateninfrastruktur ändern sollten, bevor die NAC implementiert wird. Die Antwort darauf ist nein. Die Nettatest EPS verknüpft sich ganz einfach mit der bereits vorhandenen Software und Hardware.

All in one solution Nettatest

- Verwendet IEEE 802.1X, um als Authentifizierungs- und Autorisierungsserver zu fungieren.
- Eigenständige Komplettlösung (enthält alles, was benötigt wird, einschließlich der Zertifizierungsstelle und des RADIUS-Servers).
- Verfahren zur sicheren Verteilung von Benutzer- oder Gerätezertifikaten auf allen gängigen Betriebssystemen mittels SolitonKeyManager.

ENGINSIGHT

Mit **ENGINSIGHT** schützen Sie sich vor externen und internen Sicherheitsrisiken, die Ihre Unternehmenswerte bedrohen – bestätigen auch erfahrene IT-Sicherheitsberater.

Das einfachste Security Tool für den Mittelstand

Mit Enginsight haben wir endlich eine Security-Software gefunden, die uns Analyseergebnisse ohne Quantenphysik liefert. Während ich bei Konkurrenzprodukten oder Open Source Tools im Nachgang viel Zeit darin investieren muss, einen Report auszuwerten und umgangssprachlich zu formulieren, reduziert sich bei Enginsight der Aufwand auf ein Minimum.

ANDREAS KUNZ
CEO, CONNECTING MEDIA

DAS BIETET IHNEN ENGINSIGHT

- **Schwachstellen-Scanner**
- **Monitoring**
- **Pentesting, Inventarisierung**
- **Websecurity** für alle Unternehmensgrößen
- **100% made in Germany**
- **Support auf Augenhöhe**
- **professionelle Einweisung**
- **Einfache Bedienung** auch für Nicht-Experten

Zertifiziert durch TÜV THÜRINGEN

Zertifiziert durch TÜV THÜRINGEN

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

KOSTENLOS TESTEN
UNTER ENGINSIGHT.COM

ENGINSIGHT

Warum wird immer mehr über IT-Hygiene gesprochen?

Beim Begriff der Hygiene denkt man zunächst vielleicht eher an die Medizin oder die tägliche Körperpflege als an Informationstechnik. Es ist jedoch lehrreich, den Begriff und seine Implikationen in die IT-Welt zu entlehnen. Denn viele Aspekte der Hygiene lassen sich auf die Benutzung, Administration und Absicherung von IT-Systemen übertragen. Eine gute IT-Hygiene und Cyber-Hygiene umfasst eine Reihe von Verfahren und Maßnahmen in der Informationssicherheit, um Daten sicher und gut geschützt zu halten.

Wie funktioniert Cyber-Hygiene?

Ebenso wie die menschliche Gesundheit brauchen IT-Systeme täglich einen sorgsamen Umgang, um auf Dauer sicher und zuverlässig zu funktionieren. Anstatt auf Cyberattacken zu reagieren, sind proaktive Maßnahmen für die erfolgreiche Absicherung von IT-Infrastrukturen von großer Wichtigkeit. Das heißt vor allem, Sicherheitsrisiken aufzuspüren und Sicherheitslücken zu schließen, bevor sie von Hackern ausgenutzt werden. Dabei helfen ein dauerhaftes Security-Monitoring sowie automatisierte Penetrationstests.

Als ganzheitliche Herausforderung ist IT-Sicherheit keine Spezialaufgabe der IT-Abteilung, sondern auch im Aufgabenbereich der Geschäftsführung anzusiedeln. Ein Information Security Management System (ISMS) hilft ihr, die Ganzheitlichkeit des Sicherheitskonzeptes im Auge zu behalten. Neben der Geschäftsführung besitzt jeder Mitarbeiter eine persönliche Verantwortung, mit seinen Handlungen die Sicherheit nicht zu gefährden. Die klaren Vorgaben, was geboten und was verboten ist, müssen allen Mitarbeitern in Awareness-Schulungen nähergebracht werden, sodass die Richtlinien in die Routinen des Einzelnen übergehen.

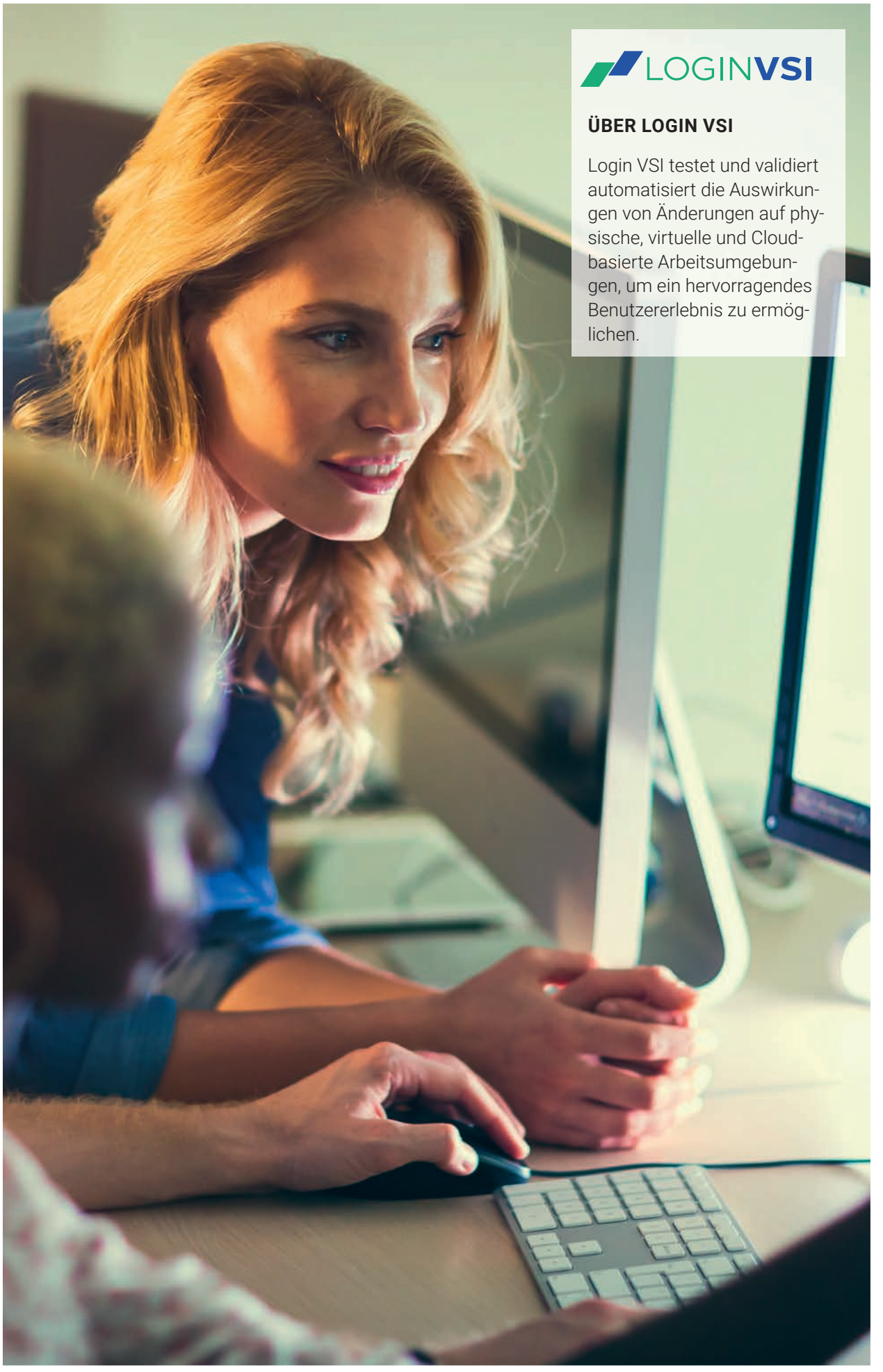
Routinen spielen auch in der Administration der IT-Systeme eine große Rolle. Die tägliche Überprüfung des Sicherheitszustandes, das Patchen gefährdeter Software, das Erkennen von Anomalien im IT-Betrieb – all das sind Aufgaben, die als Routineaufgaben viel Zeit fressen, aber zwingend notwendig sind. Technische Lösungen, die durch Automatisierung den Administrator entlasten, sind daher von großer Bedeutung, Routinen effektiv zu meisten. Sie sind außerdem wichtig, um Abweichungen vom Normalbetrieb und sicherheitskritische Cyber-Vorfälle unmittelbar zu erfassen, um das Infektionsgeschehen frühzeitig einzudämmen. Deshalb ist ein Intrusion Detection System (IDS) ein wesentlicher Stützpfeiler der Cyber-Hygiene.

