AUSGABE 1

cm magazin

0101000011010101100101 1010101010101110

HÖCHSTE ZEIT FÜR HÖCHSTE SICHERHEIT

IT-SECURITY

IT-SERVICE

DATENSCHUTZ

www.connectingmedia.de

Wir sind in verschiedensten Formaten aktiv für Sie in der Branche unterwegs

WEBINARE

MESSEBESUCHE

EVENTS

WORKSHOPS

SPEAKER

NEWSLETTER!

Registrieren Sie sich bie unserem Newsletter und erfahren Sie über die neuesten Aktivitäten und Angebote von uns:

Connecting Media

www.connectingmedia.de/kontakt/#newsletter

Liebe Leserinnen, liebe Leser!

Die Digitalisierung verändert unseren Alltag in atemberaubender Geschwindigkeit – nicht nur im Privat-, sondern ebenso im Geschäftsleben. Gerade dort zeigen sich aber auch ihre Tücken: Der Schutz vor Cyber-Attacken, IT-Compliance oder eine korrekte DSGVO-Umsetzung sind nur einige der Themen, mit denen sich Unternehmen heutzutage konfrontiert sehen.

Fehler oder leichtsinniges Verhalten in diesen Bereichen können schnell sehr teuer oder gar existenzbedrohend werden. Eine fachkundige Beratung und Unterstützung durch kompetente IT- und Datenschutz-Dienstleister sind hier von zentraler Bedeutung.

Die SecurityCruise von Connecting Media bietet Ihnen genau das: Umfassendes Fachwissen von neun der größten IT-Security-Anbietern Deutschlands – gebündelt auf einem Event mit einzigartiger Atmosphäre!

An Bord der MS Karlsruhe hat der schon erwähnte hektische Alltag Pause. Hier haben Sie die Möglichkeit, sich ganz zwanglos rund um IT-Security und Datenschutz auszutauschen und unter anderem von Top-Speakern der Branche zu erfahren, wie Sie mit Ihrem Unternehmen auf diesen Gebieten in sicheres Fahrwasser gelangen.

Ich wünsche Ihnen informative und spannende Stunden an Bord – mit erhellenden Vorträgen und Diskussionen, inspirierenden Fachgesprächen und wertvollen neuen Kontakten.

Dieses Magazin soll Sie nicht nur durch den Tag führen, sondern Ihnen auch darüber hinaus ein Begleiter sein – als Nachschlagewerk, Informationsquelle oder einfach nur zur Erinnerung.

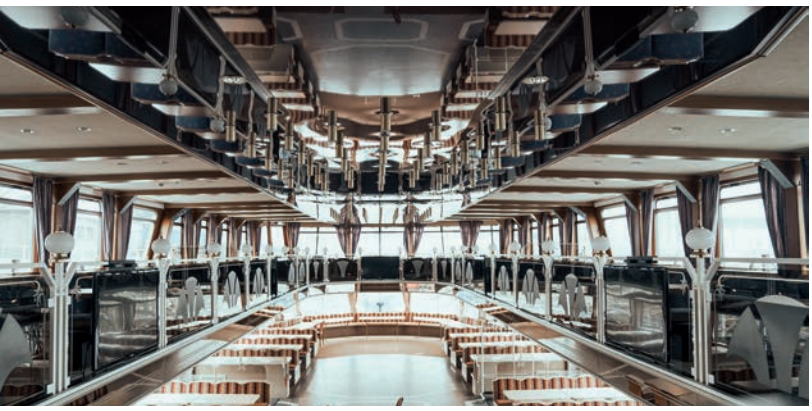
Und damit Leinen los für die SecurityCruise!

Herzlichst, Ihr

Andreas Kunz

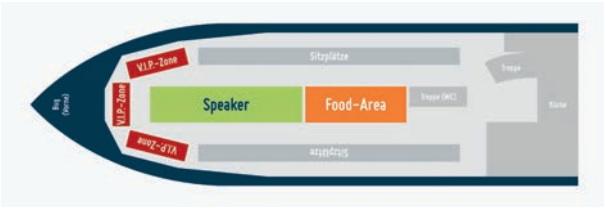
SecurityCruise

ein Name – eine Mission!



Auf 2 Decks der MS-Karlsruhe erleben Sie im Rheinhafen Karlsruhe die komplette Welt der IT-Sicherheit. Sei es Endpoint-, Netzwerk-, Cloud Sicherheit oder generell Datenschutz mit dem Schwerpunkt DSGVO. An 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 auf dem Hauptdeck die Vorträge von unseren namhaften Referenten welche die unterschiedlichsten Bereiche der IT-Sicherheit und deren Facetten beleuchten oder durchlaufen Sie in der Galerie unseren SecurityCircle. Ein Rundgang bei dem Ihnen unsere Hersteller und Lösungspartner die Handwerkzeuge vorstellen die Sie benötigen.

Nutzen Sie die Chance und bekommen Sie die neuesten Infos aus 1. Hand um den Hackern und Ihren Mitbewerben einen Schritt voraus zu sein! Vernetzen Sie sich mit Herstellern, Referenten und Firmen unterschiedlichster Branchen zum Thema IT-Sicherheit und lassen Sie den Tag bei einem leckeren mediterranen Buffet und einer Fahrt auf dem Rhein mit musikalischer Unterhaltung ausklingen.



HAUPTDECK 1: Vorträge der Referenten und Podiumsdiskussionen statt.

GALERIE DECK 2: Der SecurityCircle. Erfahren Sie alles über Lösungen und sprechen Sie direkt mit Experten.

Unsere hochkarätigen Top-Speaker


ANDREAS KECK & WERNER THEINER

Aus München dürfen wir an diesem Tag die beiden Referenten Andreas Keck – Vorstand des German Mittelstand e.V. und Werner Theiner – Geschäftsstellenleiter Süd, eco – Verband der deutschen Internetwirtschaft e.V. begrüßen. Mit Ihnen wird es eine moderierte Diskussionsrunde mit namhaften Gästen geben, die wir die nächsten Tage veröffentlichen werden. Thema Digitalisierung und IT-Sicherheit im deutschen Mittelstand.

MARCO DE FILLIPO

Marco Di Filippo ist „Hacker", Autor, Blogger, Berater und hält Fach- und Publikumsvorträge. Sein Spezialgebiet sind organisatorische und technische IT-Sicherheitsprüfungen und -konzepte. Unser Referent widmet sich diesem Thema IT-Sicherheit mit dem Eventformat Live-Hacking: Er begeistert mit spektakulären Hacks, spannender Unterhaltung, fundiertem Hintergrundwissen und wertvollen Praxistipps!

ELMAR HAAG

Elmar Haag ist Senior Sales Engineer bei der Firma LANCOM. Er verfügt über jahrelange Erfahrung im IT-Security und Netzwerk Markt und wird Ihnen die Vorteile der Cloud Management Plattform und deren Anwendungsgebiete näher bringen. Wir sind sehr froh ihn als Experte begrüßen zu dürfen, da Herr Haag ein Wegbegleiter sowie Wegbereiter in der IT-Security Laufbahn von Herrn Kunz ist und wir von seinem grandiosen Wissen schon sehr viel lernen durften!

ALEXANDER KREUTZ

Alexander Kreutz ist Solution Engineer bei der Firma Bitglass. Der Trend hin zur vermehrten Nutzung von Cloud-Diensten ist unübersehbar. So ist einer branchenübergreifenden, im Jahr 2018 von Bitglass durchgeführten Studie - befragt wurden 135 000 Unternehmen - zu entnehmen, dass bereits 81 Prozent der Firmen Cloud-Services nutzen. Er wird uns live vorführen, wie die «Cloud Access Security Broker»-Lösung (CASB) von Bitglass Unternehmen jeder Branche und Grösse, bei der Nutzung von Cloud-Diensten ermöglicht, die Sicherheitsrichtlinien der eigenen IT-Infrastruktur durchzusetzen.

