AUSGABE 2

cm magazin

0101000011010101100101 1010101010101110

HÖCHSTE ZEIT FÜR HÖCHSTE SICHERHEIT

IT-SECURITY

IT-SERVICE

DATENSCHUTZ

NEWSLETTER!

Registrieren Sie sich für unseren Newsletter und erfahren Sie mehr über die neuesten Aktivitäten und Angebote von uns:

Connecting Media

www.connectingmedia.de/kontakt/#newsletter

Ahoi!

Wir freuen uns sehr dieses Jahr wieder die SecurityCruise ausrichten zu dürfen. Aufgrund der derzeitigen besonderen Situation, mussten wir uns für ein digitales Veranstaltungskonzept entscheiden, welches wir Dank viel Herzblut und Teamwork noch kurzfristig auf dieses Format adaptieren konnten.

An alle, die letztes Jahr schon dabei waren und an alle neu dazu gekommenen Landratten ein herzliches Willkommen zur 2. SecurityCruise, dem digitalen IT-Security Kongress.

Die SecurityCruise von Connecting Media vernetzt Akteure für einen branchenübergreifenden Austausch zu den Themen IT-Security und Datenschutz.

Mit neuen Kooperationspartnern, wie der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si), dem German Mittelstand e.V. und dem Cyber Forum, finden Sie heute die passende Umgebung um sich zwanglos rund um IT-Security und Datenschutz auszutauschen.

Lernen Sie von unseren Top-Speakern der Branche, wie Sie mit Ihrem Unternehmen in sichere Fahrwasser gelangen.

Und damit Leinen los für die 2. SecurityCruise!

Andreas Kunz
CEO Connecting Media

SecurityCruise

Der digitale IT-Security Kongress

Erleben Sie am 8. Juli auf der ‚MS Digital', die komplette Welt der IT-Sicherheit. Sei es Endpoint-, Netzwerk-, Cloud Sicherheit oder generell Datenschutz mit dem Schwerpunkt DSGVO. An nur einem Tag stellen wir Ihnen Lösungen zu allen Bereichen vor, damit Sie für die täglich zunehmenden Bedrohungslagen gewappnet sind. Tauchen Sie ein in die Welt der IT-Sicherheit!

Besuchen Sie in der **Tech Academy** und den **Benefit Talks** die Vorträge von unseren Herstellern, welche die unterschiedlichen Facetten der IT-Sicherheit erläutern und tauschen Sie sich in den einzelnen **Herstellerräumen** im Detail aus. Nutzen Sie die Chance und bekommen Sie die neuesten Infos aus 1. Hand, um den Hackern und Ihren Mitbewerbern einen Schritt voraus zu sein!

Das Programm der SecurityCruise 2020

12.45–13.00 UHR **„OPENING"**

TECH ACADEMY	BENEFIT TALKS	WORKSHOPS	TALKRUNDEN
„Von Nerds für Nerds"	**„Von Entscheidern für Entscheider"**	**„Neue Horizonte entdecken"**	**„Unsere Experten im Austausch"**
13.00 –15.20 Uhr	13.00 –15.20 Uhr	13.00 –18.00 Uhr	13.00 –18.00 Uhr
Netzwerken	**Netzwerken**	Quo Vadis Datenschutz *Anna Cardillo*	Identität und Haftung
16.00 –18.00 Uhr	16.00 –18.00 Uhr	Erfolgreich, gesund, glücklich *Andreas Trienbacher*	Digitalisierung ja, aber sicher!
		IT-Sicherheit *Mark Semmler*	Wirtschaftsfaktor Rechenzentrum!
		Körpersprache *Stefan Verra*	KARLSRUHE – Das Silicon Valley Deutschlands!

Ab 18 UHR **„GET TOGETHER"**

TECH ACADEMY

Uhrzeit	Vortrag	Firma
13:00 –13:20 Uhr	Sichere Videokonferenzen DSGVO-konform betreiben	StarLeaf
13:20 –13:40 Uhr	Die richtige Netzwerkautomatisierung mit der Management Cloud	LANCOM Systems GmbH
13:40 –14:00 Uhr	Mit VPN als Managed Service die Business Continuity auch in Krisenzeiten sicherstellen	NCP engineering GmbH
14:00 –14:20 Uhr	Infrastrukturen im Wandel: Secure SD-WAN - Smart, Simple, Secure	Nuvias Deutschland GmbH
14:20 –14:40 Uhr	Wie finde ich alle Schwachstellen in meiner heterogenen IT-Landschaft?	Enginsight GmbH
14:40 –15:00 Uhr	Wie automatisiere ich die Turnschuhadministration?	RamgeSoft GmbH & Co. KG
15:00 –15:20 Uhr	Das ServiceCockpit ... die Geheimwaffe für Datenschutz und Sicherheit	Connecting Media
16:00 –16:20 Uhr	Wie funktioniert ein Cloud Access Broker (CASB) mit Bitglass?	Boll Europe GmbH
16:20 –16:40 Uhr	Data Classification und eine durchgängige Compliance auch mit Office 365	Varonis Systems GmbH
16:40 –17:00 Uhr	Wie funktioniert eine Isolation Plattform mit Menlo Systems?	Boll Engineering AG
17:00 –17:20 Uhr	DeepInstinct: mit Deep Learning zur maximalen Endpoint Sicherheit!	Spectrami GmbH
17:20 –17:40 Uhr	Maximale Sichtbarkeit mit Delta Master	Makrofactory GmbH & Co. KG
17:40 –18:00 Uhr	Leistungs- und Verfügbarkeitstest as a Service	Login VSI

BENEFIT TALKS

Uhrzeit	Vortrag	Firma
13:00 –13:20 Uhr	ROI mit Digitalisierung? Gewährleisten Sie Ihre Geschäftskontinuität!	Login VSI
13:20 –13:40 Uhr	Seien Sie jederzeit Herr Ihres Datenflusses - Dank Berechtigungsmanagement!	Makrofactory GmbH & Co. KG
13:40 –14:00 Uhr	Unbekannte Bedrohungen vor allen anderen Erkennen!	Spectrami GmbH
14:00 –14:20 Uhr	Menlo Security: Null Prozent Malware durch Isolation	Boll Engineering AG
14:20 –14:40 Uhr	Datensicherheit und Bedrohungserkennung in Microsoft 365!	Varonis Systems GmbH
14:40 –15:00 Uhr	Maximale Sicherheit im Cloud-Umfeld!	Boll Europe GmbH
15:00 –15:20 Uhr	Manuelle und intensive IT-Prozesse kinderleicht automatisieren!	RamgeSoft GmbH & Co, KG
16:00 –16:20 Uhr	Security und Datenschutz as a Service aus einer Hand!	Connecting Media
16:20 –16:40 Uhr	Cyberhygiene: Sicherer IT-Betrieb so einfach wie das tägliche Händewaschen	Enginsight GmbH
16:40 –17:00 Uhr	Social Distancing - Passende technische Lösungen für Unternehmen aller Branchen!	Nuvias Deutschland GmbH
17:00 –17:20 Uhr	Business Continuity – Enterprise VPN minimiert Geschäftsrisiken	NCP engineering GmbH
17:20 –17:40 Uhr	Reduzierte Kosten, mehr Bandbreite und maximale Flexibilität durch SD-WAN!	LANCOM Systems GmbH
17:40 –18:00 Uhr	Datenschutz- und Sicherheitsmanagement für den Mittelstand	Intervalid GmbH

WORKSHOPS

Uhrzeit	Vortrag	Speaker	Firma
13:00 –14:30 Uhr	Quo Vadis Datenschutz – Worauf Sie im Jahre 2020 besonders achten müssen!	Anna Cardillo	Cardillo Consulting
14:30 –15:30 Uhr	Erfolgreich, gesund und glücklich auch im Büroalltag!	Andreas Trienbacher	Mr. T's Fitness Factory
15:30 –17:00 Uhr	Informationssicherheit – der Brandschutz des 21. Jahrhunderts!	Mark Semmler	Mark Semmler GmbH
17:00 –18:00 Uhr	Körpersprache – Authentisch sowohl in online als auch offline Meetings!	Stefan Verra	Stefan Verra GmbH

TALKRUNDEN

Uhrzeit	Vortrag	Talkgäste	Firma
13:00 –13:40 Uhr	Identität und Haftung Moderation: Werner Theiner & Andreas Keck – German Mittelstand e.V.	Peter van Zeist Steffen Siguda Georg Lindner tba	LastPass by LogMeIn OSRAM AG Dr. Hörtkorn München GmbH Authlogics Ltd.
14:20 –15:00 Uhr	Digitalisierung ja, aber sicher! Moderation: Werner Theiner und Andreas Keck – German Mittelstand e.V.	tba Carsten Pinnow Kevin Breuer	Bundesamt für Sicherheit in der Informationstechnik (BSI) Datensicherheit.de Greenbone Networks GmbH
16:00 –16:40 Uhr	Wirtschaftsfaktor Rechenzentrum! Moderation: Werner Theiner und Andreas Keck – German Mittelstand e.V.	Joachim Astel Philip Schiede	noris network AG manage IT (ap Verlag GmbH)
17:20 –18:00 Uhr	KARLSRUHE – Das Silicon Valley Deutschlands! Moderation: Andreas Kunz – Connecting Media	Dirk Fox David Herrmanns Andre Tiede Sandra Jörg	KA-IT-Si CyberForum e.V. HubWerk01 Bruchsal BLACKPIN GmbH

Kurzfristige Änderungen sind möglich. Das tagesaktuelle Programm finden Sie unter **www.securitycruise.de ➜ Programm**

VdS Schadenverhütung:
IT-Sicherheit, die zu Ihrem Unternehmen passt

Informationssicherheit sollte insbesondere in kleinen und mittelständischen Unternehmen (KMU) individuell gestaltet werden. Der erreichbare Umsetzungsgrad hängt eng von den verfügbaren finanziellen und personellen Ressourcen ab.

Die VdS Cyber-Security Paketlösungen

Wir erleichtern Ihnen den Einstieg: VdS hat vorkonfigurierte Cyber-Paketlösungen entwickelt, die frei skalierbar sind und umfassende Module für die Verbesserung der Informationssicherheit enthalten. Die Angebotsbausteine reichen von der Ist-Analyse über Sofort-Maßnahmen bis hin zur zertifizierten Informationssicherheit nach VdS 10000 und werden zu verschiedenen Paketlösungen zusammengesetzt. Der Vorteil für Sie: Ein Paket aus einer Hand verursacht weniger administrativen Aufwand und ermöglicht eine sehr attraktive Preisgestaltung. Einige Bausteine sind bei Bedarf auch einzeln verfügbar, um Ihnen die Möglichkeit des Upgrades zu bieten, sollte sich Ihr Schutzbedarf verändern.

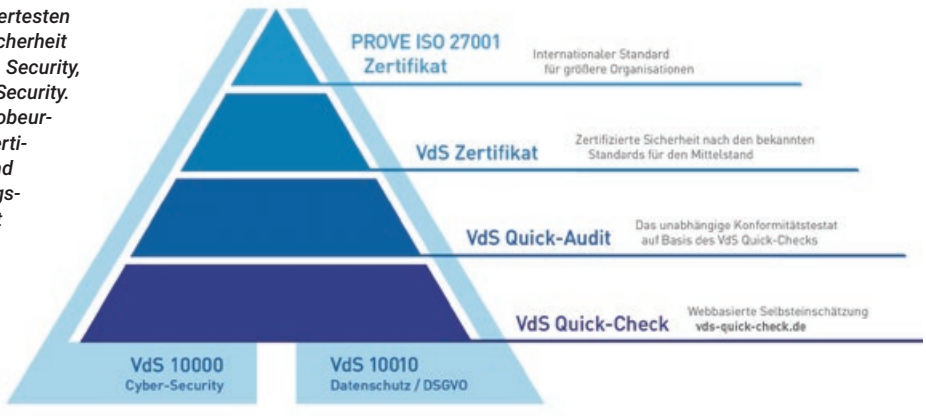
Vier vorkonfigurierte Pakete für individuellen Schutzbedarf

Die Paketlösungen beinhalten die folgenden Bausteine in unterschiedlicher Zusammensetzung:

- Das umfassende, webbasierte Schulungsprogramm für alle Ihre Mitarbeiter
- Den externen Scan Ihrer Internet-Domain
- Die Analyse Ihrer vorhandenen Cyber-Sicherheit durch den bekannten VdS-Quick-Check
- Das VdS-Quick-Audit zur effektiven Bestands- und Schwachstellenanalyse
- Der lückenlose interne Scan Ihrer IT-Systeme
- Die Zertifizierung und Überwachung Ihres Informationssicherheits-Managementsystems gemäß 10000

Ausführliche Informationen finden Sie unter:
https://vds.de/kompetenzen/cyber-security/die-vds-cyber-paketloesungen

VdS gehört zu den weltweit renommiertesten Institutionen für die Unternehmenssicherheit mit den Schwerpunkten Brandschutz, Security, Naturgefahrenprävention und Cyber-Security. Die Dienstleistungen umfassen Risikobeurteilungen, Prüfungen von Anlagen, Zertifizierungen von Produkten, Firmen und Fachkräften sowie ein breites Bildungsangebot. Das VdS-Gütesiegel genießt einen ausgezeichneten Ruf in Fachkreisen und bei Entscheidern.