IT-Security auf dem IT-Hygiene-Prüfstand

Das Konzept der Hygiene hilft, die Dynamiken der IT-Sicherheit besser zu verstehen und ergriffene Maßnahmen zu bewerten. Es legt den Fokus auf die kleinen, alltäglichen Maßnahmen, die in Summe zu einem resilienteren System führen. Es betont, dass es mit der einmaligen Installation vermeintlich allwissender Firewall- und Anti-Viren-Systeme nicht getan ist.

Mit Enginsight haben wir ein Werkzeug entwickelt, mit dem IT-Abteilungen trotz zunehmender Vernetzung und Komplexität ihre IT-Hygiene-Aufgaben einfach und entspannt erledigen können. Dazu vereint es das Beste aus den Welten IT-Sicherheit, IT-Monitoring und IT-Management in einer Softwarelösung. Enginsight ist plattformunabhängig und für Linux ebenso wie Windows optimiert sowie ohne Konfigurationen sofort einsatzbereit.

Registrieren Sie sich und testen Sie Enginsight 14 Tage mit einem kostenlosen Testaccount oder vereinbaren Sie einen persönlichen Demo-Termin.



LOGINVSI

ÜBER LOGIN VSI

Login VSI testet und validiert automatisiert die Auswirkungen von Änderungen auf physische, virtuelle und Cloud-basierte Arbeitsumgebungen, um ein hervorragendes Benutzererlebnis zu ermöglichen.

Änderungsmanagement im VDI Umfeld

Für heutige Unternehmen, konfrontiert mit im ständigen Wandel befindlichen IT-Strukturen, ist es elementar notwendig den Überblick zu behalten, agil zu bleiben und sicherzustellen, dass Kosten und Nutzen in einem wirtschaftlich optimalen Verhältnis stehen.

Die digitale Transformation in Richtung Cloudservices stellt für Unternehmen laufend neue Herausforderungen bereit, die mit bestimmten Unsicherheitsfaktoren einher gehen. So spielt in diesem Kontext beispielsweise das Thema Sicherheit eine gewichtige Rolle und dabei auch die Frage nach der Lokation, in der die Unternehmensdaten gespeichert und vorgehalten werden. Darüber hinaus muss auch die Migrationsstrategie geklärt und damit die Frage beantwortet werden, wie viel Infrastruktur benötigt wird und wie die anvisierte Infrastruktur in der Cloud bereitgestellt werden soll. Ein weiterer Aspekt ist zum Beispiel die Frage, wie die Unternehmensdaten den Mitarbeitern zur Verfügung gestellt werden, wie die Mitarbeiter auf die Daten zugreifen, welche Kosten zu erwarten sind und wie sich das Management von Änderungen in einer Umgebung verändert, die sich auf einmal außerhalb der eigenen Rechenzentrumsgrenzen befindet. Oft werden Anforderungen an Kapazität und Leistungsfähigkeit eins zu eins von der bestehenden Infrastruktur abgeleitet, wobei der Soll-Zustand aber jedoch meist eine unvollständig definierte Größe bleibt.

Aussagen hinsichtlich der Größe und der Leitungsfähigkeit der anvisierten Cloud-Infrastruktur lassen sich nur schwierig treffen, da eine verlässliche Messung und Darstellung von aussagekräftigen Kenngrößen nur schwer durchführbar ist, da schlichtweg die hierzu erforderlichen Werkzeuge fehlen. Zudem drängt sich die Frage auf, welcher Cloudanbieter denn aktuell das jeweils beste Kosten-Nutzen-Modell aufweist. Es könnte ja sein, dass Cloudanbieter 1 für die aktuellen Anforderungen hinsichtlich Kapazität und Leistungsfähigkeit in diesem Monat günstiger ist als die Cloudanbieter 2 und 3, den Monat darauf Cloudanbieter 3 der günstigste ist und einen Monat später wieder Cloudanbieter 1.

Alles dies sind Themen die IT-Leiter heute beschäftigen. Bei der Betrachtung dieser Themenfelder ist eine vorausschauende Planung sowie die Risikominimierung bei gleichzeitiger Agilität besonders wichtig. Um am Ende den besten Kosten-Nutzen-Effekt zu erzielen, muss man die individuellen Anforderung Anbieter-neutral vergleichen können, und zwar unter den realen Anforderungen der bestehenden sowie der zukünftigen Arbeitslast.

Genau an diesem Punkt setzt Login Enterprise an und bietet die Möglichkeit, unterschiedliche Konfigurationsmöglichkeiten von unterschiedlichen Anbietern auszuwählen und mit den individuellen Anforderungen an die Größe und Leistungsfähigkeit von Infrastruktur zu vergleichen. Ein ganz wesentlicher Punkt bei der Betrachtung der Leistungsfähigkeit sind die spezifischen Unternehmensanwendungen, die in die Cloud verlagert werden sollen. Somit können verschiedene Optionen eines oder mehrerer Anbieter miteinander verglichen werden, um die optimale Auslastung der Infrastruktur zu verifizieren und gleichzeitig die monatlichen Kosten für die Umgebung einschließlich der Anzahl der Nutzer zu bestimmen. Zudem besteht die Möglichkeit die Login-Zeiten für die unterschiedlichen Konfigurationen zu messen und zu berichten, um sachbezogene Entscheidungen besser treffen zu können.

Zusammengefasst lassen sich durch die beschriebenen Tests mit Login Enterprise die folgenden Faktoren bestimmen:

- Kosten pro Monat und Nutzer
- Optimale Konfiguration der Infrastruktur
- Optimaler Anbieter je Monat

DR. HÖRTKORN
MÜNCHEN

Smart Factory & Industrial IoT

Der Weg zu einem ganzheitlichen IT-Sicherheitsmanagement

Die Digitalisierung und Industrie 4.0 sind die brennenden Themen der Gegenwart und Zukunft. Parallel dazu steigt die Zahl der Cyber-Attacken signifikant an. Das fehlende Risikobewusstsein vieler Unternehmen ist äußerst kritisch zu betrachten. In erster Linie sind es insbesondere Softwareunternehmen und IT-Dienstleister, welchen eine besondere Verantwortung bei der Sicherheit ihrer Produkte zukommt. Diese beschränkt sich allerdings primär auf die Gefahren von Cyberrisiken. Auch wenn dies ein wesentlicher Bestandteil des Gefahrenpotentials darstellt, ist diese Sichtweise zu kurz gedacht. Schließlich können nicht nur Cyberrisiken zu massiven Schäden führen, sondern auch z.B. menschliches Versagen oder fehlerhafte Entwicklung im Bereich der Softwareprogrammierung.