BENIGNA PROCHASKA

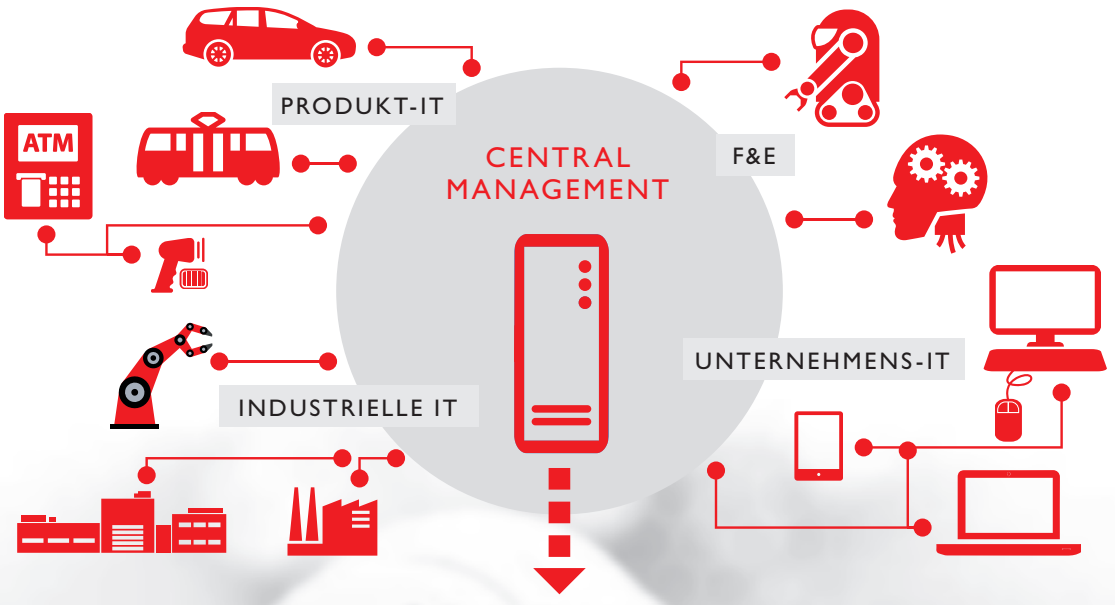
Benigna Prochaska (CEO Intervalid GmbH) ist seit 30 Jahren in der Softwareentwicklung tätig und hat die DSGVO Software Intervalid auf den Markt gebracht. Knapp 1 Jahr nach Inkrafttreten der DSGVO zeigt sie die aktuellen Herausforderungen in der DSGVO Umsetzung für Unternehmen auf. Wie gelingt es beispielsweise möglichst alle Keyplayer aktiv in den Datenschutzprozess einzubinden? Wie unterstützt hier eine moderne DSGVO Software? Erfahren Sie Lösungsansätze aus der Praxis und steigern Sie damit die Effizienz und Qualität in Ihrem Datenschutzmanagement.

CHRISTIAN VON CARLOWITZ

Christian von Carlowitz ist KeyAccount Manager der Virtual Solution AG mit dem Fokus sicheres mobiles Arbeiten mit SecurePIM zu ermöglichen. Seit ihrem Siegeszug sind mobile Endgeräte in der Arbeitswelt nicht mehr wegzudenken. Doch bereiten sie IT-Administratoren und Compliance Beauftragten Kopfzerbrechen. Die fachgerechte Verschlüsselung von Daten, die Verwaltung der Geräte und die Einhaltung aller gesetzlichen Regelungen lässt IT-Abteilungen regelmäßig an ihre Kapazitätsgrenzen stoßen. Hierfür wird Herr von Carlowitz praxisnahe Lösungswege vorstellen.

MARK SEMMLER

Mark Semmler sorgt seit mehr als 20 Jahren für die bedarfsgerechte Absicherung von Informationen. Europa- und weltweit. Langweilig und vorhersehbar? Einschläfernd? Powerpoint-Hölle? Vergessen Sie alles, was Sie über Fachvorträge gehört haben. Ganz gleich ob Vorstandsmeeting, Sensibilisierung der Mitarbeiter oder öffentlicheVeranstaltungen mit mehreren hundert Teilnehmern – Mark garantiert ein aussergewöhnliches Programm, in dem Ihre Nachrichten transportiert werden: Live, unzensiert und extra spannend. Langweilig können andere.



ÜBER NCP

NCP entwickelt seit über 30 Jahren universell einsetzbare Software-Komponenten für die einfache und sichere Vernetzung von Endgeräten und Systemen über öffentliche Netze.

Eingesetzt werden die Lösungen (zentrales, vollautomatisiertes VPN Management, Clients und Gateway sowie Verschlüsselungs- und Firewall-Technologien) in den Bereichen IIoT/Industrie 4.0/M2M, Mobile Computing und Filialvernetzung.

Secure Communication für IT und IIoT

Sichere Datenkommunikation

Die Komplexität von IT Infrastrukturen und die Anforderungen an dieselben wachsen in den letzten Jahren exponentiell an – parallel zu den immer professionelleren Bedrohungsszenarien, denen sich Unternehmen ausgesetzt sehen. Malware, gezielte Hacker-Angriffe, Industriespionage oder auch eigene Mitarbeiter als Sicherheitsrisiko, die Liste ist endlos. Das wichtigste Gut der täglichen Arbeit sind hierbei die Firmendaten, die in allen möglichen Formen vorliegen und geschützt werden müssen. Kundendaten, Produktions- und Auftragsdaten, Informationen über Mitarbeiter und deren Endgeräte wie Laptops und Smartphones oder auch Maschinen und Systeme, die ohne einen User auskommen. Die Szenarien sind ähnlich vielfältig wie auch die Bedrohungen: Mitarbeiter arbeiten von unterwegs am Flughafen oder im Home-Office, Produktionsmaschinen oder Geräte wie Geldautomaten werden ins Firmennetzwerk eingebunden, müssen Zugriff gestatten oder Daten sicher austauschen und dies teilweise ohne einen Servicetechniker oder Mitarbeiter vor Ort.

Die Firmeninfrastruktur als Ganzes betrachtet

Seit über 30 Jahren ist NCP als deutscher Softwarehersteller der Spezialist im Bereich VPN und sichere Datenkommunikation – klassisch für mobile Mitarbeiter und Filialvernetzung, in den letzten Jahren aber bereits auch weitaus komplexer in der Industrie 4.0 erfolgreich im Einsatz. Im klassischen VPN Bereich umfasst das Portfolio VPN Clients für verschiedene Betriebssysteme (Windows, macOS/OS X, iOS und Android), bei einer größeren Zahl automatisiert ein zentrales Management die Verwaltung der Endgeräte und Nutzerzugänge zum Netzwerk. Als Entscheidungshilfe dient vor allem die Größe einer Installation bzw. Infrastruktur:

– NCP Secure Entry Clients für bis zu 100 Nutzer (Einzelplätze und kleine Installationen – KMU)
– NCP Secure Enterprise Clients, Management (SEM) und VPN Gateway für größere Installationen mit über 100 Nutzern

Aus einer engen Technologiepartnerschaft mit Juniper Networks entstanden anbieter-gebunde Clients inkl. Management, die NCP Exclusive Remote Access Solution für Juniper SRX/vSRX. Die Produkte beider Hersteller wurden hierfür technologisch abgestimmt und z.B. die Juniper SRX Serie mit patentierten NCP Technologien ausgestattet.

NCP schlägt die Brücke zwischen Unternehmens-IT und Operativer Technologie

In modernen Firmennetzwerken werden inzwischen auch die Operativen Technologiebereiche wie Produktion und Logistik immer weiter eingebunden und mit der klassischen IT vernetzt. NCP hat bereits seit mehreren Jahren in verschiedenen Anwendungsszenarien Produkte zur Absicherung von Maschinen, Systemen und Geräten im Einsatz. Die Beispiele möglicher Endpunkte sind hierbei zahlreich und ebenso unterschiedlich. Von Fahrzeugen über Geldautomaten bis hin zu Fahrgastinformationssystemen, die sich z.B. an Haltestellen über Wi-Fi mit der Zentrale verbinden und Content abgesichert aktualisieren.

Beispiele für Szenarien im Bereich Industrie 4.0, IIoT und M2M:

– Connected Cars – Flottensteuerung
– Geldautomaten
– Fahrgastinformationssysteme, Displays, Digital Signage
– Healthcare

Absicherung von Sicherheitskameras oder Drohnen

Das Management System von NCP kann hier eine Brücke schlagen und als Single Point of Administration für verschiedene IT-Bereiche innerhalb des Firmennetzwerkes Übersichtlichkeit und Entlastung schaffen.