German Mittelstand

german-mittelstand.network

Netzwerk.

Beziehungen schaden nur dem, der keine hat.

Business.

Keiner hat so viele Ideen wie alle.

Club.

Sich kennen ist mehr als eine Visitenkarte.

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

Aus dem Netzwerk für das Netzwerk

CyberForum
HIGHTECH. UNTERNEHMER. NETZWERK.

Der Motor der Digitalisierung

Das **CyberForum e.V.** ist mit über 1.200 Mitgliedern das größte regional aktive Hightech.Unternehmer. Netzwerk. in Europa. Im CyberForum vernetzen sich Unternehmer, Gründer, Kreative, Mitarbeiter aus Forschungseinrichtungen und Institutionen, Studierende, Business Angels und Auszubildende. Insgesamt repräsentieren die Mitglieder rund 30.000 Arbeitsplätze. Jährlich organisiert das CyberForum bis zu 200 Events zum Netzwerken und Weiterbilden, mit über 19.000 Besucher*innen (2019). Es setzt sich in der IT-Region Karlsruhe und auch darüber hinaus für den digitalen Mittelstand ein.

Einen weiteren Schwerpunkt bilden Angebote für Unternehmen in allen Wachstumsphasen: vom „Mentoring & Coaching" für Gründungsinteressierte, über das CyberLab, bis hin zur Unterstützung bei der Fachkräftesicherung. Die CyberForum Akademie vermittelt Expertenwissen aus dem CyberForum. Die breit gefächerten Weiterbildungsangebote unterstützen insbesondere kleine und mittelständische Unternehmen bei ihren Wachstums- und Marktherausforderungen. Auf individuellen Wunsch hin sind auch eigens von der CyberForum Akademie konzipierte Inhouse-Schulungen für Unternehmen möglich.

Zum CyberForum e.V. gehören auch: die Zweigstelle CyberForum Süd in Baden-Baden, die 100-prozentige Tochter CyberForum Service GmbH und das landesweite DIZ | Digitales Innovationszentrum (Gesellschafter: CyberForum e.V. und FZI Forschungszentrum Informatik), das die Digitale Transformation im baden-württembergischen Mittelstand vorantreibt. 1997 als Private Public-Partnership gegründet, beschäftigt das CyberForum mittlerweile ein 55-köpfiges Team qualifizierter Mitarbeiter*innen.

www.cyberforum.de

CyberLab
HIGHTECH. GRÜNDER. SCHMIEDE.

Die High-Tech-Gründer Schmiede

Das **CyberLab**, der IT-Accelerator des Landes Baden-Württemberg, bietet auf einer Fläche von 1.600 Quadratmetern Platz für vielversprechende Gründer-Innovationen. Allein 2019 erhielten hier mehr als 50 Start-up-Teams im Rahmen von Acceleratoren-Programmen Zugang zu Business-Mentoren und Investoren. CyberLab-Alumnis, die nach einer PreLab-Phase und erfolgreichem Pitch den Einzug ins CyberLab geschafft haben, erzielen heute Umsätze von mehr als 100 Millionen Euro und haben bereits mehr als 600 Arbeitsplätze geschaffen. Aktuelle CyberLab-Teams profitieren zudem von der Frühförderung „Start-up BW Pre-Seed", das Gelder von bis zu 200.000 Euro verspricht. Das CyberForum als Betreiber des CyberLab nimmt weder Anteile noch Provision. Nur einige von unzähligen Beispielen: GoSilico-Gründerin Dr. Teresa Bauer zählt zu den Top 40 der deutschen Jungunternehmerinnen; für die Quantencomputer-Technologie des Start-ups HQS Quantum-Simulations interessieren sich Groß-Konzerne rund um den Globus. Erst kürzlich wurde eine dreijährige Kooperation mit dem Life-Science-Unternehmen Merck eingegangen. HelioPas AI gehört zu den Top 5 der wichtigsten AI-Start-ups in der Agrarbranche. ***„Karlsruhe war schon digitale Start-up-Hochburg, bevor die Bedeutung von Gründungen überhaupt erkannt wurde"***, so David Hermanns, Geschäftsführer des CyberForum. Im Herbst 2018 startete das IT-Security PreLab zum ersten Mal. Dieses intensive Trainingsprogramm richtete sich an Startups aus dem Bereich der IT-Sicherheit. Dabei war es egal, ob die Teams sich auf IoT, Datenschutz, Blockchain, Kryptosicherheit, Compliance oder Cloud-Sicherheit spezialisiert haben – das IT-Security PreLab war und ist themen- und branchenoffen. Das auf IT-Security spezialisierte Accelerator Programm wird in einem einwöchigen Intensivtraining mit Workshops, Vorträgen und Mentoring durchgeführt.

www.cyberlab-karlsruhe.de

4 IT-SECURITY-STARTUPS, die man im Auge behalten sollte!

Diese 4 Startups haben **vom IT-Security-Lab profitiert** und wurden im Anschluss zur weiteren Begleitung in das CyberLab aufgenommen.

Inlyse schützt Unternehmen vor Malware und Cyberangriffen mit Hilfe von künstlicher Intelligenz. Durch revolutionäre Bilderkennungsmechanismen und selbstlernenden neuronalen Netzen können selbst die neusten und gefährlichsten Cyber-Bedrohungen identifiziert und abgewehrt werden. Mittels Plugins können Unternehmen diese Cloud-basierte Technologie mühelos ohne Expertenwissen in ihre IT-Infrastruktur integrieren, um kritische Schwachstellen zu schließen.

www.inlyse.com

Made and hosted in Germany. Die **BLACKPIN** App ermöglicht sicheres Kommunizieren in einem absolut verschlüsselten und geschlossenen System. Mit BLACKPIN kommunizieren Teammitglieder miteinander, tauschen Daten aus und können diese nachhaltig bis zu 15 Jahre archivieren. Unser mobile Messenger ermöglicht schnelleren asynchronen Austausch mit Kollegen, Kunden und Partner. Die Kommunikation erfolgt durch eine Komplett-Verschlüsselung nach dem AES256 Standard und die Archivierung der Daten auf Basis zertifizierten höchsten medizinischen deutschen Standards. Alle Daten liegen zentral in Deutschland. Erst im Januar hat Blackpin durch das baden-württembergische Start-up-Förderprogramm „Start-up BW Pre-Seed“ eine Förderung in Höhe von über 250.000 € erhalten.

www.blackpin.app

Gardion VPN ist ein ausschließlich in Deutschland betriebenes, hochsicheres VPN mit leistungsfähigen Netzwerkfiltern für den optimalen Schutz Ihrer Daten. Gardion setzt aktuell auf das hochsichere IPSEC-Protokoll und verhindert damit sicher Missbrauch. Das Startup wurde 2016 von Thomas Schlenkhoff mit der Absicht gegründet, seiner Familie und sich das optimale Internet gestalten zu können. 2017 kam Benjamin Fröhlich mit an Bord und brachte sein umfassendes technisches Know-how mit ein. Mittlerweile sind wir zu viert und wollen weiter wachsen. 2018 erhielten die Gründer Bundesmittel aus dem EXIST-Programm für technische Ausgründungen aus Hochschulen.

www.gardion.de

prenode entwickelt für Unternehmen künstliche Intelligenzen (KI), die ihnen bei Entscheidungen und Vorhersagen unterstützen. Hierzu verwenden wir innovative und neuartige Technologien, die es erlauben, KI auf verteilten, unternehmensübergreifend Datensätzen sicher zu entwickeln. Wir sind damit in der Lage bessere KI zu entwickeln und die Entwicklungs- und Implementierungszeit zu reduzieren. Durch ein mehrschichtiges Sicherheitssystem können wir darüber hinaus den Datenschutz gewährleisten.

www.prenode.de

Business Continuity und sichere Kommunikation

Durch die Corona-Pandemie bekommt das Thema Home-Office eine völlig neue Richtung. Plötzlich geht es nicht mehr darum, flexible Arbeitsmodelle zur Vereinbarung von Beruf und Familie oder Mitarbeiterbindung anzubieten, sondern die Arbeitsfähigkeit des Unternehmens zu erhalten und gleichzeitig die Gesundheit der Mitarbeiter zu schützen. VPN Technologien, für die externe Anbindung der Mitarbeiter ans Firmennetz und die sichere Kommunikation, sorgen urplötzlich für Business Continuity. Nuvias hat aus aktuellem Anlass mit dem deutschen Spezialanbieter NCP engineering aus Nürnberg, gesprochen der sich seit über 30 Jahren dem Thema Secure Communications verschrieben hat.

Nuvias: *Die Belegschaften wurden relativ schnell und spontan ins Home-Office geschickt, bleiben dabei nicht Aspekte wie Flexibilität und Sicherheit auf der Strecke?*

Tina Kaiser: Viele Unternehmen kämpfen mit technischen Problemen, wenn es um die Kapazitäten und Auslegung der Internetverbindungen in der Firmenzentrale und die genutzte Hardware geht. Eine so deutlich erhöhte Anzahl an VPN-Verbindungen kann teilweise nicht geleistet werden oder nur unter schlechterer Performance. In dieser Situation profitieren Unternehmen von softwarebasierten Lösungen wie wir sie bieten, die hochskalierbar und stabil sind.

Das bedeutet, dass keine zusätzliche Hardware beschafft werden muss, was bei Engpässen und Lieferzeiten von teilweise 6–8 Wochen ein riesiges Problem darstellt. Bezüglich der Sicherheit empfehlen wir genaues Augenmerk auf die Konfiguration der Profile und VPN-Verbindungen z.B. durch 2-Faktor-Authentifizierung und Maßnahmen zur Einhaltung der Compliance-Richtlinien.

Nuvias: *Dass Datenverlust und Hackerangriffe verheerende Folgen haben können, war ja bereits vor der Krise bekannt. Sind Unternehmen in der jetzigen Situation verwundbarer als sonst?*

Tina Kaiser: Es wäre gefährlich zu glauben, dass Cyberkriminelle die angespannte Situation der Unternehmen nicht ausnutzen. Die Gefahren haben sich nicht verändert, aber viele Unternehmen sind erst einmal damit beschäftigt, den Betrieb überhaupt am Laufen zu halten. IT-Sicherheit trägt einen großen Teil zu Unternehmenszielen bei. Angefangen beim Verlust vertraulicher Daten oder unerlaubten Zugriffen und Manipulation von Produktionsdaten über verschiedene Einfallstore, geht es im schlimmsten Fall sogar um einen Stillstand von Anlagen. Derzeit wird von einem erhöhten Aufkommen an Cyberangriffen, gerade auf Mitarbeiter im Home-Office berichtet. Hier hilft eine Lösung, die Fragen der Endpoint Security berücksichtigt. Einen vollständigen Zugriff auf das Firmennetz sollten, gerade im Home-Office, nur aktuelle, virenfreie und gepatchte Systeme erhalten. Sollte dies nicht der Fall sein, kann das System in einem Quarantänebereich aktualisiert und danach vollständig in das Firmennetzwerk eingebunden werden.

Nuvias: *Bei der Vielzahl an Security-Lösungen ist es aber doch quasi unmöglich, die eierlegende Wollmilchsau zu finden, die alles absichert und gleichzeitig in mein Unternehmenskonzept passt.*

Tina Kaiser: Es gibt Merkmale, die zunächst sehr nichtssagend klingen, die in der Praxis aber schlagende Argumente sind. Universelle Lösungen bieten beispielweise den Vorteil, dass sie sich gut in vorhandene Strukturen integrieren lassen und auch künftige Veränderungen mitmachen, egal ob geplant oder noch nicht bekannt. Ein Baustein der „eierlegenden Wollmilchsau“ sind die bereits erwähnten Authentisierungsmechanismen, die zukunftsfähig sind und aktuell durch Themen wie „PSD2“ immer mehr Einzug halten. Die Authentisierung mit zwei Faktoren ist eine Methode, mit der eine gezielte Absicherung der Zugänge erreicht werden kann. Der große Vorteil ist hier, dass jeder Mitarbeiter diese Mechanismen bereits aus seinem Alltag kennt.