Eine Kombination aus technischen, organisatorischen sowie personellen Maßnahmen ist wesentlicher Bestandteil eines ganzheitlichen IT-Sicherheitsmanagements. Doch erst wenn die vierte Säule, der Risikotransfer in Form der Absicherung von Restrisiken über adäquaten Versicherungsschutz hinzukommt, ist das IT-Sicherheitsmanagement vollständig. Bei Schadensszenarien müssen wir drei Kategorien unterscheiden: Personen-, Sach- und/oder reine Vermögensschäden. Der Fokus für IT-Unternehmen liegt eindeutig in der Absicherung von reinen Vermögensschäden. So ist es heute bei vielen Versicherungen Standard, nicht nur die obligatorische Haftung bei Verschulden, sondern auch die verschuldensunabhängige Haftung, insbesondere bei Abweichen von vereinbarten Beschaffenheiten von Produkten und Leistungen, wie z.B. im Rahmen von Service Level Agreements oder Dauerschuldverhältnissen abzusichern. Selbst bei den durch Versicherer bislang sehr zurückhaltend behandelten Themen wie pauschalierter Schadensersatz oder Vertragsstrafen gibt es inzwischen Bewegung. Unter den Versicherungsschutz fallen dabei nicht nur die zivilrechtlichen Schadensersatzansprüche Dritter infolge mangelhafter Produkte oder Leistungen, sondern auch Haftpflichtansprüche in Zusammenhang mit Cyberschäden. Darüber hinaus kann sich das IT-Unternehmen durch Assistance-Dienstleistungen auch Forensik-Spezialisten sowie die Absicherung von Eigenschäden, z.B. bei Ertragsausfall oder Cybererpressung, in Form einer Cyberpolice einkaufen. Für Softwareentwickler und IT-Dienstleister existieren mittlerweile ausreichende Lösungen, um sich selbst aber auch Dritte vor selbst- oder fremdverschuldeten Schäden zu versichern.

Im Bereich Smart Factory bzw. Industrial IoT sieht das Bild noch deutlich anders aus. Bisher waren die IT und die IoT zwei getrennte Bereiche. Das hat sich mittlerweile grundlegend geändert. In diesem Zusammenhang ist auch ein neues Denken im Bereich des Risikotransfers dringend erforderlich. Gerade die Bereiche Maschinenbau, Robotik und Automation stehen in Verbindung mit Industrie 4.0 vor großen Aufgaben. Um im internationalen Wettbewerb bestehen zu können, muss die klassische Industrie in Sachen Digitalisierung massiv investieren und aufrüsten. Ziel ist es mit digitalisierten Wertschöpfungsketten

zusätzliche Effizienzsteigerung zu erreichen, aber auch durch zusätzliche Services wie Prozessüberwachung, Prozessoptimierung, Fernwartung, regelmäßigen Updates oder Upgrades bisher unerschlossene Umsatzpotenziale neu zu erschließen. Doch der unvermeidlich weiter anwachsende Einfluss der Digitalisierung in diesen Branchen erhöht auch deren Störanfälligkeit. Neue digitale Gefahren und neue Services brauchen auch neue Lösungen zur Schadenverhütung. Schnelle und kompetente Reaktion bei Störungen sind erforderlich, um existentiellen Schaden von Unternehmen fernzuhalten. Viele Versicherer setzen aktuell noch immer auf das gängige Produkthaftpflichtmodell aus dem letzten Jahrtausend, welches sich in erster Linie mit Personen- und Sachschäden aus der analogen Welt beschäftigt. Zwar werden auch heute schon gewisse Vermögensschäden aus IT-Risiken mitversichert, dies deckt den neu entstandenen Bedarf jedoch nicht ansatzweise ab. Insbesondere setzt die Leistung des Versicherers erst dann ein, wenn der Schaden schon eingetreten ist. Unterstützung im Rahmen einer schnellen und wirksamen forensischen Ursachenforschung, um Schäden in einem frühen Stadium einzufangen und klein zu halten, Fehlanzeige. Gleiches gilt auch für die aufgrund der Digitalisierung erforderlichen und neuen Services.

Maschinenbauer verfügen meist über eigene Servicetechniker, diese sind jedoch eher analog ausgerichtet und mit Problemen wie beispielsweise bei der Steuerungssoftware überfordert. Stellen wir uns nur einmal vor was passiert, wenn ein international tätiges Maschinenbauunternehmen über eine eigene zentrale Cloudlösung alle Maschinen, welche bei Kunden weltweit im Einsatz sind, steuert. Aufgrund einer digitalen Störung fallen nun die Maschinen zeitgleich aus. Ein Horrorszenario, bei dem es ganz schnell um die Existenz des Unternehmens gehen kann. Schnelle forensische Untersuchung der Ursache ist hier von elementarer Bedeutung. Doch was, wenn die eigenen Servicetechniker das Problem nicht in den Griff bekommen? Aktuell können Maschinenbauunternehmen hinsichtlich ihrer digitalen Risiken bereits eine Cyberversicherung abschließen, welche neben Eigenschäden auch eine Vermögensschadenhaftpflicht bei Drittschäden bietet. Im Fokus stehen dabei Informations- und Netzwerksicherheitsverletzungen, welche gegenüber Dritten entstehen können.

Wie eine aktuelle Auswertung des Gesamtverbandes der Deutschen Versicherungswirtschaft im Rahmen eines Branchenchecks aufzeigt, ist im Bewusstsein hinsichtlich der Notwendigkeit sich gegenüber Cyberrisiken im Maschinenbau abzusichern noch deutlich Luft nach oben. Demnach ist jeder dritte Maschinenbauer bereits Ziel von Cyberkriminalität geworden, 10% davon sogar schon mehrmals. Ungeachtet dessen halten immer noch 38% der Maschinenbauer in Deutschland das Risiko von einem Cyberangriff getroffen zu werden für eher bzw. sehr gering. Frei nach dem Sankt-Florian-Prinzip sehen sogar 55% die Risiken als eher bzw. sehr gering an, wenn es um die Einschätzung für das eigene Unternehmen geht. Eine klassische Betriebs- und Produkthaftpflichtversicherung gehört dagegen für den deutschen Maschinenbau zur Grundausstattung.

Haftpflichtpolice analog eines IT-Unternehmens mit integrierter Schadenprävention

Die Maschinenbaubranche ist im Prinzip mit zunehmendem Anteil der Digitalisierung versicherungstechnisch wie ein IT-Unternehmen zu sehen. Nur eben zusätzlich mit den klassischen Risiken eines Maschinenbauers. Als spezialisierter Versicherungsmakler für IT-Unternehmen und Cyberrisiken hat die Dr. Hörtkorn München Anfang dieses Jahres ein solches Produkt mit einem auf IT-Risiken spezialisierten Versicherer sowie einem vom BSI als APT-Response Dienstleister qualifizierten Krisenmanagementunternehmen auf den Markt gebracht. Wir verknüpfen die IT-Vermögensschadenhaftpflicht mit einer industriellen klassischen Betriebshaftpflicht und integrieren eine Assistancedienstleistung nach ISO 27001, welche die Anforderungen zur Behandlung sicherheitsrelevanter Probleme nach IEC 62443-4.1 erfüllt. Um im Bedarfsfall den Schaden schnellstmöglich zu identifizieren und die Auswirkungen klein zu halten, hat diese Assistance eine 24/365-Erreichbarkeit und ist in der Lage sich innerhalb kürzester Zeit unterstützend in die Forensik einzuschalten.

Informationen zur Absicherung von Risiken im Umfeld der industriellen Digitalisierung finden Sie unter https://www.hoertkorn-muenchen.de/maschinenbau/

Peter Janson
Prokurist der Dr. Hörtkorn München GmbH
www.hoertkorn-muenchen.de

CMSC

Connecting Media ServiceCockpit

SIEM, Monitoring und ISMS für den Mittelstand aus einer Hand!