INTERVALID I DSGVO Software

1 VORBEREITUNG
Mittels online Fragebögen und einem Formular zur Ersterhebung alle relevanten Informationen einholen

2 UMSETZUNG
Gesetzeskonform durch ein vorgefertigtes Verzeichnis der Verarbeitungstätigkeiten und Vorlagen für TOMs

3 COMPLIANCE
Checklisten bearbeiten, Folgeabschätzung durchführen, Schwachstellen via online Prüfung erkennen

4 AUFGABEN
Aufgaben an Mitarbeiter verteilen und rasch innerhalb der Software bearbeiten

5 AUSKÜNFTE
Mittels Reports erhalten Sie alle Informationen auf Knopfdruck für interne und externe Auskünfte

6 BETROFFENE
Ordnungsgemäße Umsetzung der Anfragen mittels definierten Workflow und Einhaltung der Betroffenenrechte

7 SCHULUNGEN
Mittels Umfragen Informationen einholen, Mitarbeiter mit E-Learning schulen und Kurse verwalten

8 PFLEGE
Datenschutzmanagement aufbauen, optimieren und aktuell halten, rasch auf einen Data Breach reagieren

DSGVO fit mit Intervalid

Auch knapp 1 Jahr nach Inkrafttreten der DSGVO bringt sie einige Herausforderungen mit sich: Datenschutz muss gesetzeskonform und transparent dargestellt, Mitarbeiter geschult und regelmäßige Überprüfungen sowie Optimierungen durchgeführt werden.

Doch wie lassen sich diese Herausforderungen in der Praxis meistern?

„Mit einer strukturierten Software steigern Unternehmen ihre Effizienz und gewinnen an Qualität in ihrem DSGVO Prozess", ist Benigna Prochaska, Gründerin von der DSGVO Software Intervalid, überzeugt. Kunden jeder Unternehmensgröße sowie externe Datenschutzbeauftragte werden mit dem Tool bei ihrer DSGVO Umsetzung unterstützt. Unternehmen haben bei der Erstellung ihres Verzeichnisses seit Gültigkeit der DSGVO Fortschritte erzielt, jedoch die gesetzlichen Vorgaben nicht vollständig erfüllen können. Aktuell werden technische und organisatorische Maßnahmen umgesetzt. Dazu müssen Risiken identifiziert und Prozesse für die Behebung von Schwachstellen eingeführt werden. Mit der online Prüfung von Intervalid werden derartige Gaps erkannt, entsprechende Checklisten und Workflows zur Behebung geboten und regelmäßige Audits durchgeführt. Übersichtliche Reports können auf Knopfdruck vorgelegt werden. Im Zentrum steht ein vorgefertigtes Verzeichnis der Verarbeitungstätigkeiten und Mustervorlagen für TOMs.

Insbesondere Konzerne mit Töchtergesellschaften stehen vor der Herausforderung ihre umfangreiche Struktur übersichtlich darzustellen. Viele haben das Verzeichnis mittels Excel angelegt, um zum Stichtag fertig zu sein. Heute stoßen Unternehmen damit an ihre Grenzen, da es schwierig ist, die laufende Pflege länderübergreifend zu bewältigen. Die Nachfrage an einer strukturierten Lösung, mit welcher der DSGVO Prozess schrittweise abgearbeitet und Mitarbeiter standortunabhängig eingebunden werden können, ist stark gestiegen.

Die digitale Welt birgt viele Vorteile, jedoch gewinnt dadurch das Thema Cyber Security mehr an Bedeutung. Firmen sind nie zu 100% vor einem Angriff geschützt, es ist essenziell sich auf den Notfall vorzubereiten. Intervalid bietet für Datenpannen eine gesetzeskonforme Dokumentation und Fragebögen, um Maßnahmen schnell einzuleiten und der Meldefrist gerecht zu werden. Jedes Unternehmen entwickelt sich stetig weiter: Neue Systeme, Prozesse werden eingeführt und Mitarbeiter müssen für das Thema Datenschutz sensibilisiert werden – sie sind der Schlüssel zur reibungslosen Umsetzung. Intervalid stellt dafür online Schulungen inkl. Kursdokumentation und Zertifizierung zur Verfügung.

Intervalid – sicher und effizient bei der unternehmensweiten DSGVO Umsetzung

Datenschutz ist kein einmaliges Projekt, sondern viel mehr ein Prozess, welcher ständig überprüft, angepasst und gelebt werden muss. Online Tools wie Intervalid bieten einen nachhaltigen Aufbau eines gesetzeskonformen Datenschutzmanagements und unterstützen Unternehmen so sicher bei Ihrer DSGVO Umsetzung.

Über Intervalid

- Die Intervalid GmbH ist ein effizienter Begleiter in der unternehmensweiten DSGVO Umsetzung.
- Mit der DSGVO Software Intervalid werden Unternehmen/externe Datenschutzbeauftragte optimal auf alle behördlichen Anforderungen vorbereiten.
- Mit IT-Experten und Juristen wird an der Aktualität der Software gearbeitet und wertvolle Inhalte rund um die DSGVO gegeben.
- Weitere Informationen unter www.intervalid.com

Virtual Solution

SecurePIM: das Office-To-Go

Mobiles Arbeiten auf dem Vormarsch

Mobile Technologien treiben die digitale Transformation voran. Unternehmen wollen die Potenziale dieser Technologien ausschöpfen, müssen sich aber auch der Risiken bewusstwerden. Je mehr auf mobilen Geräten gearbeitet wird, desto interessanter werden diese für Angreifer. Dies und die wachsende Anzahl unterschiedlicher mobiler Endgeräte stellt Unternehmen vor große Herausforderungen.

Herausforderung Sicherheit

Oft geht der Mitarbeiter sorglos mit dem Thema Sicherheit und Datenschutz um. Die EU-DSGVO stellt zudem das Thema Datensicherheit und Schutz der Privatsphäre, sowohl von Kunden und Geschäftspartnern als auch von Mitarbeitern in den Vordergrund. Etablierte Lösungen sind oft aufwendig und teuer oder bieten keinen umfassenden Schutz gegen alle mobilen Sicherheitsrisiken.

Mobiles Arbeiten – einfach und sicher

SecurePIM ist die schlanke Lösung für Unternehmen, die ihren Mitarbeitern die Möglichkeit geben wollen, auch unterwegs genauso produktiv zu arbeiten wie im Büro und sich dabei keine Gedanken um die Sicherheit machen wollen. SecurePIM macht mobiles Arbeiten sicher und DSGVO-konform. Das „Office To Go" vereint alle Funktionen wie E-Mail, Kontakte, Kalender, Aufgaben, Notizen, Dokumentenablage und -bearbeitung, sowie Zugriff auf Intranetseiten und eine sichere Kamera, in einer einzigen App. Die Container-Technologie sorgt dabei dafür, dass alle Daten verschlüsselt und strikt getrennt vom Rest des Gerätes sind. Und das alles nach höchsten Sicherheitsstandards, mit einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüften Lösung.

Herausforderung Flexibilität

Weil Zugriffsrechte und Konfiguration über das SecurePIM Management Portal und das SecurePIM Gateway unkompliziert und schnell geregelt sind, ist SecurePIM ohne Mobile Device Management einsetzbar. Damit ist es die einfachste und zugleich sicherste Möglichkeit, mobil zu arbeiten – auch mit Office 365.

Als Ergänzung zu vorhandenen MDM's bietet SecurePIM einen leicht zu bedienenden und umfangreichen Container für absolute Sicherheit und DSGVO-Konformität. SecurePIM ist dabei mit allen gängigen MDM's nach AppConfig-Standard kompatibel.