Interview mit: Tina Kaiser, Deputy Head of Marketing bei NCP engineering

Warum man in der (Netzwerk) IT künstliche Intelligenz benötigt

Was ist die Antwort auf die große Frage nach dem Leben, dem Universum und allem? Kurz und knapp: „42“, wenn man dem Supercomputer Deep Thought (aus dem Roman „Per Anhalter durch die Galaxis“), Glauben schenken soll. Aber es war ja auch nur die einfache Frage „Nach dem Leben, dem Universum und dem ganzen Rest“ – nicht gerade geistreich. Wieso also sollte man KI in der IT einsetzen? Kurz und knapp, weil sie jetzt verfügbar und sinnvoll nutzbar ist. Diese Technik kann uns viele Dinge erleichtern, Fehler reduzieren, auf Engpässe hinweisen, Angriffe erkennen und abwehren und damit die Effektivität unserer Systeme massiv steigern und Kosten einsparen.

KI immer und überall?

Die Ursprünge der KI reichen bis in die 50er Jahre zurück. Während beim Anhalter durch die Galaxis noch ganze Planeten für die Rechenleistungen benötigt wurden, stehen uns heute die Cloud und schnellere Prozessorleistungen zur Verfügung. Diese Rechenumgebungen erlauben es uns, auch für den geregelten Netzwerkbetrieb ein völlig neuartiges Anwendererlebnis zu bieten.

Die Herausforderungen

- Keine umfassende Sichtbarkeit von Problemen, um die Beeinträchtigungen von Benutzererfahrungen zu spezifizieren
- Für drahtgebundene und drahtlose Domänen stehen nur begrenzt Messdaten zur Verfügung
- Manuelle Konfigurations- und Verwaltungsprozesse verursachten Ineffizienzen und waren /sind fehleranfällig
- Mangelnde oder nicht eingehaltene Compliance-Regeln werden selten entdeckt, gerade bei unterschiedlich eingesetzten Lösungen

Die Lösung

Eine Plattform auf Basis von KI und moderne Cloud-Plattformen mit Mikroservices, die in der Lage sind die gestellten Anforderungen an Verfügbarkeit, Durchsatz und Sichtbarkeit zu meistern und trotzdem im laufenden Betrieb, ohne Beeinträchtigung der aktiven Verbindungen, die Skalierbarkeit zu erhöhen.

Sie sind es leid zu hören, dass die Nutzerprobleme im Netzwerk liegen?

Beweisen Sie das Gegenteil, indem Sie die Nutzererfahrung in den kabelgebundenen oder kabellosen Netzwerken anhand der geforderten Leistungsmetriken, wie Durchsatz, Kapazität, Roaming und Betriebszeit, überprüfen und z.B. das Antwortzeitverhalten von Netzwerk-Infrastruktur Services (wie DHCP, DNS, AAA) mit in die Berechnungen einbeziehen. Die Netzwerkinfrastruktur-Services hängen zwar nicht mit der eigentlichen Übertragungsqualität des Netzwerks zusammen, sehr wohl aber mit der gesamten User-Experience der Clients, die das Netzwerk nutzen.

Erhalten Sie mit Mist Wired Assurance einen besseren Einblick

Die Wireless Lösungen von Mist Systems und der dazugehörigen KI hält sich u.a. an den Grundsatz „Up ist nicht das Gleiche wie gut“. Dies bedeutet das zur Verfügung stellen von vorhersehbaren, zuverlässigen und messbareren drahtlosen Netzen, sowie völlig neuen Nutzererfahrungen durch KI und ML, gelten natürlich auch in den drahtgebundenen Netzen. Die Juniper Wired Assurance nutzt die umfangreiche Junos-Switch-Telemetrie, um einfachere Vorgänge, eine kürzere Reparaturzeit und eine bessere Übersicht über die Endbenutzererfahrungen Ihrer verbundenen Geräte, einschließlich Zugriffspunkten, Servern und IoT-Endpunkten zu ermöglichen. So wird das beste Anwendererlebnis bei gleichzeitiger Simplifizierung der Betriebsabläufe für die verantwortlichen Netzwerk-Teams erzielt. Es bedarf also nicht eines noch größeren Computers, wie im Film „Per Anhalter durch die Galaxis“ zu bauen, sondern einfach nur die bestehenden Technologien zu nutzen und daraus die richtigen Schlüsse zu ziehen, eben das was KI in der IT macht.

2020, Karl-Heinz Lutz, Partner Consultant DACH bei Juniper Networks

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

www.ramgesoft.de

Sicherheit kann auch einfach sein - **Mit SolarWinds ARM**

Auf die Frage hin: „Wer hat in Ihrem Unternehmen die meisten Rechte?“ – Erhält man in der Regel die Antwort, „der Chef“ oder „der Administrator“.
In Wirklichkeit verhält es sich aber oft anders, es ist meist der/die Auszubildende. Ein Auszubildender durchläuft während seiner Ausbildung meist alle Abteilungen der Firma. Somit benötigt er/sie auch entsprechende Berechtigungen auf Shares etc.
Wir beobachten immer wieder, dass gerade diese Berechtigungen nicht mehr zurückgenommen werden und somit Mitarbeiter im Unternehmen existieren, die Zugriff auf fast alles haben.
Der Access Rights Manager von SolarWinds, ehemals 8man, hilft dem Administrator den Blindflug in seiner Active Directory ein Ende zu bereiten. ARM, ist die schnellste und effektivste Lösung gegen die „Quick & Dirty“ Administration, die sich über Jahre im Unternehmen etabliert hat.

Access Rights Manager

Verwalten und Prüfen von Zugriffsberichtigungen über die gesamte Infrastruktur hinweg

Hauptfunktionen

- Hochrisikozugriffe überblicken und Maßnahmen ergreifen
- Die Auswirkungen interner Bedrohungen minimieren
- Dank Änderungserkennung die Compliance verbessern
- Schnell ermitteln, wer worauf Zugriff hat
- Konten schnell und präzise bereitstellen
- Hochrisikokonten erkennen und überwachen

Compliance-Anforderungen, die durch DSGVO, PCI, HIPAA und andere Vorschriften gestellt werden, erfordern eine detaillierte Überwachung des Benutzerzugriffs, insbesondere für Benutzer, die Zugriff auf kritische und sensible Daten haben.
SolarWinds® Access Rights Manager (ARM) wurde entwickelt, um benutzerdefinierte Active Directory(AD)- und Azure AD-Berichte bereitzustellen, die zeigen, wer wann auf welche Daten zugegriffen hat.

Mehr Informationen:

RamgeSoft
Europaweite Software Distribution

solarwinds
AUTHORISED PARTNER

bitglass

ÜBER BITGLASS

- Bitglass ist ein technisch führender Anbieter eines Cloud Access Security Broker (CASB) mit Sitz im Silicon Valley.
- Die Cloud Sicherheitslösung des Unternehmens bietet unter anderem einen agentenlosen Zero-Day, Daten- und Bedrohungsschutz an jedem Ort, für jede App und jedes Endgerät.
- Geschützt werden sowohl SaaS-Anwendungen, IaaS-Plattformen sowie private Cloudanwendungen.
- Bitglass ist dafür konzipiert, Daten in Echtzeit über alle wichtigen Geschäftsanwendungen hinweg zu schützen.

bitglass

Microsoft Office (O365) & Security

Office 365 von Microsoft ist schnell eine der beliebtesten Cloud-Apps für Unternehmen geworden - die von tausenden Firmen bevorzugte Email- und Produktivitätssuite. Dennoch kann, trotz der Verwendung von Office 365, Sicherheit und Compliance nicht außer Acht gelassen werden. Selbst in einer vertrauten öffentlichen Cloud-Anwendung wie Office 365 obliegt der IT – nicht den Vertreibern der App – die Verantwortung, Geschäftsdaten zu schützen. Ihre Organisation benötigt eine End-To-End-Datenschutzlösung in Office 365 und über Ihr gesamtes öffentliches Cloud-Portfolio. Die Lösung ist ein sogenannter Cloud Access Security Broker (CASB).

Obwohl Microsoft viel tut, um eigene Anwendungen und Infrastruktur gegen Ein- und Angriffe zu schützen, sind geschäftliche Daten durch große Sicherheitslücken gefährdet. Traditionelle Sicherheitssysteme wie sichere Web Gateways, Firewalls und standortbasierte DLP-Lösungen (on-premise) sind machtlos, nachdem Daten über die Firewall hinaus auf öffentliche Cloud-Apps transportiert worden sind. Dazu kommt, dass die Datenschutzkapazitäten von Applikationen wie Office 365 limitiert und nur auf einzelne Apps beschränkt sind, dadurch für die geschäftliche Nutzung teilweise ungeeignet sind.

Bitglass ermöglicht Ihrer IT sensible Daten über die Firewall hinaus zu sichern. An der Schnittstelle zwischen Anwendungen und Endgeräten bietet die Bitglass CASB Lösung einen zentralen Punkt für die komplette Sichtbarkeit und den entsprechenden Datenschutz. Bitglass CASB ist auf alle Cloud-Apps anwendbar, inklusive SaaS-Apps wie z.B. Salesforce, Slack oder Office 365, IaaS-Plattformen wie Amazon Web Services und benutzerdefinierte Anwendungen, sowohl intern verwendete als auch in der Cloud.

All das in einer agentenlosen, leicht implementierbaren Architektur, die weltweit bereits Millionen von Anwendern Sicherheit und kontinuierlich durch künstliche Intelligenz neue Apps identifiziert. Nur Bitglass bietet umfassenden Echtzeitdatenschutz auf jedem Endgerät – sowohl für Office 365 als auch für die gesamte Cloud-Anwendungssuite Ihres Unternehmens. Ob Sie Daten vor dem Upload verschlüsseln, Datenverluste kontrollieren, Einblicke in auffällige Nutzeraktivitäten erhalten oder all diese Lösungen wollen, die marktführende Datenschutztechnologie von Bitglass bietet Ihnen die Kontrolle, die Sie brauchen.

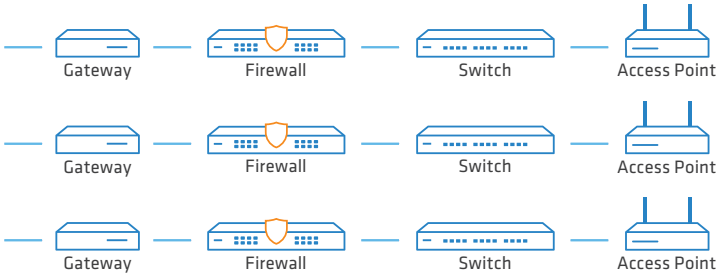
Überblick Architektur

Viele CASBLösungen verlassen sich zum Datenschutz allein auf API-basierte Scans, was zu riesigen Sicherheitslücken führt: API-Benachrichtigungssysteme brauchen teilweise mehrere Minuten zur Meldung eines Uploads oder Downloads von sensiblen Daten. So besteht die Möglichkeit einer Datenschutzverletzung. Nur ein hybrider CASB-Ansatz mit APIs und transparenten Proxys kann umfassenden Datenschutz garantieren. Über den Bitglass Reverse Proxy erhalten Sie von jedem Endgerät aus sicheren Zugang zu Ihren Daten ohne die Nutzung jeglicher Agenten oder Zertifikate. Der Reverse Proxy wurde mit der von Bitglass urheberrechtlich geschützten AJAX-VM-Technologie entwickelt und wurde konzipiert, um SaaS-Anwendungen als Proxy zu dienen. Er funktioniert ohne zusätzliche Software in jedem Webbrowser. Im Gegensatz zu traditionellen Proxys, die dynamische, clientseitige Funktionen brechen, schreibt die AJAX-VM Links in statische, servergelieferte Inhalte um und übersetzt diese automatisch in Code, der vom Browser umgesetzt wird. Die Proxys von Bitglass sind an die API-Integration von Office 365 gekoppelt.

Vertrauenswürdige Netzwerkinfrastruktur & IT-Security „Made in Germany“

Seit Mitte 2018 schaffen LANCOM und Rohde & Schwarz eine am Markt einzigartige Kombination aus vertrauenswürdiger Netzwerkinfrastruktur und IT-Security „Made in Germany“. Die neuen Next-Generation LANCOM R&S®Unified Firewalls ergänzen sichere und garantiert Backdoor-freie LANCOM Vernetzungen um state-of-the-art Sicherheitstechnologien und Unified Threat Management zu zukunftsfähigen Cybersecurity-Komplettlösungen: Gesicherte Netze und gesicherte Daten aus einer Hand!