Die Digitalisierung und Vernetzung durchdringen die Geschäftswelt immer tiefer. Ein weitreichender Prozess, der Firmen spannende Chancen und Perspektiven bietet, aber auch Herausfoderungen mit sich bringt: 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 werden Systemen anzupassen.

Ohne ganzheitlichen Ansatz geht es nicht

Wie lässt sich aber nun diese Herausforderung meistern und worauf kommt es überhaupt an? Die Lösung liegt in einem integrativen Ansatz mit einem umfassenden Blick auf die IT-Systeme. Es soll dabei nicht ein weiteres Datensilo entstehen, sondern vorhandene Systeme und Informationen lesbar und bedienbar machen. Bei einer Fehleranalyse soll so nicht die bekannte Nadel im Heufhaufen gesucht werden müssen, sondern zielgerichtet gearbeitet werden und alles in einer Oberfläche zentral vereinen.

Connecting Media denkt weiter

Wer bereits ein Informationssicherheitsmanagementsystem (ISMS) in der Firma 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. Eine Schwierigkeit bleibt aber weiterhin bestehen: Für das ISMS gilt es, permanent eine Vielzahl von Hard- und Softwarekomponenten, Netzwerken, Cloud-Lösungen und weiteren Bausteinen der firmeneigenen IT zu kontrollieren. Eine echte Mammutaufgabe.

Das Connecting Media ServiceCockpit

An dieser Stelle kommt das ServiceCockpit von Connecting Media (CMSC) ins Spiel. „Mit unserem ISMS der nächsten Generation hat der Nutzer alles ganz einfach im Blick“, bringt Geschäftsführer 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.

Das Schweizer Taschenmesser für alle Einsatzzwecke

Auch in punco Implementierung wurde das Produkt bereits zu Ende gedacht. Je nach Kundengröße und vorhandener Infrastruktur passt sich die Installation des ServiceCockpit problemlos den Gegebenheiten an. Ob 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 ist für jeden Use Case etwas dabei.

Das ISMS der nächsten Generation

Das bietet Ihnen das ServiceCockpit von Connecting Media (CMSC):

Lückenlose Überwachung und einfache System-Inventarisierung. Egal ob Hardware, Software, Netzwerke oder Kommunikationsgeräte: Das CMSC bildet beliebig viele IT-Infrastrukturkomponenten Ihres Unternehmens unter einer übersichtlichen Oberfläche ab. So behalten Sie auch bei komplexen Systemen immer die Kontrolle.

Automatische Berichte

Reports liefern Ihnen alle relevanten Informationen zum aktuellen Status der im System integrierten Komponenten. Durch diese proaktive Überwachung können Sie Fehler meist schon beheben, bevor sie zu Problemen werden. Ein echter Service-Mehrwert, den auch Ihre Kunden zu schätzen wissen.

Konfigurierbare Alarmierungen

Das CMSC sorgt dafür, dass die System-Meldungen zielgenau zugestellt werden: Per E-Mail, Team-Messenger oder über Ihr Ticket-system. Sie bestimmen selbst, wer in welchen Fällen benachrichtigt werden soll.

Managed Security

Das CMSC verwaltet alle Ihre Security-Systeme, informiert Sie über Compliance-Verstöße und hilft Ihnen dabei, Security Incidents zu verfolgen und zu dokumentieren.

IoT-Kompatibilität

Es ist flexibel erweiterbar. Ob klassi-sche IT-Devices wie PC, Smartphone und Laptop oder Trendthemen wie Industrie 4.0, Smart Metering und Smart Home – Connecting Media liefert Ihnen auf Wunsch für all Ihre Anforderungen und Schnittstellen eine individuelle Anpassung. Die Daten-abfrage findet entweder über TCP oder per REST-API statt. Sprechen Sie uns für weitere Möglichkeiten einfach an!

Integration von Cloud-Systemen

Auch Ihre Cloud Systeme aggregieren wir im CMSC. Alle Events und Alarme laufen in einer Konsole zusammen.

Skalierbarkeit

Das ServiceCockpit ist sowohl als virtuelle Software per Hyper-V und VMware wie auch auf unseren CMSC-Appliances verfügbar. Es passt sich jederzeit an Ihre Umgebung an und die Daten bleiben physikalisch stets in Ihrer Obhut und unter Ihrer Kontrolle.

Entlastung von Ressourcen

Durch die automatisierte Alamierung werden ihre IT-Mitarbeiter aktiv entlastet. Da sie schon vorab auf Probleme reagieren können und schnell sowie gezielt der Ursache auf die Spur kommen.

Erweiterbarkeit

Das CMSC wächst dynamisch mit Ihrer Infrastruktur. Der Funktions-umfang ist durch Anbindung neuer Konnektoren jederzeit erweiterbar und stellt somit für sie ein zukunfts-sicheres Investment dar.

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

German Mittelstand

Netzwerk.
Beziehungen schaden nur dem, der keine hat.

Business.
Keine(r) hat so viele Ideen wie alle.

Club.
Sich kennen ist mehr als eine Visitenkarte.

Machen. Ist wie wollen. Nur krasser.

Vision.

Im zukunftsorientierten, innovativen German Mittelstand sind eigenverantwortliche, neugierige und mutige Unternehmer(innen) aktiv engagiert, die dort Inspiration, Know-how sowie tragfähige Beziehungen finden und schätzen.

Themen.

Wir greifen die Themen auf, die unsere Zukunft und Strategien bestimmen, beleuchten Trends und sind aktiv in Sachen Innovation, Digitalisierung, E-Health, Finance, Cybersecurity, Leadership, Nachhaltigkeit, Mobilität oder auch Marketing & Sales. Um nur ein paar Aspekte zu nennen.

www.german-mittelstand.network

Aus gezeich net!

3 Ausgaben zum Sonderpreis

IT-Strategien und Lösungen für Entscheider. Testen Sie die, von der Deutschen Fachpresse ausgezeichnete Zeitschrift »*manage it*«, im Probeabonnement.

https://ap-verlag.de/angebote

Auch als **ePaper** im Abonnement

#chefsache: SecurITy WEEK

Eine Woche Know-how, Kontakte & Inspiration!

Foto: Tierney/Stock.Adobe.com

CYBER-BEDROHUNGEN ERKENNEN UND STOPPEN

Mit dem neuen Standard im Endgeräteschutz

CROWDSTRIKE

- CrowdStrikes Mission lautet: Wir verhindern Sicherheitsvorfälle
- Mit der Kombination von modernem AV, verwalteter Bedrohungssuche und Threat Intelligence können über die schlanke Single-Agent-Architektur selbst ausgefeilte Angriffe auf alle Workloads verhindert werden.
- Mehrfach von Kunden und führenden Analysten ausgezeichneter Endgeräteschutz

Cyberangriffe

Wie Unternehmen sich wappnen können

von Jörg Schauff, Strategic Threat Intelligence Advisor bei CrowdStrike

Opfer eines Cyberangriffes werden – für viele Unternehmen ein Schreckensszenario. Trotzdem unterschätzen noch immer viele die reale Gefahr, die von der heutigen Bedrohungslandschaft (Threat Landscape) ausgeht. Allein im Jahr 2020 sind laut CrowdStrike fast 60 Prozent der im Rahmen der Global Cybersecurity Attitude Survey befragten deutschen Unternehmen mindestens einmal Opfer eines Ransomware-Angriffs geworden. Und die Anzahl der Cybercrime-Aktivitäten steigt weiter, wie der Global Threat Report 2021 verdeutlicht. Mittlerweile gehen fast 80 Prozent aller von CrowdStrike OverWatch aufgedeckten Angriffe auf das Konto von eCrime-Akteuren. Ein beliebter Angriffsvektor ist dabei die Lieferkette, wie die jüngsten, hochkarätigen Backdoor-Angriffe verdeutlicht haben. Ein Grund mehr, sich intensiv mit der sich ständig wandelnden Bedrohungslandschaft und ihren Akteuren auseinanderzusetzen, um wirkungsvolle Methoden gegen ihre Tools, Techniken und Prozeduren (TTPs) zu finden.