Vorteile von SecurePIM

- Alle Funktionalitäten in einer App
- Strikte Trennung von privaten und geschäftlichen Daten – auf demselben Gerät
- Absolute Absicherung gegen Risiken auf mobilen Endgeräten
- State-of-the-Art Verschlüsselung bei der Datenübertragung und -speicherung
- Einfache Installation für IT und Nutzer
- Passend für bestehende IT-Infrastrukturen und jedes Gerät (iOS oder Android)
- Fernlöschung der Daten bei Verlust des Gerätes oder wenn der Mitarbeiter das Unternehmen verlässt
- Firmensmartphone oder eigenes Gerät – beides ist möglich
- Deutscher Hersteller mit Entwicklung in Deutschland

Sicherheit auf höchstem Niveau

Bei der Entwicklung des Produktes SecurePIM wurde eng mit dem BSI zusammengearbeitet und die Lösung SecurePIM Government SDS ist vom BSI für die Datenkommunikation bis zur Sicherheitsstufe „VS-NFD" zugelassen. Dies unterstreicht den hohen Sicherheitsanspruch, den Virtual Solution an seine Produkte hat.

bitglass

ÜBER BITGLASS

- Bitglass ist ein weltweit tätiger Anbieter eines Next-Gen 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.

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.

LANCOM

UNIFIED SECURITY

DATEN. NETZWERK. GESICHERT.

SecurITy made in Germany

Die LANCOM Systems GmbH ist führender europäischer Hersteller von Netzwerk- und Security-Lösungen für Wirtschaft und Verwaltung. Das Portfolio umfasst Hardware (WAN, LAN, WLAN, Firewalls), virtuelle Netzwerkkomponenten und Cloud-basiertes Software-defined Networking (SDN). Soft- und Hardware-Entwicklung sowie Fertigung finden hauptsächlich in Deutschland statt, ebenso wie das Hosting des Netzwerk-Managements.

Besonderes Augenmerk gilt der Vertrauenswürdigkeit und Sicherheit. Das Unternehmen hat sich der Backdoor-Freiheit seiner Produkte verpflichtet und ist Träger des vom Bundeswirtschaftsministerium initiierten Qualitätszeichens **„IT-Security Made in Germany“.**

HIGH-TECH-SYNERGIE „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 IN-A-BOX

Moderne Sicherheitstechnologien garantieren zuverlässigen Schutz von Netzwerken und Daten vor Spam, Viren und Malware.

SSL INSPECTION

› Abwehr von Cyberangriffen durch Erkennen von Malware in verschlüsselten Datenströmen

DEEP PACKET INSPECTION

› Detaillierte Filterung und Kontrolle von Anwendungen und Protokollen

MACHINE LEARNING

› KI-Technik teilt große Datenmengen anhand bestimmter Eigenschaften in Cluster ein

SANDBOXING

› Isolierte Prüfung von Daten-fragmenten vor Eintritt

ANTIVIRUS

› Sandboxing & Machine Learning in der Cloud, mehrstufiges Scan-Konzept

INTRUSION DETECTION & PREVENTION

› Angriffe auf Server oder Netze erkennen und verhindern

APPLICATION LAYER FIREWALL AND CONTROL

› Layer-7-Paketfilter ermöglicht Filtern nach Applikationen und Erstellung von Black- oder Whitelists

Die **Unified Firewall** vereint alle heute relevanten Funktionen des Themas Netzwerksicherheit in einem Gerät. Durch die geplante Einbindung der **Unified Firewalls** in die **LANCOM Management Cloud** in Form von Software Defined Security kann die gesamte Infrastruktur bestehend aus Konnektivität und Sicherheit dann über alle LANCOM Produkte hinweg zentral orchestriert werden.

Weitere Infos ›

LANCOM Systems

Sicherheit, Integrität und Kontrolle

Die heutige schnelllebige digitale Welt ermöglicht es Unternehmen, effizienter zu arbeiten, Wettbewerbsvorteile zu erlangen und den Bedürfnissen ihrer Kunden besser als je zuvor gerecht zu werden. Jedoch wachsen mit den Chancen auch die Sicherheitsrisiken. Unsere kryptographischen Lösungen sichern neue Technologien – Cloud, IoT, Blockchain, digitale Zahlungen – und helfen bei der Erfüllung neuer Compliance-Anforderungen. Dabei verwenden wir dieselbe bewährte Technologie, auf die unsere Kunden heute bereits angewiesen sind, um ihre sensiblen Daten, ihre Netzwerkkommunikation und ihre Unternehmensinfrastruktur zu schützen. Wir garantieren die Sicherheit Ihrer geschäftskritischen Informationen und Anwendungen, gewährleisten die Integrität Ihrer Daten und geben Ihnen die volle Kontrolle – heute, morgen und in Zukunft.

IoT und Blockchain

Während Technologien wie das IoT und Blockchain neue Möglichkeiten der Kundenbindung und des Informationsaustauschs versprechen, darf der frühe Einsatz dieser Möglichkeiten nicht auf Kosten der Sicherheit gehen. nCipher trägt dazu bei, Innovation und Wachstum zu sichern, indem es Integrität bei der Entwicklung neuer IoT- und Blockchain-Implementierungen gewährleistet und so eine Vertrauensbasis schafft, die sich von der Einführung bis zum Einsatz erstreckt.

Cloud Sicherheit

Verschlüsselte Cloud-Datenbanken enthalten zunehmend sensible Unternehmensdaten. Diese sind dort jedoch nur so sicher wie die Verschlüsselungscodes der jeweiligen Anwendung. nCipher HSM ermöglichen Ihnen eine manipulationssichere, unabhängig zertifizierte Kontrolle über die Schlüssel, die Ihre sensiblen Daten in mehreren Cloud-Umgebungen verschlüsseln.

Unternehmensanwendungen

Die heutige digitale Welt bietet völlig neue Chancen für Effizienzsteigerung und Wachstum. Ohne ein sicheres, auf Vertrauen aufgebautes Fundament können sensible Daten, Systeme und Benutzer jedoch gefährdet sein. nCipher bietet praxiserprobte Sicherheit für die wichtigsten, geschäftskritischen Anwendungen, auf die Sie sich jeden Tag verlassen, indem es die Integrität Ihrer Daten gewährleistet und sicherstellt, dass Sie jederzeit die Kontrolle behalten.

Digitale Zahlungen

Neue Möglichkeiten für digitale Zahlungen sorgen für zusätzliche Einnahmequellen, schnellere Transaktionen und ein verbessertes Kundenerlebnis. Sie können sie jedoch nur dann einsetzen, wenn kein Zweifel an ihrer Sicherheit besteht. nCipher ermöglicht neue Modelle für digitale Zahlungen, die auf kryptografischen Protokollen basieren, ebenso wie einen zuverlässigen Schutz der für die Zahlung notwendigen Informationen.

ÜBER nCHIPHER

nCipher Security, eines der führenden Unternehmen auf dem Markt für Mehrzweck-Hardware-Sicherheitsmodule (HSM), unterstützt weltweit führende Unternehmen, indem es die Sicherheit, Integrität und Kontrolle Ihrer geschäftskritischen Informationen und Anwendungen gewährleistet.

CMSC
Connecting Media Service Cockpit

Eine Welt im Wandel

Egal ob Prozesssteuerung, Kunden- und Auftragsdaten, technische Pläne, Personalakten oder Datenbanken: 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. Dazu werden im Unternehmen unter anderem bestehende Schwachstellen analysiert und Arbeitsprozesse dokumentiert, Leitlinien aufgestellt, Ziele formuliert und entsprechende Lösungen erarbeitet. All diese Maßnahmen fließen in die Informationssicherheitsstrategie ein, die es dann umzusetzen, fortwährend zu überwachen sowie den weiteren Entwicklungen anzupassen gilt. Orientierung und wertvolle Hinweise zur technischen und organisatorischen Absicherung eines Unternehmens bieten hierbei die VdS-Richtlinen 10000 „Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU)“.

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. 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 Connecting Media 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 Connecting Media Service Cockpit (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 ins 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

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

IoT-Kompatibilität

Das CMSC 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 alle Ihre Anforderungen und Schnittstellen eine individuelle Anpassung. Die Datenabfrage findet entweder über TCP oder per REST-API statt. Der Fantasie sind dabei keine Grenzen gesetzt. Sprechen Sie uns 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 Connecting Media 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.