SecurITy made in Germany

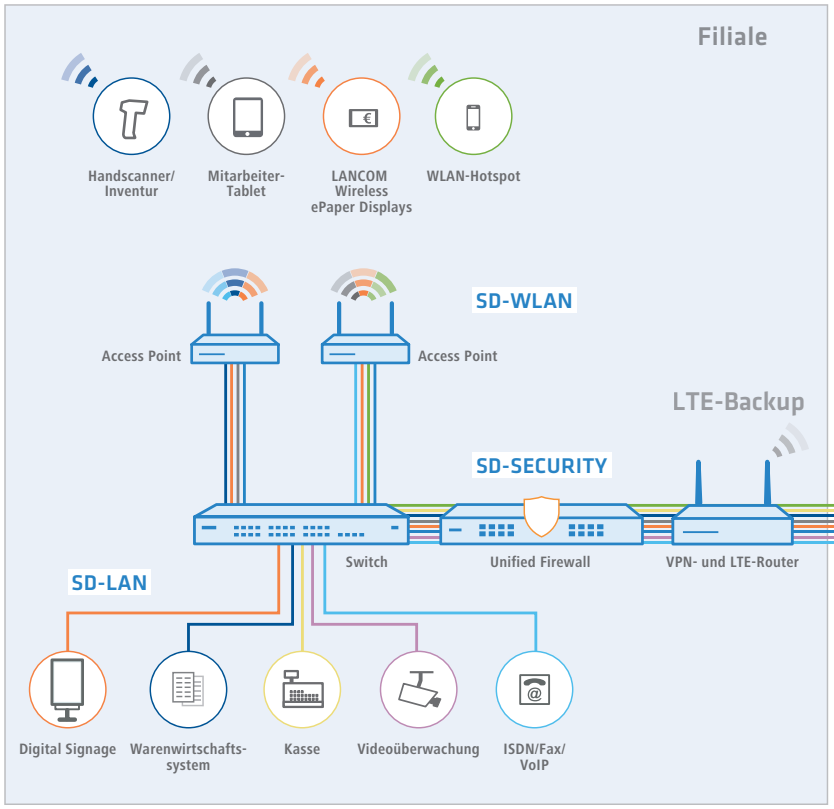


Durch die Integration der Unified Firewalls in die LANCOM Management Cloud in Form von Software-defined Security wird die gesamte Infrastruktur bestehend aus Konnektivität und Sicherheit über alle LANCOM Produkte hinweg zentral orchestriert.

HYPER INTEGRATION NETZWERK & IT-SECURITY

Beispiel Software Defined Branch

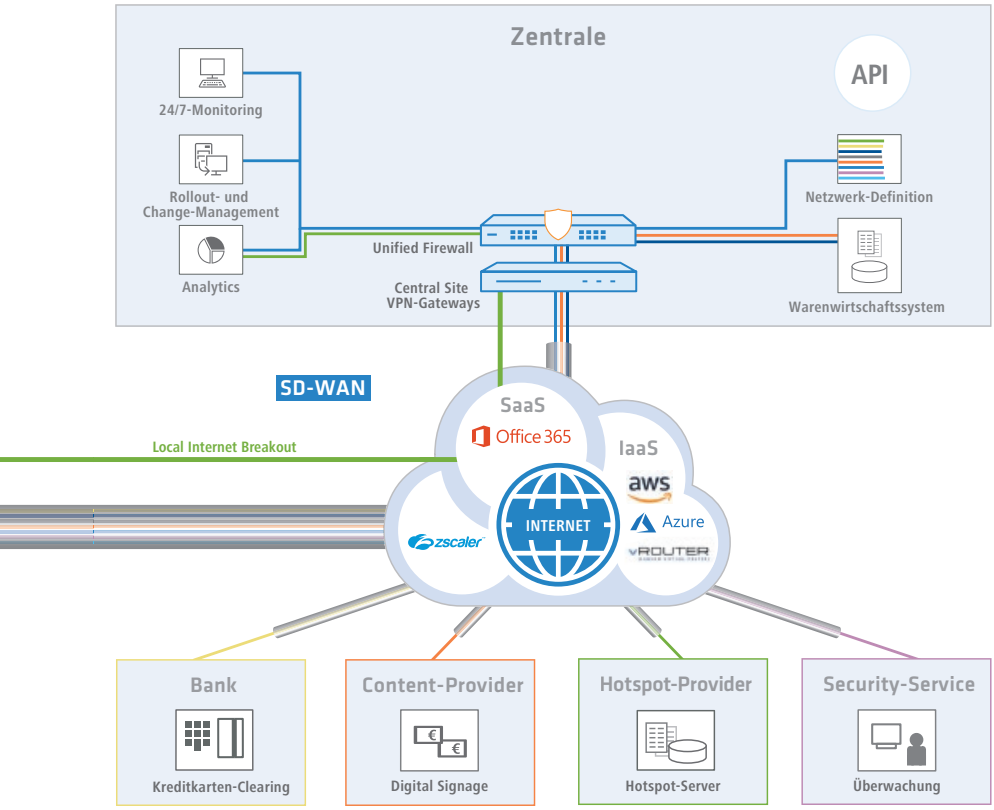
Netzwerk & Security Premium Portfolio – Hard- und Software



ZENTRALES NETZWERKMANAGEMENT MIT DER LANCOM MANANGEMENT CLOUD

Die LANCOM Management Cloud ist das weltweit erste hyper-integrierte Management-System, das Ihre gesamte Netzwerkarchitektur in den Bereichen WAN, LAN, WLAN und Security intelligent organisiert, optimiert und steuert. Mittels hochmoderner „Software-defined"-Technologie (SD-WAN, SD-LAN, SD-WLAN, SD-Security) wird die Bereitstellung eines integrierten Netzwerks drastisch vereinfacht, sodass die manuelle Einzelgerätekonfiguration entfällt. Das System stellt sich dynamisch auf Ihre Anforderungen ein, ist zukunftsorientiert und maximal sicher.

- Maximale Agilität und Flexibilität
- State-of-the-art Sicherheit
- Radikale Zeit- und Kostenerparnis
- Hochautomatisierte Multi-Service-Netzwerke in Top-Qualität



Durch die stetig zunehmenden Anforderungen im Zuge der Digitalisierung, braucht es moderne und skalierbare Netzwerkarchitekturen. Informieren Sie sich über die Vorteile und Möglichkeiten der LANCOM Komplettlösungen, auf Basis neuester Technologie. Sprechen Sie mit Ihrem LANCOM Partner über individuelle und bedarfsgerechte Konzepte, damit Sie sich auf Ihr Kerngeschäft konzentrieren können und Ihr Netzwerk sicher und zuverlässig funktioniert.

LANCOM Systems

LOGINVSI

ÜBER LOGIN VSI

- Login VSI testet und validiert automatisch die Auswirkungen von Änderungen auf physische, virtuelle und Cloud-basierte Arbeitsumgebungen, um ein hervorragendes Benutzererlebnis zu ermöglichen.
- Sicherung der Anwendungs- und Desktop-Performance. Senkung der Kosten und Steigerung der Effizienz. Vermeidung einer Beeinträchtigung der Systemleistung und von Ausfallzeiten.
- Login VSI ist völlig anbieterunabhängig und wird in VMware Horizon, Citrix Virtual Apps and Desktops, Microsoft Remote Desktop Services (RDS) und Microsoft Windows Virtual Desktop (WVD) eingesetzt

Die Lösung für ein perfektes Benutzererlebnis

Ein hervorragendes Benutzererlebnis ist ein wichtiger Erfolgsfaktor für alle SBC-, VDI- und DaaS Implementierungen. Login VSI ist der Marktführer im Bereich synthetisches Testen und bietet eine vollständige Softwarelösung für die Maximierung und Sicherung der Leistungsfähigkeit, Skalierbarkeit und Verfügbarkeit von Anwendungen und virtuellen Desktop Umgebungen (einschließlich Cloud). Login Enterprise ist völlig anbieterunabhängig und wird in VMware Horizon, Citrix Virtual Apps and Desktops, Microsoft Remote Desktop Services (RDS) und Microsoft Windows Virtual Desktop (WVD) eingesetzt.

Kontinuierliche Performance trotz Veränderungen

Seit einigen Jahren sind IT-Umgebungen immer stärker von Veränderungen betroffen. Diese verursachen den Großteil aller IT-Probleme. Dazu zählen sowohl geplante Login Enterprise Veränderungen – z. B. neue Versionen von Geschäftsanwendungen – als auch ungeplante Veränderungen, darunter solche, die von dem Active-Directory-Team vorgenommen werden, ohne dass Sie sich dessen bewusst sind. Darüber hinaus kann die Nutzung bei hoher Speicherauslastung und einer starken Beanspruchung sonstiger Geräte eine allmähliche Verschlechterung der Desktop und Anwendungsperformance nach sich ziehen. Login Enterprise ist derzeit die einzige Komplettlösung auf dem Markt, die Unternehmen dabei unterstützt, potenzielle Performance-Probleme infolge von Veränderungen jeglicher Art zu vermeiden.

LOGIN ENTERPRISE ERMÖGLICHT:

Leistungs-/Verfügbarkeitstests

Login Enterprise testet fortwährend die Verfügbarkeit und Leistungsfähigkeit der Infrastruktur sowie von virtuellen Desktops (einschließlich Cloud) und Anwendungen an einem oder mehreren Standorten. Die Lösung warnt nicht nur rechtzeitig vor einer Verschlechterung der Leistung oder Unterbrechungen der Verfügbarkeit, sondern gewährt auch Einblick in die Entwicklung der Performance. Dies ermöglicht es Ihnen, rechtzeitig geeignete Maßnahmen zur Aufrechterhaltung eines hervorragenden Benutzererlebnisses zu ergreifen.

Anwendungslasttests

Ein typischer digitaler Arbeitsplatz umfasst viele Anwendungen. Diese haben in jeder Desktop Infrastruktur einen großen Einfluss auf das Benutzererlebnis und die Produktivität. Veränderungen in den Anwendungen, der Desktop-Konfiguration oder der zugrunde liegenden Infrastruktur können erhebliche Auswirkungen auf die Leistungsfähigkeit haben. In der Praxis machen sich zahlreiche potenzielle Engpässe oder ein verändertes Verhaltens jedoch erst bei einer hohen Auslastung des Systems bemerkbar. Login Enterprise versetzt Unternehmen in die Lage, potenzielle Performance-Probleme schnell zu identifizieren, indem es die Ladezeiten und die Reaktionsfähigkeit von Anwendungen misst und vergleicht. Unsere synthetischen Benutzer melden sich auf einem Desktop an, starten die Anwendungen sowie interagieren mit diesen und messen deren Reaktionsfähigkeit. Die Produkte von Login VSI sind der Industriestandard hinsichtlich Benchmark- und Lasttests für Unternehmensanwendungen in den Rechenumgebungen von Endbenutzern. Unsere Lasttests decken geschäftskritische Anwendungen sowie Virtualisierungslösungen von Citrix, Microsoft und VMware ab. Login VSI wird eingesetzt, um Produktionsumgebungen möglichst kostensparend anzupassen und gleichzeitig die Desktop- und Anwendungsleistung zu maximieren.

Kompatibilitätstests

Login Enterprise testet automatisch die Kompatibilität von Anwendungen und der Updates ihrer Desktop Abbilder. Es „lernt“ von IT-Ingenieuren und Anwendungsbesitzern und genehmigt bzw. lehnt automatisch Anwendungen ab, deren Verhalten nicht den Erwartungen entspricht. Login Enterprise stellt leicht verständliche Berichte bereit, die Sie in die Lage versetzen, schnell zu entscheiden, ob Sie mit der Implementierung von Änderungen fortfahren wollen oder ob Sie eine bestimmte Anwendung eingehender prüfen möchten, um mögliche Probleme festzustellen.

Menschen, Orte und Räume verbinden

Ihre Mitarbeiter sind Ihr größtes Kapital, aber bietet ihr Arbeitsplatz auch die Voraussetzungen, damit sie ihr Bestes geben können?

In der modernen Welt ist die Kommunikation zwischen Menschen und Unternehmen unerlässlich. StarLeaf bietet eine flexible Plattform für einfache, zuverlässige und sichere Video-Kommunikation rund um den Globus für eine effiziente Arbeitsweise und eine hohe Produktivität und Zufriedenheit Ihrer Mitarbeiter – egal ob sie von zu Hause, vom Büro oder von anderen Orten aus arbeiten.

Weitere Informationen und Kontakt unter
www.StarLeaf.com/de
hello@starleaf.com

Digitale Meetings für Unternehmen – Sicherheit und Zuverlässigkeit im Mittelpunkt

Das Coronavirus hat nicht nur unsere heutige Arbeitsweise verändert, sondern wird weitaus größere und langfristige Auswirkungen haben. Es geht um die Zukunft der Unternehmen, was sie während der Pandemie gelernt haben und wie es von Vorteil sein kann, die Dinge für die Zukunft anzupassen. Viele Unternehmen haben bereits begonnen, ihre vorherigen Arbeitspraktiken in Frage zu stellen. Die Welt hat noch nie so viele Videokonferenzen durchgeführt und das wird voraussichtlich so bleiben. Der Anspruch und das Selbstverständnis der Menschen zur Zusammenarbeit per Video hat sich verändert und viele wollen auch zukünftig nicht darauf verzichten, egal ob sie irgendwann ins Büro zurückkehren, weiterhin von zu Hause arbeiten oder ihren Arbeitsort flexibel wählen wollen. Dazu kommen die politisch geführten Diskussionen zum Anspruch von Mitarbeitern auf Homeoffice. Bereiten Sie ihr Unternehmen darauf vor. Organisationen, die für die Zusammenarbeit auf Videokommunikation angewiesen sind, sollten einen Videokonferenzdienst nutzen, der Sicherheit und Zuverlässigkeit garantiert.