Überblick und Schnelligkeit wichtiger als je zuvor

Da Angreifer ihr Arsenal stetig um neue TTPs erweitern sowie neue Allianzen bilden, um ihre Möglichkeiten auszubauen und die Reichweite zu vergrößern, sind Überblick und Schnelligkeit wichtiger als je zuvor. IT-Sicherheitsteams müssen flexibler, proaktiver und produktiver werden, um den Bedrohungen einen Schritt voraus zu bleiben. Mit aktuellen Bedrohungsdaten kann das Sicherheitsteam die Motive, Ziele und das Angriffsverhalten eines Angreifers besser verstehen. Und kann dadurch schnellere, fundiertere und datengestützte (IT-)Sicherheitsentscheidungen treffen und das eigene Verhalten im Kampf gegen Bedrohungsakteure von reaktiv auf proaktiv umstellen.

Eine Faustregel, die sich für IT-Infrastrukturen bewährt hat, ist die 1-10-60 Regel: Innerhalb einer Minute muss der Angriff erkannt werden, innerhalb von zehn Minuten muss er untersucht und bewertet sein und innerhalb von 60 Minuten muss er mit geeigneten Gegenmaßnahmen abgewehrt werden. Moderne und automatische Präventionsmittel, wie die signaturlose Schadcode-Erkennung durch KI-gestützte Verfahren in Kombination mit der kontinuierlichen Überwachung von Prozessen auf schädliches Verhalten machen dies möglich.

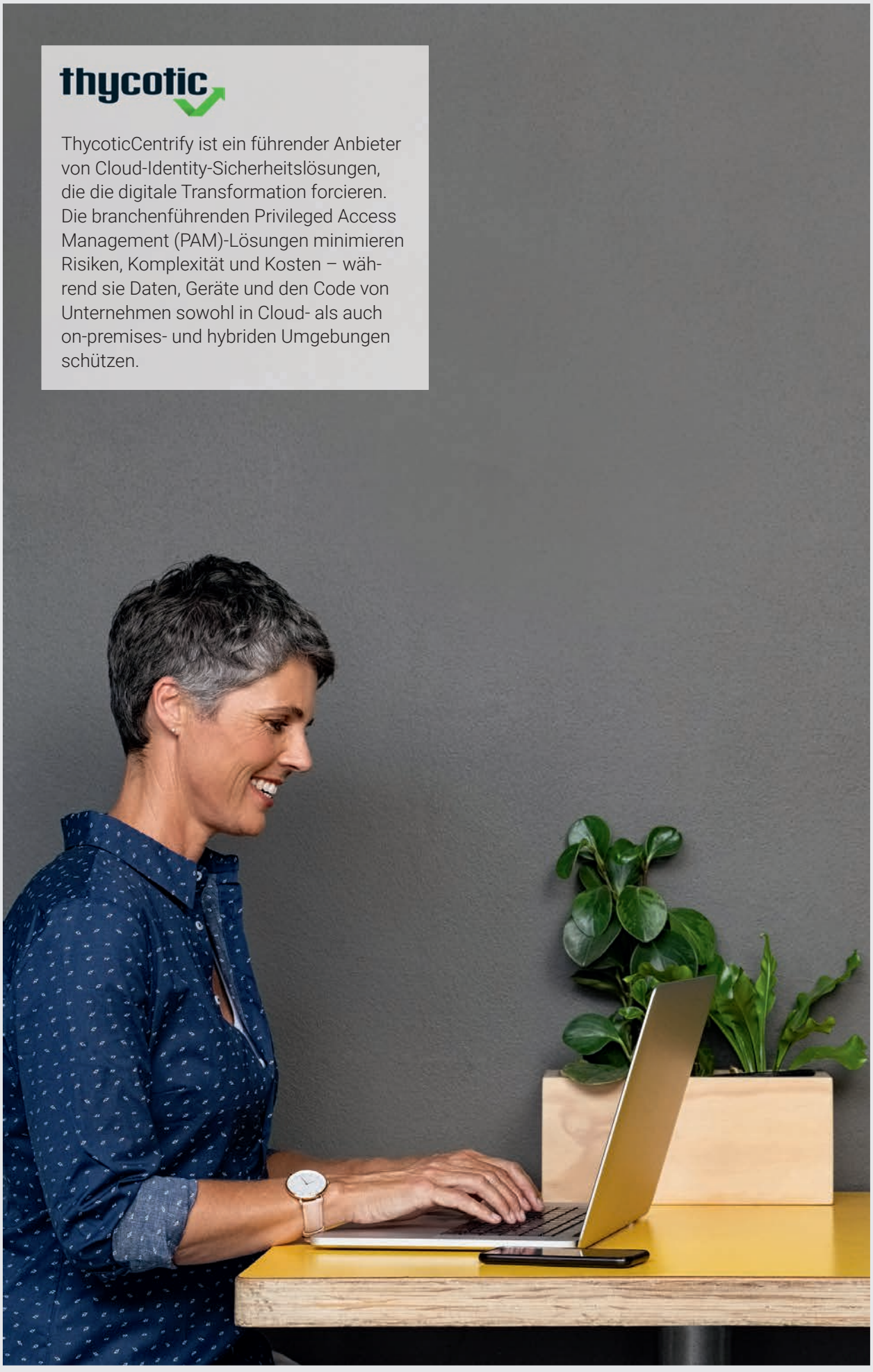
Was tun, wenn's brennt?

Wird ein Angreifer im Unternehmensnetzwerk entdeckt, ist ebenfalls die Geschwindigkeit entscheidend. Je länger es dauert, bis ein Spezialist hinzugezogen wird, desto höher ist die Chance, dass der Angreifer nicht nur umfangreich Daten abzieht, sondern sich im Netzwerk festsetzt (Lateral-Bewegung) und auch Vorkehrungen trifft, die ihm ermöglichen, bei einer Entdeckung jederzeit zurückzukehren. Daher sollte jede Organisation über einen Notfallplan verfügen.

Für Unternehmen geht es heutzutage nicht mehr um die Frage, ob sie Ziel eines Cyberangriffes werden, sondern wann. Bedrohungsdaten (Threat Intelligence) helfen Unternehmen, eine Verteidigung gegen die wahrscheinlichsten Angreifer vorzubereiten und ermöglichen es den Bedrohungsjägern (Threat Hunter), die Anzeichen eines Einbruchs zu erkennen und die Eindringlinge aus dem Netzwerk zu entfernen. Nur so können IT-Sicherheitsteams richtig und effektiv eingesetzt werden. In vielen Fällen ist es empfehlenswert, zusätzlich zu Threat Intelligence ein externes, vollständig gemanagtes Cybersicherheits-Serviceteam zu beschäftigen, das nicht nur Threat Intelligence, sondern auch Incident Response, Threat Hunting, Endpoint Recovery Services und proaktives Monitoring durchführen kann, um Sicherheitslücken zu schließen.