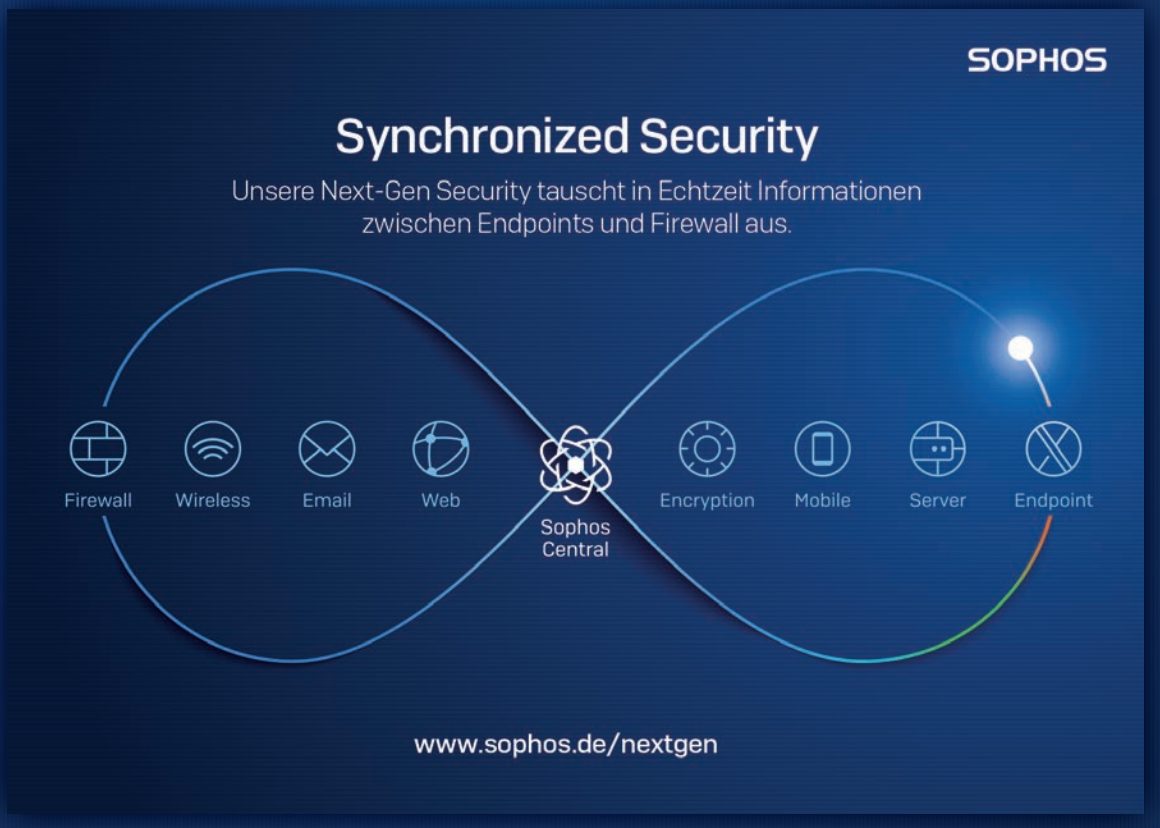
Entlastung von Ressourcen

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.

Mehr unter www.connectingmedia.de



ÜBER SOPHOS

IT-Sicherheitsprodukte sind mittlerweile so kompliziert wie die Netzwerke, die sie schützen sollen. Wir bei Sophos wissen: Die Lösung für komplexe IT-Sicherheit kann nicht noch mehr Komplexität sein. Deshalb begegnen wir Sicherheitsherausforderungen mit klar konzipierten und leicht zu bedienenden Lösungen – mit Sophos sind Sie einfach sicher.

Wir entwickeln schon seit fast 30 Jahren Antivirus- und Verschlüsselungsprodukte. Heute sichern unsere Produkte Netzwerke, die von 100 Mio. Menschen in 150 Ländern und 100.000 Unternehmen genutzt werden – unter anderem bei Pixar, Under Armour, Xerox, Ford, Avis, und Toshiba. IT-Netzwerke werden immer komplexer. Unser Ziel ist es, IT-Sicherheit nicht auch noch komplex zu gestalten, sondern zuverlässig und einfach. Wir wissen, dass eine vernünftige Sicherheitsstrategie alles einbeziehen muss: Netzwerke, Server und Geräte (alle Geräte!). Außerdem muss sie sich einfach über die Cloud verwalten lassen.Mit unseren Produkten können Sie alle Endpoints in Ihrem Netzwerk schützen – Laptops, virtuelle Desktops, Server, Internet- und E-Mail-Verkehr sowie mobile Geräte. Den Schutz übernehmen Produkte, die genau zu Ihren individuellen Anforderungen passen. Wir sichern Ihr Netzwerk und bieten Ihnen dabei das, was sonst niemand kann: Einfachheit.

SOPHOS
Cybersecurity made simple.

Start in eine neue IT-Security-Welt

Jahrelang galt für Unternehmen und öffentliche Einrichtungen in puncto IT-Sicherheit die Maxime „Netzwerk ein Anbieter und Endpoint ein Anbieter – das sorgt für optimalen Schutz". Doch dieses Mantra gilt heutzutage nicht mehr. Der Grund dafür ist die ständige Weiterentwickelung von Technologien. Das gilt sowohl für Hersteller von IT-Security-Lösungen als auch für die Hackerszene. Tradition ist gut und notwendig. Das gilt auch für IT-Sicherheitslösungen. Ohne die Erfahrungen der letzten Jahrzehnte wären Infrastrukturen bei weitem nicht so gut geschützt, wie sie es heute sind. Allerdings ist das alleinige Vertrauen auf Tradition eine Sackgasse. Es müssen neue Wege gefunden werden, modernen Hackerangriffen einen Riegel vorzuschieben und sich für die Herausforderungen durch immer weiter auflösende Peripherien sowohl in der Geschäfts- als auch Alltagswelt zu wappnen. Es ist heutzutage einfach nicht mehr ausreichend, zwei Produkte mit einer guten Erkennungsrate zu verbinden, um für ausreichend Schutz zu sorgen. Die Netzwerkgrenzen werden immer durchlässiger und die Verantwortlichen für IT-Sicherheit müssen neue Werkzeuge an die Hand bekommen, um auf die zunehmende Mobilität der Arbeitswelt reagieren zu können.

Drei Eckpfeiler sorgen für bestmögliche Sicherheit:

1. Sicherheit muss umfassend sein: Eine Lösung muss alle Funktionen beinhalten, die notwendig sind, um die Sicherheitsanforderungen gänzlich zu erfüllen – egal ob Netzwerk, Server oder Nutzer
2. Sicherheit muss einfach zu managen sein: Diese Einfachheit darf sich nicht auf einzelne Bereiche beschränken, sondern muss sich auf alle Aspekte der Lösung erstrecken, u. a. auf die Bereitstellung, Verwaltung, Lizenzierung, den Support und die Bedienung.
3. Sicherheit ist effektiver im Teamplay: Wenn Technologiekomponenten kommunizieren und kooperieren, anstatt isoliert voneinander zu agieren, ergeben sich ganz neue Möglichkeiten.

Effektive IT-Sicherheitssysteme müssen miteinander kommunizieren

Die immer häufigeren Schlagzeilen über gehackte Behörden, Konzerne oder öffentliche Einrichtungen wie Krankenhäuser machen deutlich: Wir stehen an einem Scheideweg in Sachen IT-Sicherheit. Egal ob Sony oder Bundestag, selbst Systeme, bei denen man getrost davon ausgehen darf, dass State-of-the-Art-Lösungen im Einsatz sind, lassen zu viele Lücken zu. Erkennungsraten top, die Firewall perfekt eingerichtet, Technologien wie Advanced Threat Protection installiert – und dennoch Einbrüche über den Onlinekanal? „Wie kann das sein?", werden sich viele fragen. Die Antwort ist recht einfach. Während bislang mit den traditionellen Herangehensweisen Hacker meist ausreichend in die Schranken gewiesen werden konnten, hat sich auch der Cyberkriminalismus weiterentwickelt, ist sehr viel versatiler geworden. Und eben diese Flexibilität macht den traditionellen Sicherheitssystemen zu schaffen, da Ihnen die Schwarmintelligenz fehlt. Sämtliche Funktionen für sich gesehen funktionieren einwandfrei, aber entscheidend ist heute, dass alle diese Systeme intelligent miteinander verknüpft sind, miteinander kommunizieren.