Was heißt das konkret?

Branchenweit führende Verschlüsselung, modernste Authentifizierung und sicheres Firewall-Traversal sind das Fundament einer sicheren und zuverlässigen Videokonferenzplattform. Darüber hinaus spielen aber weitere Faktoren eine entscheidende Rolle. So ist eine Sicherheitszertifizierung des Anbieters sowie eine DSGVO-konforme Datenverarbeitung ebenso wichtig wie die Frage, wo die Server stehen oder ob eine nach deutschen Gesetzen geltende Auftragsvereinbarung geschlossen werden kann. Durch unser eigenes globales Netzwerk bieten wir unseren Kunden die optimale Sicherheit, die sie für eine produktive und stets verfügbare Zusammenarbeit benötigen und sie vor Reputationsschäden bewahrt.

Wir bieten:

Sichere Plattform – StarLeaf hat seine eigene globale Plattform entwickelt, um erstklassige Videokonferenzen bereitstellen zu können

Service-Level-Vereinbarung – StarLeaf ist branchenweit einziger Anbieter mit 99,999%iger Verfügbarkeitsgarantie, die wir durch mehrere Präsenzpunkte und vollständige Plattformeigentümerschaft zusichern können

ISO/ICE 27001 Zertifizierung – Unsere robusten Sicherheitsmaßnahmen haben uns eine Zertifizierung nach ISO/ICE 27001 ermöglicht

Datenschutz – Daten werden gemäß den in Ihrer jeweiligen Rechtsordnung geltenden Datenschutzvorschriften verarbeitet

Datenzuständigkeit – Unsere Datenzuständigkeitsgarantie versichert unseren Kunden, dass ihre Daten unter ihrer Kontrolle und jeweiligen Hoheitsgebiet bleiben

Privacy Policy – Uns sind Privatsphäre, Sicherheit und Transparenz wichtig, die wir durch unsere Privacy Policy garantieren

Rechtliches – Wir haben alle unsere rechtlichen Dokumente zusammengetragen, die die Sicherheit und Zuverlässigkeit unseres Dienstes unterstützen.

StarLeaf

- StarLeaf bietet Lösungen, die sich den unterschiedlichen Ansprüchen anpassen, sei es für mobiles Arbeiten mit der StarLeaf App, das StarLeaf Huddle für professionelles Arbeiten von Zuhause oder kleine Meetingräume sowie Lösungen für mittlere bis große Konferenzräume.
- Unsere Lösung passen sich den vorhandenen Arbeitsabläufen an und lassen sich in bestehende Geschäftsanwendungen integrieren (Microsoft Outlook, Teams, Slack, Google Calendar usw.) Aufgrund der Interoperabilität können Unternehmen gute und sichere Verbindungen in Echtzeit mit allen standardbasierten Meeting-Systemen von Drittanbietern aufbauen können.

CMSC

Connecting Media Service Cockpit

Eine Welt im Wandel

Die Digitalisierung und Vernetzung durchdringen die Geschäftswelt immer tiefer. Ein weitreichender Prozess, der Firmen spannende Chancen und Perspektiven bietet, aber auch Schattenseiten hat: Je abhängiger ein Unternehmen von seiner IT-Infrastruktur wird, desto verheerender 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 Security-Standards der rasanten digitalen Entwicklung mit immer komplexer werden Systemen anzupassen.

Ohne ganzheitlichen Ansatz geht es nicht

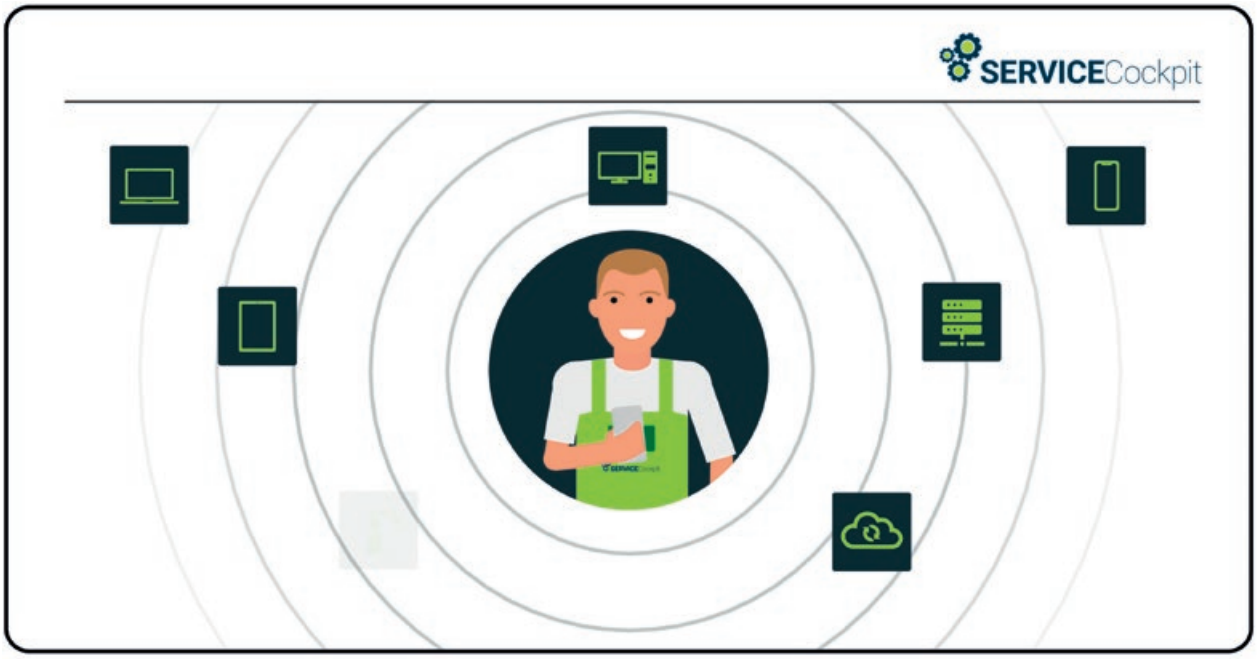
Wie lässt sich aber nun dieser Herausforderung Herr werden? Die Lösung bietet ein Information Security Management System (ISMS). Dieses definiert umfassende, maßgeschneiderte Verfahren und Regeln für ein ganzheitliches Sicherheitskonzept und eine Informationssicherheitsstrategie.

Connecting Media denkt weiter

Wer ein ISMS in seiner 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 Information Security Management System 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 Service Cockpit

An dieser Stelle kommt das Service Cockpit von Connecting Media ins Spiel. „Mit unserem ISMS der nächsten Generation hat der Nutzer alles ganz einfach im Blick“, bringt Geschäftsführer Andreas Kunz das neue Produkt auf den Punkt. Das Service Cockpit fasst dazu unzählige Datenquellen zusammen, bereitet sie nutzerfreundlich auf und vereint sie unter einer übersichtlichen Benutzeroberfläche. So werden Informationssicherheit und Gefahrenabwehr für Ihr Unternehmen zum Kinderspiel.



Das ISMS der nächsten Generation

Das bietet Ihnen das Service Cockpit 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 Ticketsystem. 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 klassische 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 Datenabfrage 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 Service Cockpit 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 Funktionsumfang ist durch Anbindung neuer Konnektoren jederzeit erweiterbar und stellt somit für sie ein zukunftssicheres Investment dar.

Ihr direkter Kontakt:

David Staab – Sales Manager
Tel. 07243 / 9397463
vertrieb@connectingmedia.de
https://servicecockpit.io/

UNTERNEHMENSPROFIL

- Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten in Deutschland gegründet.
- Die Appliances der Reihe Greenbone Security Manager (GSM), sowohl physisch als auch virtuell, und die Cloud-basierte Plattform (GMSP) analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können.
- Bestandteil der Lösungen ist ein tägliches, automatisiertes Security-Update.

Greenbone
Sustainable Resilience

Greenbone
Sustainable Resilience

Digitale Widerstandsfähigkeit in all ihren Formen

Betriebsunterbrechungen und Cyber-Angriffe sind für Unternehmen in Deutschland die beiden größten Geschäftsrisiken, und beide sind eng miteinander verzahnt. Unternehmen erbringen mit Waren und Dienstleistungen einen Mehrwert für Ihre Kunden und einen Wert für das eigene Unternehmen. Erzeugt werden diese durch Geschäftsprozesse und Produktionsabläufe, die nicht mehr ohne digitale Systeme und Vernetzung denkbar sind. Egal wie weit die Digitalisierung im Unternehmen schon ist, Ausfälle von digitalen Systemen (z.B. der eigenen Website, des Email-Systems oder der Warenwirtschaft) bedeuten einen nicht zu unterschätzenden Schaden. Schäden durch Ausfälle in der Produktion, durch Unterbrechungen der Zulieferkette, oder auch durch Image-Verlust bei einem Cyberangriff, es gibt viele Gründe warum Unternehmen widerstandsfähig gegen Cyber-Angriffe sein müssen. Damit Unternehmen ihre Fähigkeiten ausspielen und sich auf die eigenen Kompetenzen fokussieren können, sorgt das breite Produktportfolio angefangen bei physischen Appliances, über virtuelle bis hin zur Cloud-basierten Lösungen, für widerstandsfähige IT-Infrastrukturen, frei von Schwachstellen in Anwendungen und Systemen der IT und der OT.

Eine andere Perspektive einnehmen

Das Schwachstellen-Management ist ein wichtiger Baustein, um IT-Netzwerke gegen die wachsenden Cyberbedrohungen widerstandsfähig zu machen. Unternehmen können damit Sicherheitslücken aufdecken, priorisieren und Schutzmaßnahmen anstoßen.

Außerdem erkennt das System unsichere Einstellungen in Programmen und Abweichungen von Policies- beziehungsweise Compliance-Richtlinien. Gleichzeitig arbeitet es Hand in Hand mit anderen Sicherheitssystemen wie Firewalls und Intrusion Detection (IDS)- oder Prevention- Systemen (IPS) zusammen. Bausteine der Greenbone Technologie sind das Betriebssystem Greenbone OS und der Greenbone Security Feed, mit derzeit über 79.700 Schwachstellen-Tests, wobei diese Zahl mit täglicher automatischer Aktualisierung ständig wächst. Alle Produkte unterstützen grundsätzlich eine unbegrenzte Anzahl von Zielsystemen. Die tatsächliche erreichbare Zahl hängt von Unternehmens- und Aufgabengröße ab. Das passende Modell können Unternehmen anhand der Anzahl ihrer Target IP-Adressen auswählen. Daten verlassen bei den physischen wie auch virtuellen Appliances dabei zu keinem Zeitpunkt das Unternehmensnetzwerk, sondern werden ausschließlich lokal gespeichert.

Hochwertiges Resilience-Management als Managed Service

Die neue Greenbone Managed Service Plattform (GMSP) bietet eine Lösung, mit der Schwachstellen in der eigenen Netzwerkinfrastruktur ohne Installation von virtuellen oder physischen Appliances innerhalb von wenigen Schritten aufgespürt und Anweisungen zu deren Behebung in Form von Berichten aufgezeigt werden.