Kontaktieren Sie uns unter:
germany@crowdstrike.com

+++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++


thycotic
ThycoticCentrify ist ein führender Anbieter von Cloud-Identity-Sicherheitslösungen, die die digitale Transformation forcieren. Die branchenführenden Privileged Access Management (PAM)-Lösungen minimieren Risiken, Komplexität und Kosten – während sie Daten, Geräte und den Code von Unternehmen sowohl in Cloud- als auch on-premises- und hybriden Umgebungen schützen.

thycotic

Effektive Least-Privilege-Kontrollen

Endpunkte stellen nach wie vor die größte Schwachstelle in der Unternehmens-IT dar. In Zeiten, in denen immer mehr Mitarbeiter dezentral im Homeoffice arbeiten und Endgeräte – einschließlich Laptops, Tablets oder Smartphones – immer häufiger die geschützte Unternehmensumgebung verlassen, ist die Bedrohung realer denn je. Denn die Benutzeridentität ist nun zum neuen Perimeter der Cybersicherheit geworden, was die Angriffsfläche der Unternehmen drastisch vergrößert hat. Galten lange Zeit ausschließlich IT-Mitarbeiter wie Administratoren als privilegierte und daher besonders schützenswerte Nutzer, müssen heutzutage so gut wie alle Mitarbeiter, die Zugang zur Unternehmens-IT oder der Cloud-Infrastruktur haben, als Privileged User eingestuft und dementsprechend gemanagt werden.

Ein effektiver Weg, um das Risiko von Privilegien-Missbrauch über Endpunkte zu kontrollieren, führt über ein strategisch umgesetztes Endpoint Privilege Management (EPM). Dieses umfasst eine Reihe von Technologien und Sicherheitsmaßnahmen, welche die Umsetzung eines risikobasierten Zero-Trust-Modells sowie eines Least-Privilege-Ansatzes verfolgen. Denn durch die konsequente Beschränkung von Zugriffen gemäß der Rolle und Funktionalität eines jeden Users hilft EPM den IT-Abteilungen, Bedrohungen wie Ransomware, Datendiebstahl oder Manipulationen auszumerzen und Schäden zu mindern.

Was bedeutet EPM?

Dringen Cyberkriminelle in ein Netzwerk ein, nutzen sie in erster Linie Windows-, macOS- und Linux-Endgeräte als Einstiegspunkt. Dort angekommen, versuchen sie, privilegierte Accounts zu kompromittieren. Angriffe dieser Art sind in erster Linie auf mangelhafte Passwort-Hygiene zurückzuführen sowie auf Benutzer, die über zu weitgefasste Berechtigungen für den Zugriff auf Endpunkt- und Netzwerkressourcen verfügen.

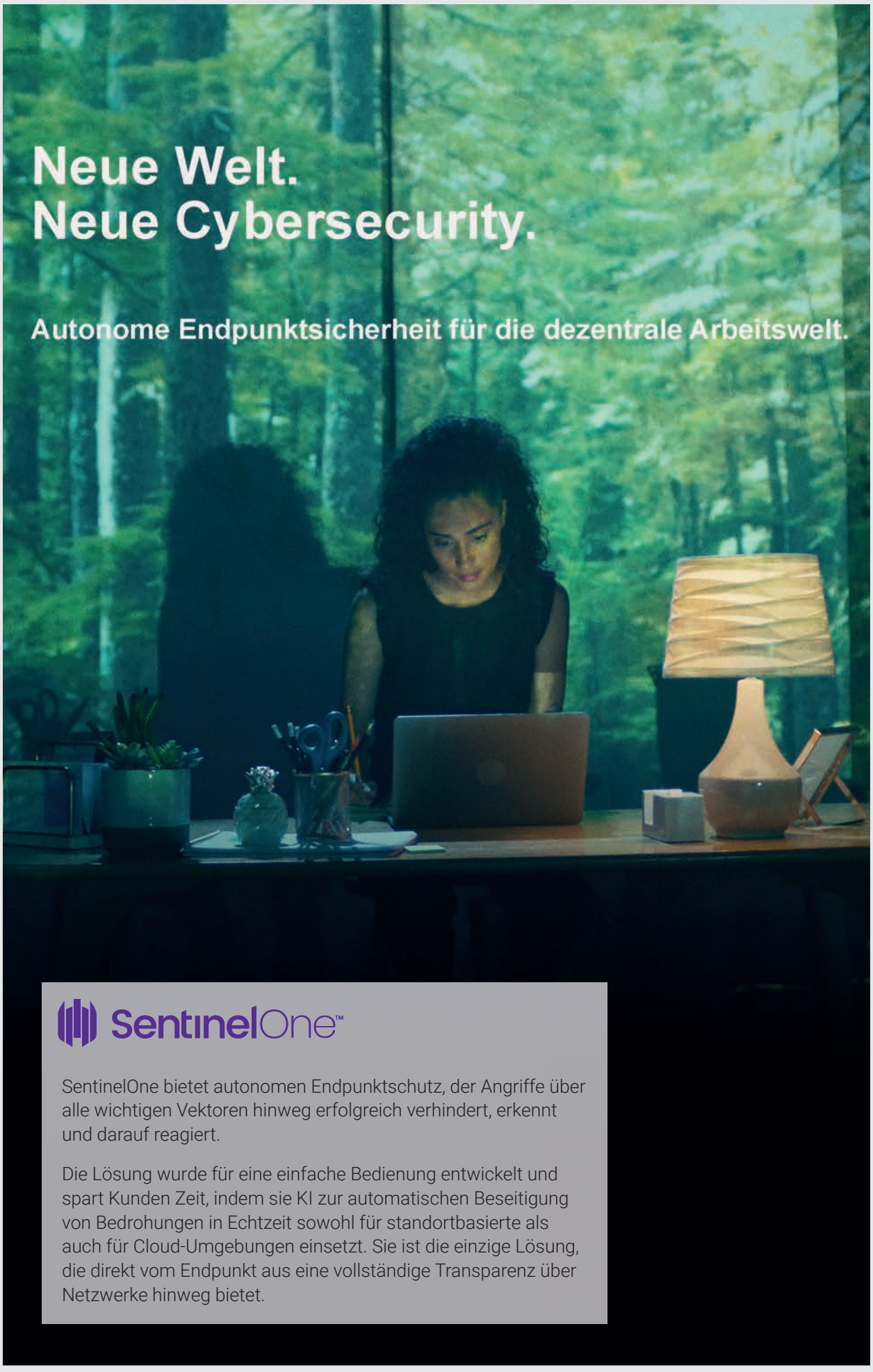
Endpoint Privilege Management (EPM) dämmt diese gefährliche Schwachstelle ein, indem es einen Zero-Trust-Ansatz verfolgt und auf sämtliche Benutzer, Anwendungen und Dienste das Least-Privilege-Prinzip anwendet. Hierbei wird sichergestellt, dass jede Identität nur auf die Programme und Daten zugreifen kann, die sie zum Ausführen ihrer Tätigkeit auch benötigt. Berechtigungen zur Erhöhung von Privilegien müssen dabei streng kontrolliert und überwacht werden.

„Komplexität ist tödlich“

Dieser Satz gilt für die Endpunktsicherheit wie für die gesamte IT-Security. Daher gilt es eine EPM-Lösung zu wählen, die eine ausgewogene Balance zwischen Leistung und Benutzerfreundlichkeit bietet und die Produktivität der Mitarbeiter nicht behindert. Die Software sollte richtliniengesteuert, flexibel und automatisiert sein. Sie sollte zudem eine schnelle Implementierung und aus IT-Sicht relativ einfache Installation ermöglichen. Eine skalierbare und flexibel erweiterbare Lösung stellt sicher, dass sich diese stets an die Anforderungen des Unternehmens anpasst und nicht umgekehrt.