Automatisierte IT-Security-Prozesse entlastet die Verwaltung

Synchronisierte Sicherheit beinhaltet einen sicheren Kommunikationskanal zwischen Endpoint- und Netzwerk-Sicherheitslösungen. Erkennt die Firewall schädlichen Datenverkehr, benachrichtigt sie umgehend den Endpoint-Agenten. Dieser reagiert dynamisch, identifiziert und hinterfragt den verdächtigen Prozess. In vielen Fällen kann er den Vorgang automatisch beenden und die restlichen infizierten Komponenten entfernen. Auf diese Weise werden IT-Abteilungen entlastet und können gleichzeitig einen besseren Schutz von Daten garantieren – inklusive Next-Gen-Technologien wie Deep Learning oder Sandboxing.

UNTERNEHMENSPROFIL

- Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten in Deutschland gegründet.
- Die Appliances der Reihe Greenbone Security Manager (GSM) 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

CYBER RESILIENCE
ist für Unternehmen heute Pflicht

Durch die zunehmende Vernetzung von Geräten und Systemen in Unternehmen vergrößert sich die Angriffsfläche für Hacker immer mehr. Jedes zusätzlich an ein Netzwerk angeschlossene Asset eröffnet ein weiteres potenzielles Einfallstor für Angreifer. Zudem ergeben sich durch neue Programm-Versionen und veraltende Systeme immer neue Schwachstellen. Diese können Cyber-Kriminelle ausnutzen, um sich Zugriff auf gesamte Unternehmensnetzwerke zu verschaffen. Besonders fatal wäre dies bei kritischen Infrastrukturen (KRITIS) wie Wasser- oder Energieversorgern. Fallen diese aus, können große Teile des gesellschaftlichen Lebens zusammenbrechen – und im schlimmsten Fall Menschen zu Schaden kommen.

Insbesondere KRITS-Unternehmen sollten daher nicht mehr nur auf einzelne reaktive Security-Maßnahmen setzen, sondern präventiv einen Zustand der Sustainable Cyber Resilience anstreben – einer nachhaltigen Widerstandsfähigkeit gegen Hacker-Attacken. Das Konzept beinhaltet verschiedene technische und organisatorische Maßnahmen wie Backups und Notfallkommunikationspläne. Eines der Kernelemente ist jedoch ein effektives Schwachstellen-Management.

Greenbone Security Manager erkennt Schwachstellen in Netzwerken

Genau das bieten die Appliances der Reihe Greenbone Security Manager (GSM). Sie überprüfen alle an einem Netzwerk angeschlossenen Geräte auf mögliche Schwachstellen. Dabei bewertet die Lösung das Risiko der gefundenen Sicherheitslücken und stößt Prozesse an, um diese zu beseitigen. 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. Über Konnektoren lässt sich der GSM nahtlos mit Enterprise-Security-Lösungen, wie zum Beispiel Palo Alto, integrieren. Bausteine des Greenbone Security Managers sind das Betriebssystem Greenbone OS und der Greenbone Security Feed, die auf einer eigens dafür entworfenen Hardware-Plattform installiert werden. Im Security Feed sind derzeit über 67.600 Schwachstellen-Tests, wobei diese Zahl mit täglicher automatischer Aktualisierung ständig wächst. Der Greenbone Security Manager unterstützt grundsätzlich eine unbegrenzte Anzahl von Zielsystemen. Die tatsächliche erreichbare Zahl hängt von Unternehmens- und Aufgabengröße ab. Den passenden GSM können Unternehmen anhand der Anzahl ihrer Target IP-Adressen auswählen. Daten verlassen dabei zu keinem Zeitpunkt das Unternehmensnetzwerk, sondern werden ausschließlich lokal gespeichert.

Gewinner des it security award: Höchstpunktzahl in allen Kategorien

Die Angriffsfläche für Hacker nimmt durch die fortschreitende Digitalisierung von Geschäftsprozessen stetig zu. Gerade bei kritischen Infrastrukturen wie Energie- und Wasserversorgern oder Krankenhäusern kann dies fatale Folgen haben. Mit dem Greenbone Security Manager will der Security-Experte Greenbone dazu beitragen, Unternehmen widerstandsfähig gegen Cyber-Angriffe zu machen und ihnen dabei helfen, einen Zustand der Sustainable Cyber Resilience – der nachhaltigen Widerstandsfähigkeit – zu erreichen. Dafür wurde Greenbone im vergangenen Jahr mit dem it security award ausgezeichnet. Der Preis wird jährlich in vier Kategorien auf der IT-Security-Leitmesse it-sa vergeben. Das Sicherheitsprodukt Greenbone Security Manager (GSM) erreichte Höchstpunktzahl in allen Bewertungskategorien.

HORNETSECURITY

ÜBER HORNETSECURITY

Hornetsecurity ist der in Europa führende deutsche Cloud Security Provider für E-Mail und schützt die IT-Infrastruktur, digitale Kommunikation sowie Daten von Unternehmen und Organisationen jeglicher Größenordnung.

Das Produktportfolio umfasst alle wichtigen Bereiche der E-Mail-Security, von Spam- und Virenfilter über rechtssichere Archivierung und Verschlüsselung, bis hin zur Abwehr von CEO Fraud und Ransomware.

10 OFFICE STANDORTE
WELTWEIT, DAVON 6 IN EUROPA

9 RECHENZENTREN
WELTWEIT, DAVON 3 IN DEUTSCHLAND

40.000 UNTERNEHMEN
VON UNS GESCHÜTZT

HORNETSECURITY
Der Cloud Security Pionier

Laut des aktuellen „Global Risks Report“ des World Economic Forum, gehört sie zu den größten globalen Bedrohungen und ist gegenwärtig verantwortlich für einen weltweiten Schaden von rund 600 Millionen Dollar: Cyberkriminalität. Vor allem Unternehmen sind durch die wachsende Gefahr betroffen – Ransomware, Banking-Trojaner und Spionage-Programme führen zu Produktions-Stopp, Betriebsstillstand oder gar zur Insolvenz.

Hornetsecurity gibt dieser Entwicklung entschieden Kontra: Bereits seit 2007 setzt sich der Cloud Security Pionier für die sichere IT-Infrastruktur von Unternehmen ein. Mit ihren innovativen Technologien bietet Hornetsecurity umfassende Lösungen in den Bereichen E-Mail-Security, Web-Security und File-Security. Und das mit Erfolg: Mehr als 40.000 Kunden weltweit setzen mittlerweile auf die qualitativen Services. Das trägt auch zum stetigen Wachstum des Unternehmens bei, denn Hornetsecurity ist inzwischen mit rund 200 Mitarbeitern global an 10 Standorten, unter anderem in den USA, Teilen Südamerikas, der DACH-Region und den Benelux-Staaten, vertreten. Darüber hinaus verfügt Hornetsecurity über ein kontinuierlich wachsendes, länderübergreifendes Netzwerk von mehr als 750 Vertriebspartnern.

Innovative und qualitative Managed Security Services

Um der zunehmenden Bedrohung durch Cyberangriffe gut gerüstet entgegenzutreten, bietet Hornetsecurity eine starke Servicepalette: Das Produktportfolio hält Lösungen für die gesamte Sicherheit des E-Mail-Verkehrs von Unternehmen jeder Größe bereit, darunter der mehrstufige Spam- und Virenfilter, die vollautomatische E-Mail-Verschlüsselung, die rechtssichere E-Mail-Archivierung und der E-Mail-Continuity Service, der bei einem Ausfall die E-Mail-Kommunikation und somit die Produktivität im Unternehmen aufrechterhält. Für ein einheitliches Auftreten und die Ergänzung rechtlicher Pflichtangaben bei der Kommunikation nach außen, sorgt der E-Mail Signature und Disclaimer. Mit Advanced Threat Protection haben besonders durchdachte und gezielte Angriffe wie Ransomware und CEO-Fraud keine Chance und schützenswerte Informationen bleiben, dank des Hornetsecurity Spy-Out-Forensiksystems, im Unternehmen. Im Bereich Web-Security schirmt der Hornetsecurity Webfilter Unternehmen vor den Gefahren des Internets ab. Im Oktober 2018 wurde das neueste Produkt vorgestellt: 365 Total Protection ist die branchenweit einzigartige Security & Compliance Suite, die speziell für Microsoft Office 365 entwickelt wurde. Neben dem zuverlässigen Schutz des E-Mail-Verkehrs, überzeugen die Services von Hornetsecurity insbesondere durch außerordentliche Anwenderfreundlichkeit, einfache Verwaltung und einem hohen Grad an Transparenz und Kontrolle.