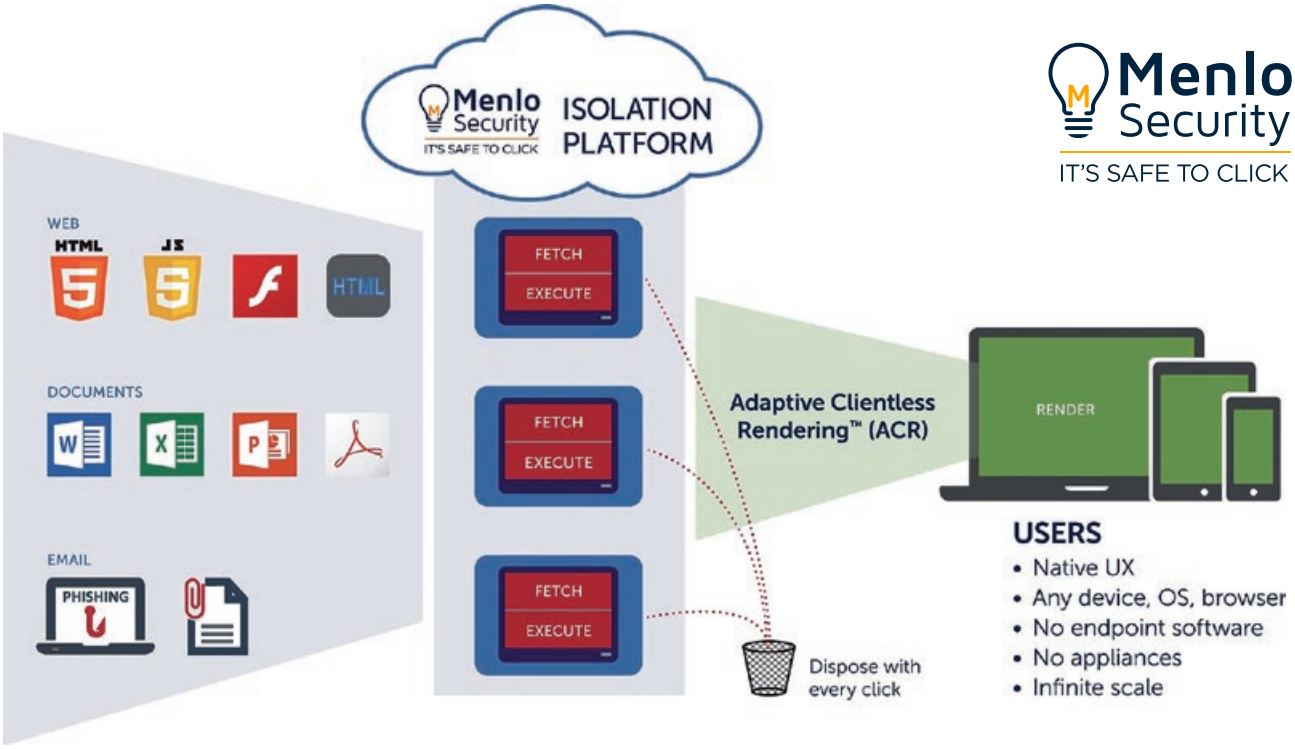
Dazu bietet sie vordefinierte Pakete für Unternehmen unterschiedlicher Größen an. Kleinst-Unternehmen mit hohem Sicherheitsbedarf können diese Plattform genauso im Self-Service benutzen wie große Mittelständler oder Städte und Gemeinden. Dabei können sowohl die öffentlichen IP-Services (WWW-Server, E-Mail-Server, usw.) als auch interne Netze überprüft werden. Die Pakete sind als Abos strukturiert und können monatlich gekündigt oder je nach Bedarf verändert werden. Interessenten können zu Beginn einen 14-tägigen Test buchen und die Plattform ausgiebig inspizieren.

GEFAHRLOSES SURFEN UND MAILEN DURCH ISOLATION

Der wachsenden Bedrohungen aus dem Cyberspace Herr zu werden, wird immer schwieriger. Besonders wenn wie in heutigen Zeiten die Mitarbeitenden vermehrt von Remote-Arbeitsplätzen aus arbeiten und sich somit ausserhalb des Firmen-Netzwerkes aufhalten. Ein neuer technischer Ansatz sorgt dafür, dass Schadcode und Phishing-Angriffe den Anwender überhaupt nicht mehr erreichen: Browser-, Dokumenten- und E-Mail-Isolation über eine zentrale Plattform.

- Web- und E-Mail-Security-Lösung mit revolutionärer Isolation-Technologie
- 100% sicherer Zugriff auf jegliche Websites (Secure Browsing)
- Eliminiert Drive-by Infections, Zero-Day Malware und Ransomware
- Security für Cloud-Anwendungen
- Agentless: keine Software auf dem Client nötig
- Erhältlich als globaler Cloud-Service oder als virtuelle Appliance

BOLL
IT Security Distribution



Null Prozent Malware dank Isolation

Das Cybercrime-Problem nimmt rasant zu. Bisher unbekannte Bedrohungen und unbekannte Schwachstellen spielen dabei zunehmend die Hauptrolle. Die wichtigsten Angriffsvektoren sind Websites oder Office- und PDF-Dokumente mit eingebettetem Schadcode sowie Phishing-E-Mails. Konventionelle Lösungen zur Abwehr von Cyber-Attacken basieren oft auf der Erkennung bekannter Malware-Signaturen (Detection) und daraus abgeleiteter Merkmale. Bedrohungen, die mit neuen Mechanismen arbeiten, werden so nicht abgefangen. Eine andere Methode ist die Kontrolle aller eingehenden Inhalte durch Ausführung des potenziellen Schadcodes in einer geschützten Umgebung (Sandboxing) – ein rechen- und zeitaufwendiger Vorgang, der ebenfalls mit der Erkennung von Schadcode arbeitet.

Neuartiger Ansatz

Einen völlig neuartigen Weg geht Menlo Security. Das Ziel ist, dass Schadsoftware erst gar nicht zum Anwender gelangt. Dazu isoliert die «Isolation Platform» von Menlo die eingehenden Inhalte (Websites, Dokumente, E-Mail-Links und -Attachments) jeweils in einem Container (eine abgesicherte virtuelle Umgebung) und führt dort den allenfalls enthaltenen aktiven Code aus (JavaScript, Flash, Java). Handelt es sich um Malware, läuft sie innerhalb des Containers und kann keinen Schaden anrichten. Der Container wird unmittelbar danach entsorgt.

Der unschädliche Nutzinhalt wird auf Basis des «Document Object Models» (DOM) von HTML als gerenderte Information (Adaptive Clientless Rendering) ohne aktive Elemente an den Anwender übermittelt. So ist gewährleistet, dass der Client von jeglichem Schadcode isoliert ist. Die eigentliche Browser-Verarbeitung findet auf der Isolation Platform statt. Analoges gilt für E-Mails und Dokumente. Auf dem Endgerät muss dazu keine Software installiert werden. Der Anwender arbeitet wie gewohnt mit seinem Browser, der Office-Suite, dem PDF-Reader und dem E-Mail-Client.

IT-Sicherheit ohne Kompromisse

Die fehleranfällige Analyse, ob es sich um «gute» oder «böse» Inhalte handelt, entfällt. Die Lösung von Menlo Security kommt ganz ohne Detection aus. Dies hat den Vorteil, dass die zahllosen Security-Alerts, wie sie bei Detection-basierten Lösungen üblich sind, völlig wegfallen. Das Sicherheitsteam wird entlastet.
Auf Wunsch lässt sich die «Isolation Platform» von Menlo aber auch mit einem konventionellen Malware-Schutz kombinieren.

Menlo Security bietet zwei kombinierbare, aber auch einzeln nach Bedarf einzusetzende Dienste an: Web und Document Isolation Service sowie E-Mail-Link und Attachment Isolation Service. Zusätzlich kann die Menlo Next-Gen Proxy mit DLP oder CASB erweitert werden. Die Lösung ist als Cloud-Service oder als virtuelle Appliance für den Betrieb vor Ort erhältlich.

Boll Europe GmbH / Ringstrasse 3, DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com
Boll Engineering AG / Jurastrasse 58, CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
Boll Engineering SA / En Budron H15, CH-1052 Le Mont-sur-Lausanne / Telefon +41 51 533 01 60 / contact@boll.ch

ENGINSIGHT

IT-SICHERHEIT GANZ EINFACH

100 % validierte Analysen und ein **hoher Automatisierungsgrad** schaffen **volle Transparenz** zum Sicherheitszustand Ihres Unternehmens.

Dies ermöglicht es Ihnen,
mit **wenigen IT-Mitarbeitern** die **volle Kontrolle** über eine **immer komplexer werdende IT-Infrastruktur** zu behalten.

SecurITy made in Germany

100% selbst entwickelt, MADE IN GERMANY

Perfekt für KMU!

Ganz ohne Konfiguration oder langwierige Einarbeitung, direkt mit allen Security Analysen starten.

Kundenauswahl, starke Partner und Pressestimmen

Leipziger Verkehrsbetriebe · HDI · HanseYachts · JENOPTIK

Forbes · Allianz für Cyber-Sicherheit · BVMW · Security Insider

„One of the 30 Top AI-Startups of the DACH Region"

„Swiss Army Knives for IT Security"

Ihr persönlicher Ansprechpartner

Mario Jandeck (CEO)
mario.jandeck@enginsight.com
03641 271 49 66

ENGINSIGHT.COM

ENGINSIGHT

IT-Sicherheit für den deutschen Mittelstand

Enginsight bietet Ihnen die effizienteste Lösung für die zunehmenden Herausforderungen der IT-Sicherheit im deutschen Mittelstand. Die 100% eigenentwickelte Software ermöglicht es Unternehmen, innerhalb weniger Minuten ihre gesamte IT automatisiert zu überwachen und sicherheitstechnisch zu analysieren. Informationen über Sicherheitslücken oder Konfigurationsmängel werden ebenso aufgezeigt, wie gerade live stattfindende Cyberangriffe. Mit simulierten Hackerangriffen können Sie außerdem Ihren Blickwinkel ändern, um die gesamte IT einem Härtetest zu unterziehen.

Dies ermöglicht es Ihnen, mit wenigen IT-Mitarbeitern die volle Kontrolle über eine immer komplexer werdende IT-Infrastruktur zu behalten. In Kombination aus u.a. Schwachstellen-Scanning, Penetration-Testing oder Patchmanagement sowie Netzwerk- und Systemeventlog-Analysen erhalten Sie das Wesentliche aus den Welten IT-Security, Monitoring und IT-Management in EINER (Made in Germany) Lösung. Die praxisnahen Analyseergebnisse und konkreten Handlungsempfehlungen unterstützen Sie, proaktiv tätig zu werden, bevor es zum Schadensfall durch Cyberkriminelle kommt. Ein Ausfall der IT, der Produktion oder der Abfluss sensibler Daten kann so frühzeitig verhindert werden.

Der Ansatz von Enginsight konzentriert sich auf die Bedürfnisse des Mittelstandes. Bisher setzen mittelständische oder kleine Unternehmen auf mehrere Spezialtools. Das ist aufgrund der mehrfachen Lizenzgebühren nicht nur teuer, sondern auch ineffizient, weil die Software untereinander nicht ausreichend kommuniziert und der Überblick verloren geht. Deshalb begreift sich Enginsight nicht als weiteres Spezialtool, um das vermeintlich letzte Perzentil mehr Sicherheit zu erreichen, sondern möchte das Fundament einer umsichtigen IT-Sicherheits-Strategie legen. Die Zunahme von vernetzten Geräten und die steigende Komplexität bei gleichzeitigem Personalmangel verlangt nach Automatismen und autonom agierenden Lösungen. Deshalb bietet Enginsight eine Vielzahl an Automatisierungsmöglichkeiten, die sich nach individuellen Bedürfnissen einrichten lassen. Um vollkommen autonom Anomalien aufzuspüren, kommen intelligente Algorithmen und machine learning zum Einsatz.

Im Sommer 2017 in Jena als Startup mit überschaubarem Team und großer Vision gestartet, befindet sich Enginsight inzwischen bei namhaften Unternehmen und Partnern im Einsatz. Es begeistert die Anwender durch die intuitive Bedienung, das durchdachte Featureset, die tiefgreifenden Analysen und vor allem die schnelle und einfache Einsatzbereitschaft.

ÜBER ENGINSIGHT GMBH

Nach einigen Jahren Berufserfahrung als IT-Verantwortliche in größeren Unternehmen gründeten Eric Range und Mario Jandeck Enginsight im Jahr 2017. Kurz nach der Gründung folgten erste Auszeichnungen, wie der Thüringer Gründerpreis, den KfW-Award und die begehrte IT-Security Förderung des Bundes. Nach nur zwei Jahren wurde aus der Idee eine innovative und leistungsstarke Software. Enginsight macht IT-Security einfach und sorgt bei immer mehr Unternehmen für Sicherheit „Made in Germany".

www.enginsight.com ENGINSIGHT

intervalid

ÜBER INTERVALID GMBH

- Mit Intervalid DSMS und Intervalid ISMS haben wir uns auf die Umsetzung der EU Datenschutz-Grundverordnung sowie den Schutz unternehmensweiter Daten spezialisiert.
- Wir unterstützen nachhaltig unsere Kunden jeder Unternehmensgröße bei der Etablierung ihres Datenschutz- sowie Informationssicherheitsmanagement-Systems.
- Weitere Informationen unter www.intervalid.com

Minimieren Sie Ihr Sicherheitsrisiko mit Intervalid ISMS

Der schnelle technologische Fortschritt verändert unsere Geschäftswelt. Das bietet neben vielen Chancen auch Informationssicherheitsrisiken, die beispielsweise durch Hackerangriffe, Datenmissbrauch, technische oder menschliche Fehler verursacht werden und die es für Unternehmen zu bewältigen gilt. Laut der TÜV Cybersecurity–Studie 2019 haben 29% der Unternehmen in Deutschland einen Sicherheitsvorfall gemeldet. Die Kosten für diese Schäden belaufen sich weltweit auf ca. 520 Mio EUR pro Jahr (Schätzung des center of strategic and international studies). „Der Schutz von unternehmensweiten Informationen ist für Organisationen essenziel und wird auch zukünftig an Bedeutung gewinnen, um eine hohe Geldstrafe oder einen Reputationsschaden zu vermeiden" so Benigna Prochaska, Gründerin der Intervalid GmbH. Der Einsatz eines strukturierten Informationssicherheitsmanagement-Systems (kurz ISMS) schafft hierbei Abhilfe. Es umfasst standardisierte Verfahren, Richtlinien und vorgegebene Maßnahmen für Ihre Organisation, um die Unternehmenswerte zu schützen und Risiken zu minimieren. Mit Intervalid ISMS erhalten Sie eine sichere „all-in-one-Lösung", um das komplexe Thema Informationssicherheit erfolgreich in Ihrem Unternehmen umzusetzen und den Anwender effizient zu unterstützen. So sparen Sie Zeit, Personalressourcen und Kosten.