Beim Implementierungsprozess müssen sich die Security-Experten zunächst auf die Endpunktsicherheits-Tools konzentrieren, die die geringsten Auswirkungen auf die Benutzer haben. Anschließend sollte in der gesamten IT-Umgebung schrittweise das Least-Privilege-Prinzip eingeführt und durchgesetzt werden. Sobald das erledigt ist, können weitere unverzichtbare Endpunkttechnologien wie Antivirus- oder Endpoint-Detection-and-Response-(EDR)-Lösungen integriert werden, um schließlich eine umfassende Defense-in-Depth-Strategie zu realisieren.

+++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++



SentinelOne™

SentinelOne bietet autonomen Endpunktschutz, der Angriffe über alle wichtigen Vektoren hinweg erfolgreich verhindert, erkennt und darauf reagiert.

Die Lösung wurde für eine einfache Bedienung entwickelt und spart Kunden Zeit, indem sie KI zur automatischen Beseitigung von Bedrohungen in Echtzeit sowohl für standortbasierte als auch für Cloud-Umgebungen einsetzt. Sie ist die einzige Lösung, die direkt vom Endpunkt aus eine vollständige Transparenz über Netzwerke hinweg bietet.

Security in einer sich wandelnden Welt

Die fordernden Ereignisse des letzten Jahres wurden für Unternehmen auch zu einer Angelegenheit der Cybersicherheit: Die rasche Absicherung der Arbeitskräfte im Home Office erhielt Priorität. Menschen, Technologie, Visionen – alles befindet sich in der heutigen Arbeitswelt im ständigen Wandel, muss mit der Zeit gehen und sich ständig anpassen. Es ist daher notwendig, veraltete Technologie, wie traditionellen Virenschutz und althergebrachte Endpunkt-Lösungen, hinter sich zu lassen. Die heutige Betriebsumgebung erfordert Technologie, die speziell für die moderne Welt entwickelt wurde.

Durch die Einbettung einer Künstlichen Intelligenz (KI) in jedes Gerät zur Prävention von Bedrohungen und Reaktion darauf in Echtzeit, in Verbindung mit der hohen Cloud-Skalierung, ist SentinelOne sehr gut positioniert, um Unternehmen in Zeiten des Home Office zuverlässig zu schützen – sie darüber hinaus sogar stärker, widerstandsfähiger und erfolgreicher zu machen.

Dynamische IoT-Sicherheit für jedes Gerät

Das moderne Unternehmen besteht nicht mehr nur aus Windows- und Mac-Endpunktgeräten oder Linux-Servern. Ob zu Hause oder im Büro: CISOs müssen wissen, wie viele Geräte im Unternehmen vorhanden sind, wo sich diese Geräte befinden und um welche Geräte es sich handelt. SentinelOne bietet die einzigartige Möglichkeit, durchdringende Transparenz der Netzwerkumgebung zu erreichen und die Kontrolle über die Absicherung der Angriffsfläche des Unternehmens zu erlangen – ohne neue Software oder Hardware einsetzen zu müssen. Ganz gleich außerdem, ob es sich um ein Endpunktgerät, einen Container oder einen Drucker handelt: Die Singularity-Plattform von SentinelOne ist die einzige Sicherheitsplattform für Endpunkte, um diese Vorteile nutzbar zu machen.

Online- und Offline-Schutz in Echtzeit

Derzeitige Malware braucht keine bestehende Internetverbindung, um auf dem Zielrechner zu handeln, doch alle Cybersicherheitsprodukte auf dem Markt benötigen diese Verbindung, um zu funktionieren. Cyberkriminelle haben also den Vorteil, dass viele Unternehmen noch veraltete Antivirus-Lösungen verwenden und sich damit angreifbar machen. Die patentierte Sicherheitslösung von SentinelOne zur Prävention, Erkennung und Reaktion hingegen arbeitet auch ohne aktive Anbindung ans Internet. Das ist enorm wichtig angesichts der Bedrohungslage, denn das Unternehmen heutiger Prägung benötigt Schutz in jeder Sekunde – unabhängig von der Netzwerkkonnektivität.

Rückblickend betrachtet haben sich die vergangenen Monate als Zeitraum des beschleunigten Wandels erwiesen, insbesondere im Bereich der Cybersicherheit. Hier still zu stehen und nicht zu handeln, bedeutet eigentlich einen Rückschritt. Doch die Taktik besteht heutzutage nicht mehr nur aus der Verschlüsselung von Geräten, sondern es gilt das Durchsickern von Daten zu verhindern, um Erpressung unmöglich zu machen. Sonst werden Unternehmen geschädigt und Kundendaten kompromittiert. Es reicht darum nicht mehr aus, dem Problem mit mehr Mitarbeitern in der IT-Abteilung zu begegnen – die sowieso auf dem Arbeitsmarkt kaum vorhanden sind – denn die Zeitmenge, um auf eine Bedrohung zu reagieren, ist kostbar und sollte daher gering gehalten werden. Automatisierte Lösungen sind hier schneller, fehlerfreier und entlasten außerdem das Personal. Hinzu kommt, dass die Vorfälle, die derzeit für Schlagzeilen sorgen, immer wieder zeigen, dass veraltete Technologie die Gegner nicht aufhalten kann. Es ist daher die Zeit reif für neue Maßnahmen, Techniken und Sicherheitslösungen zur Bekämpfung der aktuellen Bedrohungslandschaft.

+++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++

zoom

Zoom is for you. Mit unserer Video-basierten und sicheren Kommunikationsplattform setzen wir den Standard für Innovation. Aufgrund der intuitiv zu bedienenden Oberfläche und der hohen Skalierbarkeit ist Zoom gleichermaßen für Endanwender, kleine und mittlere Unternehmen sowie Konzerne geeignet. Zoom wurde 2011 gegründet, ist börsennotiert (NASDAQ:ZM) und hat seinen Hauptsitz in San Jose, Kalifornien.

Eine sichere hybride Arbeitswelt

Das vergangene Jahr war vor allem durch einen kollektiven und plötzlichen Wandel hin zu einer dezentralen Belegschaft gekennzeichnet. Auch 2021 bringt einige Veränderungen mit sich und wird mehr und mehr zum Jahr der hybriden Arbeitsmodelle. Während einige Mitarbeitende sicher zur Arbeit zurückkehren, werden andere weiterhin von zuhause aus arbeiten. Daneben wird es auch eine Mischung aus beidem geben. Eine solche hybride Belegschaft bringt zwar Flexibilität und Skalierbarkeit, gleichzeitig stellt sie aber auch eine komplexe Herausforderung an die IT dar, die einen durchdachten Sicherheitsansatz erfordert. Dabei muss es sich um eine Strategie handeln, die auf den Schutz der Mitarbeitenden ausgelegt ist. Um diese moderne Art des Personals abzusichern, sollten IT-Teams die folgenden vier Ansätze verfolgen:

1. Den Datenschutzprozess weiterentwickeln

Eine verteilte Belegschaft führt unweigerlich zu unterschiedlichen Daten. Wenn Mitarbeitende weltweit Informationen austauschen und dabei sowohl private als auch Firmengeräte verwenden, kann die Überwachung dieser Aktivitäten eine große Herausforderung für die IT-Abteilung darstellen. Verstärkt wird dies noch durch wichtige Fragen des Datenschutzes. Die Belegschaft arbeitet in einzigartigen Umgebungen – Mitarbeitende müssen deshalb sehr sorgfältig mit Kundendaten umgehen, um deren Privatsphäre immer zu priorisieren. Eine effektive Endpunkt-Datenschutzstrategie wird somit zum entscheidenden Faktor.