Von Experten anerkannte Kompetenz

Als engagiertes Unternehmen der IT-Branche, setzt sich Hornetsecurity in verschiedenen Verbänden sowie gemeinnützigen Vereinen, wie beispielsweise dem eco-Verband der deutschen Internetwirtschaft, Initiative Cloud Services Made in Germany und Initiative Security Made in Germany, ein. Hornetsecurity ist stolz auf die bisherigen Erfolge, die das Unternehmen auf seinem aufstrebenden Entwicklungsweg verzeichnen konnte. So freut sich der in Europa führende Cloud Security Provider für E-Mail unter anderem über folgende besondere Auszeichnungen: Zum vierten Mal eines der 50 am schnellsten wachsenden Technologieunternehmen Deutschlands, prämiert mit dem Fast 50 Award von Deloitte, die Auszeichnung des Services Hornetdrive als „Best SaaS on the Market“ sowie zuletzt die Anerkennung des großen Beitrags Hornetsecuritys zu mehr Sicherheit in der IT-Branche durch den „InfoSec Award 2019“ in der Kategorie Most Innovative SaaS/Cloud Security.

Kontakt

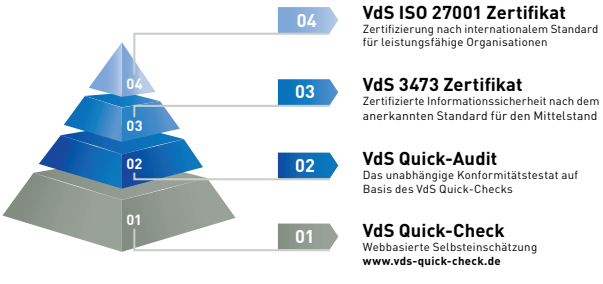
Hornetsecurity GmbH
Am Listholze 78
30177 Hannover
www.hornetsecurity.com
Phone: +49-511 515 464-0

CYBER-SECURITY

für kleine und mittlere Unternehmen (KMU)

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. Zu den Kunden zählen Industrie- und Gewerbebetriebe aller Branchen, international führende Hersteller und Systemhäuser, kompetente Fachfirmen sowie risikobewusste Banken und Versicherer.

Der 1. Cyber-Security-Standard speziell für den Mittelstand Bei tausenden Angriffen täglich erbeuten Cyber-Kriminelle immer wieder wichtige Unternehmensdaten. Digitaler Wissensdiebstahl bedroht die Existenz ganzer Betriebe, Cyber-Attacken können sogar Unternehmensprozesse lahmlegen. Deutschland ist das weltweit am stärksten von Cyber-Kriminalität betroffene Land. Gerade bezüglich des IT-Schutzniveaus unseres Mittelstandes mit seinen vielen hochinnovativen Ideen sprechen IT-Experten von „offenen Scheunentoren". Deswegen hat VdS mit den Richtlinien 3473 – „Cyber-Security für KMU" den 1. Informationssicherheits-Standard speziell für den Mittelstand geschaffen. Diese pragmatische Lösung stellt Europas Nr.1-Institut für Unternehmenssicherheit kostenlos zur Verfügung (www.vds.de/cyber). Die VdS 3473 gehören bereits zu den Top 3 der implementierten Informationssicherheits-Standards und wurden mit dem als „Branchenoscar" bekannten „Security Innovation Award" ausgezeichnet.

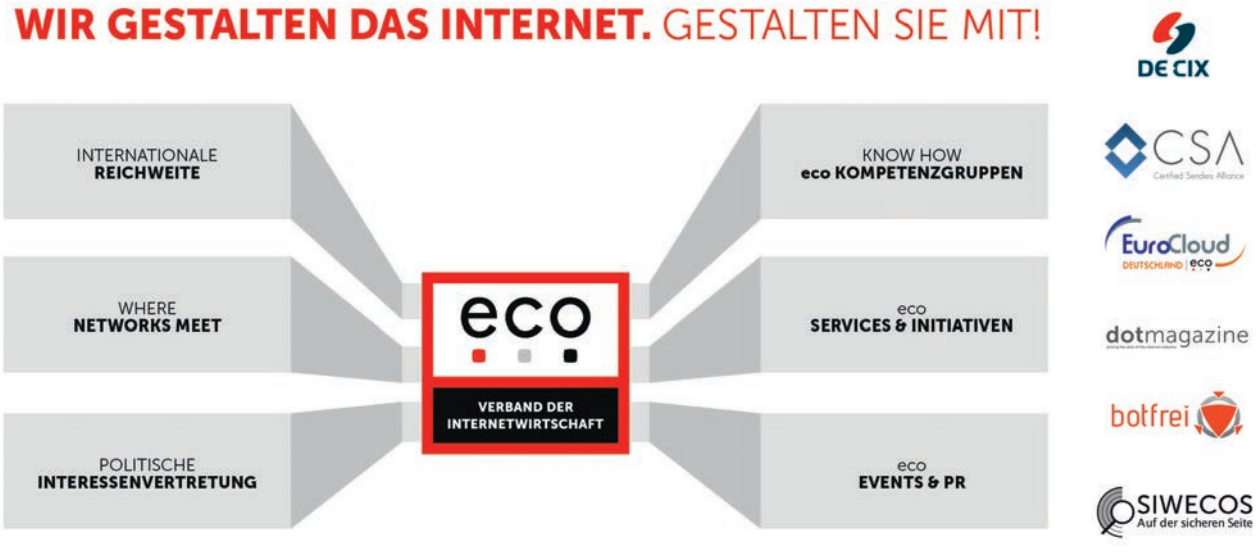


Bei eco finden Sie die Power der ganzen Branche

Tragfähige Netzwerke und ständig aktuelles Branchenwissen sind heute die notwendige Basis für jedes Business. Beides bekommen Sie bei eco. Und: Wir kümmern uns um Ihre Interessen und nehmen Einfluss auf politische Entscheidungen in Berlin und Europa sowie in (inter)nationalen Gremien. Wo viele einzelne Player mit einer Stimme sprechen, erreichen alle gemeinsam mehr.

Treffen Sie neue Geschäftspartner und Kunden: Tausende Kontakte in mehr als 1100 internationalen Mitgliedsunternehmen sind Ihr Branchennetzwerk und machen eco zum größten Verband der Internetwirtschaft in Europa. Seit 1995 gestalten wir maßgeblich die Entwicklung des Internets in Deutschland, fördern neue Technologien, Infrastrukturen sowie Märkte und formen Rahmenbedingungen. In den eco Kompetenzgruppen sind alle wichtigen Experten und Entscheidungsträger der Internetwirtschaft vertreten und treiben aktuelle und zukünftige Internetthemen voran, gemeinsam mit einem Team von über 70 Mitarbeitern. Halten Sie Ihr Know-how auf dem neuesten Stand. In nahezu 100 Veranstaltungen im Jahr, an denen Sie kostenfrei teilnehmen können, erfahren Sie alles über aktuelle Trends und Entwicklungen. Informieren und präsentieren Sie sich vor Ort und nutzen Sie die Chance zum Wissensaustausch mit Fach- und Führungskräften aus allen Segmenten der Internetbranche.

Profitieren Sie von zeitnahen Informationen über Gesetzesinitiativen und politische Entwicklungen, die die Geschäftsmodelle der Internetbranche beeinflussen. Erschließen Sie Synergien sowie Umsatzpotenziale oder entspannen Sie vom Businessalltag bei einem netten Get-together.



JUNIPER NETWORKS

Juniper Networks ist einer der weltweiten Markt- und Technologieführer in den Bereichen Netzwerksicherheit, Netzwerkhardware und Netzwerkperformance. Juniper Networks bietet Unternehmen jeder Größenordnung eine breite Palette dedizierter Lösungen, die eine sichere, stabile und schnelle IP-Kommunikation ermöglichen. Das Portfolio umfasst neben Firewalls mit integrierbaren Security-Features wie IDP-, AV-, Web-Filtering und Anti-Spam auch leistungsstarke Switches, Access-, Routing- Lösungen sowohl als physikalische Plattform als auch virtueller Maschine.