ES UNTERSTÜTZT SIE BEI:

– der Definition von Informationswerten
… legen Sie den Anwendungsbereich und die Grenzen Ihres ISMS fest, binden Sie Verantwortliche aktiv ein und nutzen Sie Formulare zur Erhebung der IST-Situation.

– der Erfassung von Informationswerten
… befüllen Sie das strukturierte Asset Register mit Ihren Informationswerten, profitieren Sie von Mustervorlagen und wählen Sie technische und organisatorische Maßnahmen.

– der Erkennung von unternehmensweiten Risiken
… bestimmen Sie den Schutzbedarf Ihrer Geschäftsprozesse anhand von Schutzbedarfsklassen, führen Sie eine Risikoanalyse bei gefährdeten Prozessen durch und stellen Sie so Ihren weiteren Handlungsbedarf fest.

– der Informationsvermittlung an Entscheider
… leiten Sie nach Priorisierung und Kosteneinschätzung, die vorgeschlagenen Maßnahmen an die Geschäftsleitung zur Freigabe weiter.

– die Umsetzung von Maßnahmen zur Risikobehebung
… leiten Sie genehmigten Maßnahmen zur Risikobehebung ein und überprüfen Sie laufend die Effektivität.

– der Prozesskommunikation mit allen verantwortlichen Mitarbeitern
… verteilen Sie Aufgaben an die Verantwortlichen inkl. Deadline zur Umsetzung der Maßnahmen und behalten Sie den aktuellen Status im Blick.

– der laufenden Kontrolle und Verbesserung
… nutzen Sie die Überwachungsmaßnahmen des Systems für eine internen Audit. Durchlaufen Sie regelmäßig Ihre Geschäftsprozesse, führen Sie Verbesserungen ein, erkennen Sie neue Risiken und minimieren Sie so kontinuierlich Ihr Geschäftsrisiko.

Ziehen Sie Ihren Vorteil aus den vielfältigen Mustervorlagen des Systems, damit sie nicht bei null anfangen und die Anforderungen von Beginn an korrekt erfüllen. Automatisierte Reports stellen alle Daten transparent zur Verfügung. Zusätzlich sind Sie mit Intervalid ISMS auf einen Audit zu einer ISO 27001 Zertifizierung vorbereitet. Dadurch steigern Sie Ihr Image und verbessern ihre Wettbewerbsfähigkeit. Intervalid ISMS wurde als SaaS (Software as a service) entwickelt und ist in einem nach ISO 27001 Rechenzentrum installiert. Auf Wunsch ist die Software auch als On-Premise-Version erhältlich.

> 20 Security Best Practices

> Basierend auf bekannten und aktuellen Angriffs-Mustern und -Methoden

> Priorisiert je nach Anforderungen und Dringlichkeit

> Basierend auf den CIS Critical Security Controls / SANS Top 20

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

SIND SIE SICHER?

Company Security – auch „as a Service" by Makro Factory

In den letzten Jahren ist ein deutlicher Anstieg an Cyber-Attacken zu beobachten. Doch nicht nur die pure Masse macht IT-Sicherheitsabteilungen zu schaffen, sondern die zunehmende Varianz in der Art der Angriffe stellt für Unternehmen eine besondere Herausforderung dar. Wir von der Makro Factory sehen die IT-Security in Unternehmen daher als eine Art Mosaik, die nur in ihrer Gesamtheit ein sinnvolles Bild ergibt. Unser Konzept umfasst unter anderem folgende Aspekte:

2-Faktor-Authentifizierung
Ein 6-stelliges Passwort kann mit neuartigen Angriffsmethoden in nur 7 Sekunden geknackt werden. Wieso setzen so wenige Unternehmen dann auf eine 2-Faktor-Authentifizierung? Mit modernen, wireless Lösungen kann die Sicherheit um ein Vielfaches gesteigert werden – und das ohne Mehraufwand auf Seiten des Users.

Firewall as a Service
Eine aktuelle Firewall bildet die Basis im Sicherheitskonzept. Eine einmalige Einrichtung reicht jedoch nicht aus, um sich dauerhaft zu schützen. Für viele – insbesondere kleine und mittelständische – Unternehmen bedeutet die Pflege jedoch einen erheblichen finanziellen Aufwand. Eine Möglichkeit, Kosten bei der Firewall einzusparen, ohne, dass die Sicherheit darunter leidet, bietet das „Firewall as a Service" Konzept, bei dem sich ein IT-Dienstleister bspw. um Updates- und Patches kümmert.

E-Mail Security
Das Abwehren von Angriffen über E-Mails gehört zur Tagesordnung der IT-Security Abteilung. Immer wieder müssen dabei täuschend echte Phishing Mails identifiziert werden – mit manueller Klassifikation stößt man sofort an die Kapazitätsgrenzen. Dementsprechend wichtig sind automatisierte E-Mail Security Systeme, die bestenfalls auf einer künstlichen Intelligenz beruhen. Nur so kann die False-Positive Rate so gering wie möglich gehalten und sichergestellt werden, dass keine Informationen durch irrtümliches Blockieren verloren gehen.

Office 365
Mit abnehmender Skepsis vor Cloud Anwendungen steigt insbesondere der Einsatz von Office 356 Produkten, um die Flexibilität und Produktivität der Mitarbeiter zu steigern. Im Umkehrschluss steigt jedoch das Risiko von Datenpannen. Sensible Daten werden teilweise öffentlich geteilt oder auf privaten Geräten abgespeichert. Unternehmen müssen dementsprechend Cloud-Security Lösungen etablieren, mit denen sichere Zugriffe gewährleistet werden können.

DSGVO
Im Jahr 2019 wurden im Rahmen der DSGVO insgesamt 428.937.244,00 € Bußgelder ausgesprochen – Tendenz für 2020 steigend. Ein Sicherheitsrisiko stellen Mitarbeiter*innen dar, die aufgrund von fehlender Sensibilisierung oder Unwissenheit Daten weitergeben. Diese Gefahr lässt sich beispielsweise mit einem Rechtemanagement basierend auf einer Business Intelligence Lösung minimieren, in dem ersichtlich wird wer, wann, warum und auf welche Daten Zugriff hat.

Endpoint Security
Die Corona Pandemie hat uns gezeigt wie wichtig Home Office Arbeitsplätze sein können. Doch auch außerhalb solcher Krisen arbeiten immer mehr Angestellte von zu Hause. In der Regel sind Heimnetzwerke jedoch nicht so gut geschützt wie Firmennetze. Um die Vorteile von Heimarbeit vollumfänglich zu nutzen, nicht in der täglichen Arbeit eingeschränkt zu sein und trotzdem kein Sicherheitsrisiko darzustellen, müssen die Endgeräte der Mitarbeiter*innen entsprechend gesichert werden.

Für alle Risikoszenarien gibt es verschiedene Lösungsansätze, die wir gerne mit Ihnen erarbeiten und umsetzen. Je nach Anforderungen können Sie all unsere Dienstleistungen auch als flexibles „as a Service" Paket nutzen.

IHRE VORTEILE

- IST-Analyse Ihrer bestehenden Security Infrastruktur
- Erstellung eines individuellen Sicherheitskonzepts
- 20 High Level Security Controls nach Reifegrad der Security beim Kunden
- Konkreter Maßnahmenkatalog abhängig von Größe und Risiko-Faktoren

deepinstinct
BEFORE YOU KNOW IT

ÜBER DEEP INSTINCT

- Deep Instinct bringt die Cybersicherheit auf einen neuen Level, indem es sich die Stärke des Deep Learning zunutze macht, um Bedrohungen umgehend verhindern zu können.
- Die On-Device-Lösung von Deep Instinct schützt vor Zero-Day-, APT- und Ransomware-Attacken sowie vor bekannter und unbekannter Malware - mit bislang unübertroffener Genauigkeit und Geschwindigkeit.
- Deep Instinct ist in der Lage sich mit einer sehr breiten Palette an potentiellen Sicherheitsbedrohungen auseinanderzusetzen, da es als erstes Unternehmen ein dediziertes Deep-Learning-Framework als Grundlage für seine Lösung verwendet. Der auf „tiefgehendem Lernen" basierende Agent kann nicht nur bekannte Malware, sondern auch anspruchsvolle noch unbekannte Malware wie APTs und Zero-Day-Bedrohungen erfolgreich erkennen und verhindern. Darüber hinaus ist er in der Lage zuverlässig das gesamte Spektrum dateibasierter Viren wie ausführbare PE-Dateien, Office, Makros usw. sowie dateifreie Viren wie Skripte und Power Shells abzuwehren.

Wir verhindern was andere nicht finden

Welche Lösungen haben wir im Portfolio?

Mit dem Ziel, Cyber-Bedrohungen für das Unternehmen auszumerzen, bietet Deep Instinct Schutz für Endpunkte, Netzwerke, Server und mobile Geräte. Die mit Betriebssystemressourcen äußerst sparsam umgehende Lösung steht für die meisten Betriebssysteme (Windows, Chrome, Mac, Android und iOS) und in verschiedenen Umgebungen (Air-Gapped NW, bereitgestellt in einer Multi-Tenancy für MSSPs oder VDI) bereit und ist auch unabhängig von der Netzwerk- oder Internetverbindung voll funktionsfähig und kann vor Ort oder über ein Cloud-Natives Design zur Verfügung gestellt werden. Die Implementierungs- und Wartungskosten dieses Leightweigth-Agenten sind minimal. Da das Produkt eine All-in-One-Schutzlösung für Sicherheitstransparenz und -remedation bietet, entfällt die Notwendigkeit, sich mit mehreren Anbietern, Lizenzen, Support oder Produkten befassen zu müssen. Alternativ kann die Lösung zusätzlich zu anderen Cybersicherheitslösungen eingesetzt werden. Diese einfache Handhabung erleichtert es jedem Unternehmen, eine vollständige Kontrolle über alle Endpunkte zu haben, während der eigentliche Betrieb der Lösung keine erkennbaren Verzögerungen oder Geschäftsinterferenzen verursacht.

Das hebt uns von der Masse ab

Deep Instinct ist das erste und einzige Unternehmen, das End-to-End Deep Learning für die Cybersicherheit anwendet. Im Gegensatz zu detektions- und reaktionsbasierten Lösungen, die erst auf den Angriff warten, bevor sie reagieren, arbeitet die Lösung von Deep Instinct präventiv. Durch einen präventiven Ansatz werden Dateien und Vektoren vor der Ausführung automatisch analysiert, so dass Kunden umgehend geschützt sind. Dies ist bei der derzeitigen Bedrohungslage, in der Echtzeit meist zu spät ist, von entscheidender Bedeutung.

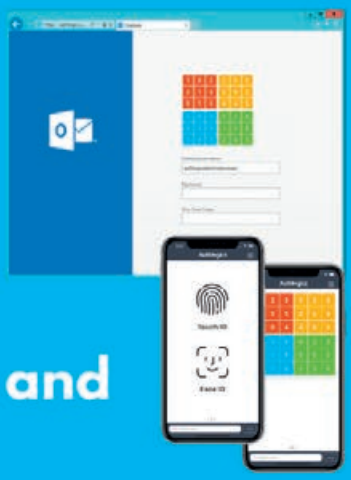
Deep-Learning ist die am weitesten entwickelte Untergruppe der künstlichen Intelligenz (KI), die sich von der Arbeitsweise des menschlichen Gehirn inspirieren lässt und lernt, mit bislang unübertroffener Genauigkeit Vorhersagen zu treffen und zu erkennen. Im Gegensatz zum maschinellen Lernen erfordert sie kein Feature-Engineering durch einen Menschen und kann auf Hunderte von Millionen von Trainingsproben skaliert werden. Das bedeutet, dass sie sowohl bekannte als auch neue Malware mit größerer Genauigkeit und Geschwindigkeit erkennen und verhindern kann. In noch nicht einmal fünf Jahren ist es Deep Instinct gelungen auf über 150 Mitarbeiter an fünf globalen Standorten anzuwachsen. In dieser Zeit wurde Deep Instinct unter anderem mit zahlreichen Preisen ausgezeichnet:

- 2016 Cool Vendor von Gartner
- Artificial Intelligence and Machine Learning vom Cyber Defense Magazine
- Most Disruptive Start-Up von Nvidia
- The Best Cybersecurity Start-Up 2017 von Cybersecurity Excellence Award
- Top 25 Cybersecurity Companies 2019 von the Software Report
- Best Use of AI in Security and Cyber Crime Protection von Global Annual Achievements Award

Deep Instinct schützt nachweislich mit unübertroffener Genauigkeit vor bekannten und unbekannten Malware-Angriffen und hat bei den von SE Labs durchgeführten Tests eine Erkennungsrate von 100 % mit null falsch-positiven Ergebnissen erzielt.