2. Private Geräte strategisch nutzen

Damit hybride Belegschaften erfolgreich sein können, müssen Unternehmen die aktuellen Umstände zu ihrem Vorteil nutzen. Da "Bring Your Own Device" (BYOD) zur Norm wird, können IT-Teams diese privaten Geräte über eine Multi-Faktor-Authentifizierung strategisch nutzen. So kann durch eine solche Authentifizierung das Risiko einer Datenkompromittierung auf privaten Smartphones & Co. verringert werden. Zudem wird das Thema Sicherheit zu einem Teil der täglichen Routine der Mitarbeitenden.

3. Regelmäßige Schulungen priorisieren

Eine der effektivsten Möglichkeiten, die Sicherheit eines Unternehmens zu erhöhen, besteht im Anbieten moderner Trainings. Schulungen und kontinuierliches Lernen helfen den Mitarbeitenden zu verstehen, welche Rolle sie als Endnutzer für die Gesamtsicherheit eines Unternehmens spielen. Dies schafft eine Sicherheitskultur, in der sich alle Beteiligten in den Gesamtschutz einer Organisation eingebunden fühlen.

4. Technologie einsetzen, die sich auf Flexibilität und Sicherheit fokussiert

Zoom ermöglicht mit flexiblen und skalierbaren Lösungen eine effektive Zusammenarbeit in der hybriden Arbeitswelt. Mit Zoom Meetings, Zoom Video Webinars, Zoom Phone und Zoom Rooms können Nutzer von überall aus arbeiten – im Büro, zu Hause oder beides. Bei der Entwicklung dieser Lösungen steht die Sicherheit immer an erster Stelle. Jedes Angebot umfasst dabei eine Reihe von Funktionen, die für die Absicherung des Zoom-Erlebnisses entwickelt wurden.

Fazit: Arbeitskräfte sollten überall befähigt werden

Eine hybride Belegschaft erfordert einen hybriden Ansatz für die Sicherheit, der zur Förderung einer agilen Strategie sowohl Technologie als auch Schulungen nutzt. Indem Unternehmen die neuen Anforderungen der hybriden Arbeitswelt annehmen, schaffen sie einen realistischen und skalierbaren Sicherheitsansatz, der sich mit dem Unternehmen weiterentwickelt. So können Unternehmen ihre Abläufe zukunftssicher gestalten und gleichzeitig eine sichere und effektive Zusammenarbeit ermöglichen. Mehr über die aktuellsten Sicherheitsvorkehrungen von Zoom und wie Mitarbeitende sich überall unterstützen lassen, finden Sie auf zoom.us.

+++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++ SecurITy WEEK +++

noris network
RZ-SICHERHEIT?
WIR ÜBERTREIBEN
GERNE!
FREIE RECHENZENTRUMSFLÄCHEN
MÜNCHEN | NÜRNBERG | HOF
noris.de/unsere-rechenzentren

SecurITy WEEK

Partner & Unterstützer

Foto: Tierney/Stock.Adobe.com

Foto: photon_photo/Stock.Adobe.com

„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-Sicherheits- 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 Managementsysteme 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-Sicherheit 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

digiWiesn

18. September bis 03. Oktober 2021

Mit dabei u.a.:

StM Dorothea Bär

Werner Theiner

Julia Christina Bauer

Andreas Keck

Franz Georg Strauß

Célia Martin

Die Business Wiesn unter der Schimherrschaft von Staatsministerin Dorothea Bär.

Für viele ist das Münchner Oktoberfest auch ein Ort fürs Business. Hier trifft man Geschäftsfreunde, werden bestehende Kontakte gepflegt und neue geknüpft.

Die #digiWiesn ist eine großartige Plattform für branchenübergreifende Kontaktpflege und -erweiterung, für Sichtbarkeit im Markt, Erfahrungsaustausch, Wissensvermittlung und Inspiration.

Jetzt informieren:

www.digiWiesn.bayern

ein Event von Werner Theiner

präsentiert von:

noris network

in Kooperation mit:

German Mittelstand

unterstützt von:

HUAWEI zoom WZON smart business networking

Sichere Geschäftskommunikation mit GoToConnect

HERAUSFORDERUNG

Connecting Media ist zwar ein Kleinunternehmen, betreut aber Kunden vom Friseurladen nebenan bis hin 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 LogMeIn Channel Team kontaktiert wurde: „Ich muss gestehen, bis dato war mir LogMeIn 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 Elmar Kaufmann kennen, der einen technischen Pitch zu **GoToConnect, der Voice-over-IP-Telefonanlage von LogMeIn, 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 GoToConnect war ich von Tag eins so begeistert, dass ich gleich Nägel mit Köpfen machte und die Telefonanlage in unser Produktportfolio mitaufnahm“, 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 LogMeIn vertraut und mit GoToConnect gut aufgestellt, war die Suche nach einer professionellen Telefonanlage für Connecting Media also abgeschlossen.

LÖSUNG

Die Integration und Einbindung von GoToConnect 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 so weit, dass ich fast nur noch GoToConnect pitche." Besonders überzeugt haben Kunz aber die einfache Bedienbarkeit und die Benutzeroberfläche: „Gerade im Vergleich mit anderen Anbietern ist die Bedienbarkeit keine Raketenwissenschaft. Bei GoToConnect muss sich 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 Boot hole, weil ich hier Schulungsaufwand habe. Heißt im Klartext: Ich muss meine Techniker briefen", betont Kunz an dieser Stelle und lobt: „Bei GoToConnect 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.

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

Außerdem konnte Connecting Media über GoToConnect 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 GoToConnect 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.

„Mit GoToConnect 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

ISO SCHMIEDE

IHR WEG ZUR ZERTIFIZIERUNG

ANALYSE

Bestandsaufnahme der vorliegenden Dokumente und Strukturen

Erstellung Projektplan

Abschlussbericht

UMSETZUNG

Bereitstellung bewährter ISO-Dokumentvorlagen

Anleitung zur Handhabung der Dokumente

Eine Korrektur-schleife aller bereitgestellten ISO-relevanten Dokumente

INTERNES AUDIT

Durchführung eines internen Audits gemäß ISO-Norm

Detaillierter Auditbericht

Prozess-sensibilisierung zertifizierungs-verantwortlicher Mitarbeiter

Die ISO Schmiede ist eine Marke der Connecting Media. Es gelten Impressum, Daten-schutz und auch die AGBs der Connecting Media, für sämtliche Dienstleistungen der ISO Schmiede.

Foto: WrightStudio/Stock.Adobe.com

UNSERE BETREUUNGSPAKETE

GOLD (24 Monate Laufzeit nach Stufe 2)

1.000 € PRO MONAT

- 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)

750 € PRO MONAT

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

BRONZE (24 Monate Laufzeit nach Stufe 2)

200 € PRO MONAT

- 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 (z.B. DQS, TÜV Süd, Dekra)

FEINJUSTIERUNG

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

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" – DER PODCAST FÜR IT-SICHERHEIT, DATENSCHUTZ, UND IT-SERVICE!

Erfahren Sie, wie Sie Ihr Unternehmen sicher in das 21. Jahrhundert steuern und so bestens für die Zukunft gewappnet sind. Im Angesicht der Digitalisierung ist Sicherheit nie genug – denn: Der Hacker stirbt nie!

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

Verfügbar auf:

Listen on Apple Podcasts

Listen on Spotify

Listen on YouTube

IMPRESSUM

Connecting Media
Andreas Kunz, CEO & Founder

Ettlinger Straße 31
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.

Connecting Media

Folgen Sie uns auf:

in	**LINKEDIN**	www.linkedin.com/company/27108974/
X	**XING**	www.xing.com/companies/connectingmedia
f	**FACEBOOK**	www.facebook.com/ConnectingMedia.de/
	INSTAGRAM	https://www.instagram.com/connecting_media/
	YOUTUBE	http://youtube.connectingmedia.de