Authlogics...

Improve the security and reduce the complexity of passwords.



Help ensure regulatory compliance and mitigate risk.

Remove and reduce the reliance of passwords.

Improve customer experience with a simple, memorable and secure login.

"Authlogics provide end to end protection, with the end goal being a passwordless solution that prevents account takeover and compromised credentials."

Steven Hope, CEO

ÜBER AUTHLOGICS

- Authlogics bietet Unternehmen des öffentlichen und privaten Sektors eine einzigartige und kos. tengünstige Alternative zu traditionellen Authentifizierungsmethoden.
- Unsere Lösungen umfassen Passwortsicherheitsverwaltung und Multi-Faktor-Authentifizierungstechnologien, die es Unternehmen ermöglichen, eine einfache, sichere und NIST-konforme Passwortrichtlinie für ihre Benutzer zu verwenden und den Anmeldevorgang mit unserer patentierten MFA abzusichern. Diese Technologien können ihnen auch beim Übergang zu einem komplett passwortlosen Authentifizierungsprozess helfen.

Authlogics

https://authlogics.com

Authlogics

Weniger ist Mehr –

Kein Passwort, kein Problem

Passwörter sind dafür bekannt, ein schwacher Berechtigungsnachweis zu sein, wie nahezu tägliche Security-News zeigen. Das Dark Web ist übersät mit Dumps von Passwort-Breaches, die aus Datenbanken gestohlen oder bei Phishing-Angriffen geangelt wurden. Einmal gestohlen, können diese Zugangsdaten für den Zugriff auf Unternehmens- oder private Daten mittels Credential-Stuffing verwendet werden, was sehr schwer zu erkennen sein kann. Veraltete „komplexe" Passwort-Richtlinien schützen nicht vor diesen realen Bedrohungen. Heutzutage möchten Unternehmen ihre IT durch die Migration zu einem kennwortlosen Login UX und die Reduzierung der Abhängigkeit von Kennwörtern zusätzlich absichern. Bis jedoch ganz auf Passwörter verzichtet werden kann ist eine sichere und konforme Passwortlösung nach wie vor erforderlich.

Die Authlogics **Password Security Management (PSM) und Multi-Factor Authentication (MFA)** Suite bietet eine umfassende Sammlung an Werkzeugen, mit denen IT-Manager ihre Sicherheit im Allgemeinen verbessern und Unternehmen eine einfache, sichere und konforme Authentifizierungsmethode für ihre Benutzer zur Verfügung stellen können. Dies wird erreicht durch:

Passwort-Compliance

- Führen Sie Echtzeit-Prüfungen mit unserer Password-Breach Datenbank durch, die aus über 2 Milliarden Zugangsdaten besteht, um den Passwort-Sicherheitsstatus des Unternehmens zu bewerten und sicherzustellen, dass nur NIST-konforme Passwörter verwendet werden.

- Die automatische Korrekturfunktionalität stellt sicher, dass Benutzer gezwungen werden, ihre Passwörter zu ändern, sobald ein Passwort als kompromittiert erkannt wird, und gewährleistet so eine kontinuierliche Konformität. Berichte und Warnmeldungen werden automatisch erstellt, um die Sichtbarkeit für Administratoren zu gewährleisten.

Multi-Faktor-Authentifizierung

- Die MFA-Lösung umfasst 5 Technologien, darunter das patentierte PIN-Grid, PINpass, PINphrase, YubiKey und biometrische Faktoren.

- Bahnbrechende gerätelose OTP-Technologie.

- Vor-Ort- und Offline-Authentifizierung.

Kennwortlos

- Alternative Wissensfaktoren.

- Sichere Passwortablage für Active Directory-Passwort Reply Single Sign-On.

Die **Password Security Management** verhindert, dass gebrachte Passwörter in Ihre Organisation gelangen, und gewährleistet die fortlaufende Einhaltung von NIST SP 800-63B-Passwörtern durch Echtzeit- und zeitgesteuerte Überwachung und Abhilfemaßnahmen. PSM verhindert auch die gemeinsame Nutzung von Passwörtern und ermöglicht die Rücksetzung von Passwörtern durch Benutzer-Self-Service über ein Webportal.

Authlogics kann nicht nur sichere Passwörter implementieren, sondern sie auch entfernen, indem das Passwort als Wissensfaktor durch einen oder mehrere andere Faktoren ersetzt wird. Das Authlogics **Multi-Factor Authentication** bietet mehrere wissens- und gerätebasierte sowie biometrische Alternativen zu einem Kennwort in einer einzigen Lösung. Die Weiterentwicklung unserer Suiten orientiert sich selbstverständlich an aktuellen Einflüssen und wird in Kürze u.a. auch eine Unterstützung für FIDO bereitstellen.

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, Finanz, Retail, Fertigung oder Energie.

VARONIS

Datensicherheit in einer komplexen, hybriden Umgebung

Wir erleben gerade eine globale Verlagerung von rein lokaler Informationstechnologie zu hybriden IT-Umgebungen. Zahlreiche Unternehmen verschieben aufgrund der aktuellen Situation Teile Ihrer Infrastruktur für E-Mails und Dateien in die Cloud, wobei Office 365 eindeutig der Marktführer ist. Beim Einsatz von Office 365 in Kombination mit lokalen Datenspeichern treten neue Herausforderungen für die Datensicherheit und Daten-Governance auf, die angesichts weltweiter Datenschutzverletzungen und strenger Datenschutzbestimmungen dringend bewältigt werden müssen. Für Führungskräfte mit der Verantwortung für Sicherheit und Risikoabwehr bedeutet das, dass sie einheitliche und nachhaltige Datensicherheitskontrollen und bewährte Vorgehensweisen in ihren lokalen Datenspeichern und Cloud-Repositories implementieren sollten. Isolierte Datenschutz-Tools, die nur kleine Lücken stopfen, können teuer werden und neben gesteigerter Komplexität wachsen auch die Risiken. Varonis ersetzt bisher voneinander getrennte Sicherheitstools durch eine einzige Lösung und ermöglicht die Datensicherheitskontrollen zentral zu koordinieren und Richtlinien über eine Vielzahl von Datenspeichern hinweg einheitlich durchsetzen zu können – dies gilt sowohl im lokalen Netzwerk und in der Cloud. Anhand von sieben einzigartigen Funktionen verdeutlichen wir Ihnen wie die Datensicherheitsplattform von Varonis die integrierten Sicherheitsfunktionen von Office 365 optimiert.

1. Einheitliche Kontrolle über lokal gespeicherte Daten und Office 365-Daten

2. Vollständige Transparenz und Verwaltung von Berechtigungen

3. Erkennen sensibler Daten

4. Umfassende Audit- und Überwachungsprozesse mit dem Fokus auf Dateninhalte

5. Erweiterte Bedrohungserkennung (UEBA)

6. Automatisierung von Riskoabwehr und Begrenzung auf die minimalste Berechtigung

7. Verwaltung der Zugriffsberechtigung wird durch den Daten-Eigentümer geregelt.

Durch die Kombination leistungsfähiger Analysefunktionen mit Inhaltsanalysen und intelligentem Berechtigungsmanagement schützt Varonis mit einer Schnellerkennung, optimierten Zugriffskontrollen und datenbasierter Richtliniendurchsetzung vor Insider-Threats. Zusätzlich zum Schutz vor Insider-Threats schützt Varonis Unternehmen auch vor Malware, APTs und der Übernahme von Konten. Dabei kommt ein datenzentrierter Ansatz zum Einsatz, der sich auf einige der wertvollsten, umfangreichsten und anfälligsten Datenkonzentrationen konzentriert – die auf lokalen und in der Cloud gehosteten Datei- und E-Mail-Systeme.

Fazit: Die Datensicherheitsplattform von Varonis unterstützt Sie bei der Beantwortung der wichtigsten Sicherheitsfrage: **Sind meine Daten sicher?**

Erfahren Sie sowohl in unseren regelmässig stattfindenden Webinaren oder in einem indivduell durchgeführten Termin bei Ihnen vor Ort wie das Portfolio von Varonis Ihre Daten wirkungsvoll vor Verlust schützt.

Gerne demonstrieren wir Ihnen unsere Leistungsfähigkeit auch im Rahmen eines für sie absolut kostenlosen Data Risk Assessment. Hierbei unterstützt Sie ein Team von Spezialisten sowohl bei der Installation als auch der Analyse der Ergebnisse. Sie erhalten nach wenigen Tagen eine 360 Grad – Sicht auf Ihre Daten und können Ihr Risiko direkt bewerten und die ersten Massnahmen ableiten und relevante Daten (Bereiche) effektiv schützen.

IT SECURITY DISTRIBUTION
AT ITS BEST

Das 1988 gegründete IT-Unternehmen BOLL Engineering AG (BOLL) zählt zu den führenden Adressen im Channel-Business. **Der Value-Add-Distributor für IT-Security- und Open-Networking-Produkte** vertreibt wegweisende Lösungen in den Bereichen Netzwerk- und Mail-Security, Identity Control und Access Management sowie Server Load Balancing und Open Network. Dabei bietet BOLL seinen Channel-Partnern umfassende Dienstleistungen an, die weit über den üblichen Distributionssupport hinausgehen. Das kontinuierlich wachsende Unternehmen BOLL befindet sich in Privatbesitz und beschäftigt am Hauptsitz in Wettingen, in der Niederlassung Lausanne und am deutschen Geschäftssitz in Ulm (Boll Europe GmbH) gesamthaft rund 50 Personen.

Mehrwert für den Channel

BOLL vertreibt ein breites Portfolio führender IT-Security-Produkte sowie Lösungen im Bereich Open Networking. Dabei steht nicht primär die Distribution im Vordergrund, sondern das Schaffen von Mehrwert für den Channel. Die ausschliesslich von erfahrenen und kompetenten Mitarbeitenden erbrachten Pre- und Post-Sales-Services reichen von massgeschneiderten Marketing- und Sales-Services über Business-Development, Tech- und Logistik-Dienstleistungen bis hin zum hochkarätigen Schulungs- und Zertifizierungsangebot im eigenen «Premier Authorized Training Center» (ATC). Geradezu wegweisend ist dabei der ausschliesslich durch qualifizierte Ingenieure erbrachte, für die Channel-Partner kostenlose Tech-Support – dies im eigenen «best rated» Support-Center. Ob Consulting oder Seminare, Tech-Support oder Projektbegleitung, ob Marketingunterstützung oder Lead-Generation: **BOLL schafft nachhaltigen Kundennutzen.**

- Sales Services
- Business Development
- Marketing Services
- Logistics
- Tech Services
- Education

Boll Europe GmbH / Ringstrasse 3, DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com
Boll Engineering AG / Jurastrasse 58, CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
Boll Engineering SA / En Budron H15, CH-1052 Le Mont-sur-Lausanne / Telefon +41 51 533 01 60 / contact@boll.ch

BOLL
IT Security Distribution

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 15 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!

INNOVATIONSPREIS-IT BEST OF 2018 initiative mittelstand CONSULTING

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

SPENDEN AKTION*

Keine kalten Füße

Obhut, Hilfe und Bildungsmöglichkeiten – dafür steht das Sybelcentrum der Heimstiftung Karlsruhe.

Alle Kinder und Jugendlichen verdienen gute Startchancen in ihr Leben: Voraussetzung dafür ist eine Umgebung, in der sich junge Menschen wohl fühlen und entfalten können: die dringend notwendige Sanierung des Sybelcentrums und die Ausstattung mit moderner Infrastruktur sind wichtige Bausteine hierfür. „Keine kalten Füße“ startete vor über zwei Jahren als Projekt, das die Teilhabe von Kindern und Jugendlichen fördert und das Sanierungsvorhaben mit Spendenakquise unterstützt.

Mit Hilfe Ihrer Spende schaffen wir einen Ort für Kinder und Jugendliche, an dem sie mit warmen Füßen und klarem Kopf ins Leben starten können.

Weitere Informationen unter:
www.keine-kalten-fuesse.de

* 10% der Ticketeinnahmen der 2. SecurityCruise gehen zu Gunsten der lokalen Kampagne ‚Keine kalten Füße‘.

Keine kalten Füße

IMPRESSUM

Connecting Media
Andreas Kunz, CEO & Founder

Ettlinger Straße 31
76275 Ettlingen

Telefon +49 7243 6528-274
info@connectingmedia.de
www.connectingmedia.de

Auflage 1.000

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	connecting_media
	YOUTUBE	http://youtube.connectingmedia.de