Wieso eigentlich Juniper?

Um zu verstehen, woher Juniper kommt und der Vision angemessen Ausdruck zu verleihen, lohnt sich ein kleiner Blick in die Historie. Über 20 Jahre ist es jetzt her, dass Juniper mit seinem revolutionären M40-Router begonnen hat, die eigene Mission mit Leben zu füllen. Schon damals prägten diese drei Sätze das Leitbild:

Einfachheit ist unsere Leidenschaft.
Einfach bedeutet leistungsstark.
Und „einfach" ist immer eine Frage der Technik

War man in den ersten Jahren nach der Gründung 1996 hauptsächlich mit High-End-Routern erfolgreich, die im Core- und Edge-Bereich des Internet-Backbone eingesetzt werden, hat sich Juniper im Laufe der Jahre zum zweitgrößten Netzwerkausrüster der Welt gemausert. Lösungen und Technologien, unter anderem für die Bereiche Routing, Switching, Security, automatisierte Netze, Data Center, Analyse und Cloud, machen Junipers Portfolio zu einer einzigartigen Plattform, um aus den Netzwerken Ihrer Kunden mehr rauszuholen, als nur die Summe seiner Einzelteile. Ein Unternehmen, das eine solche Größe und Strahlkraft erreicht hat, muss in der Vergangenheit vieles richtig gemacht haben. Wir als Nuvias und auch viele unserer Partner konnten sich, seit wir den Weg im September 2017 gemeinsam gehen, bereits davon überzeugen: Juniper ist der Vorreiter, wenn es darum geht, angesichts der Fülle neuer Technologien und Herausforderungen, der damit einhergehenden Komplexität den Zahn zu ziehen. Denn Komplexität ist das Gegenteil von Fortschritt. Dementsprechend ist auch das aktuelle Motto weitaus mehr als nur ein Marketingslogan.

So wurden aus drei Sätzen zwei Worte:
„Engineering Simplicity"

Juniper lebt die Idee, dass Einfachheit durch Technik die höchste Innovationsstufe darstellt. Mehrwert und Vision eines Technologie-Riesen.

Doch was genau macht eine Zusammenarbeit mit Juniper erstrebenswert? Bevor wir uns der Beantwortung dieser Frage auf den Seiten 18 bis 21 dieser Broschüre noch ausführlich widmen, dürfen wir ein paar gewichtige Argumente bereits hier ins Feld führen:

- wettbewerbsfähiges, leistungsstarkes Portfolio das nahezu alle Netzwerkbereiche abdeckt
- ein überragendes, einheitliches Betriebssystem
- sehr großer Forschungs- und Entwicklungsetat, Etablierung neuer Technologien
- vorbildliche 3rd Party Integration und offene Standards
- breites Spektrum an zielführenden, unterstützenden Maßnahmen für Partner
- Übertragung von High-End Enterprise Features auf den klassischen Mittelstand
- „Sicherheit" in allen Lösungen und Technologien für Unternehmensnetzwerke
- hervorragende Wettbewerbsposition – nicht nur einer von vielen

Fordern und testen Sie uns und vergewissern Sie sich, die richtige Entscheidung getroffen zu haben.

Für Sie! Für Ihre Kunden!
Für Ihr Business!

NetFactory®

ÜBER NETFACTORY

Seit 1989 betreuen wir unsere gewerblichen Firmen- und privaten Endkunden durch verschiedene Vertriebskanäle sowohl online als auch im stationären Handel durch unseren Store in Karlsruhe und unseren Vor-Ort-Service. Neben unserem Handel mit Hardware bieten wir Ihnen ein vielfältiges Portfolio an EDV-Dienstleistungen. Darüber hinaus sind wird Vertriebspartner der Firma Segway und bieten dieses neuartige Fortbewegungsmittel exklusiv in unserer Region an. Ein Kundenstamm von über 250.000 Kunden beweist Ihr Vertrauen in uns.

NetFactory

kompetente Analyse, Beratung und Lösungen für jede Ihrer Problemstellungen

Die Digitalisierung im täglichen Arbeitsleben schreitet mit großen Schritten voran, mit einer Zunahme an Komplexität und Vielfältigkeit der IT relevanten Themen. Daher ist es wichtig den richtigen Partner an der Seite zu haben der das eigene Leistungsportfolio ergänzt um für Sie als Kunde ein Rundum Sorglos Service aus einer Hand bieten zu können. Die NetFactory ist unser Partner des Vertrauens für kompetente Beratung mit kundenorientierten Service auf höchstem Niveau. Damit wir einen noch besseren Service und eine entsprechende Tiefe der IT Themen anbieten können, haben wir uns die Firma NetFactory als Partner mit ins Boot geholt, um Beispielsweise eine 24/7 Service Abdeckung oder als Ansprechpartner für Spezialthemen in denen wir als Connecting Media keine dedizierten Ressourcen haben. Das Ziel ist nämlich, dass wir uns gegenseitig ergänzen und gemeinsam ein komplettes Digitalisierungsportfolio aus einer Hand anbieten zu können. Sollten Sie also kurzfristig oder langfristig Hilfe mit Ihrer IT benötigen? Sind Sie mit unserem Partner Net Factory auf dem richtigen Weg: Mit über 20 Jahren Erfahrung als IT-Dienstleister bietet die NetFactory Ihnen kompetente Ansprechpartner für alle aktuellen Problemstellungen, die auf Sie in der digitalen Welt zukommen.

- ✖ Sie benötigen eine komplett neue IT-Infrastruktur an einem neuen Firmenstandort?
- ✖ Sie müssen Ihre in die Jahre gekommene EDV dringend modernisieren, wissen aber nicht, wie Sie es am sinnvollsten anfangen sollen?
- ✖ Irgendwie laufen Ihre Programme nicht mehr so, wie sie es eigentlich sollten, obwohl niemand etwas geändert hat?
- ✖ Ihre Server funktionieren wie sie sollen, aber Ihr Backup besteht aus sporadisch auf USB-Sticks kopierten Daten – was Sie recht unruhig schlafen lässt?
- ✖ Sie bekommen andauernd E-Mails mit verdächtigen Anhängen, sind sich aber nicht wirklich sicher, ob jeder Mitarbeiter diese offensichtlichen Köder als solche erkennt?
- ✖ Sie arbeiten viel von zuhause aus oder greifen von überall auf der Welt auf ihre IT-Infrastruktur zu, vermuten aber, dass Ihre Systeme nur mit dem Benutzernamen und Login zu ungeschützt über das Internet erreichbar sind?

Wir bieten kompetente Analyse, Beratung und Lösungen für jede Ihrer Problemstellungen.

Vereinbaren Sie einen Termin, damit wir uns ein Bild von Ihrer bestehenden IT-Struktur machen können. Besprechen Sie ihre Ideen, Anforderungen und Wünsche mit unseren Experten, damit wir gemeinsam mit Ihnen erarbeiten können, wie Ihre IT Ihnen gerecht wird. Wir können Ihnen natürlich auch helfen, wenn es eigentlich schon zu spät scheint. Auftretende Probleme – egal ob Hardware- oder Softwareseitig – können durch unsere Techniker analysiert werden um Ihre IT-Abhängigen Abläufe schnellstmöglich zu entstören. Situationsbedingt können wir die Entstörung auch gerne aus der Ferne durchführen um Ihre Ausfallzeit weiter zu minimieren. Doch bevor es „zu spät“ ist, überarbeiten wir gerne ihre Backup-Strategie, damit im schlimmsten Fall der Fälle nur ein Minimum Ihrer wertvollen Daten verloren geht.

Und damit es trotz eines potentiellen Hardware-Defekts gar nicht erst zu einem Datenverlust, oder zu einer Ausfallzeit kommt, beraten wir Sie auch gerne zu redundanten Hochverfügbarkeits-Lösungen und helfen Ihnen diese Konzepte in Ihrem Unternehmen umzusetzen. Sicherheitskonzepte, die die Gefahren von unberechtigtem Zugriff auf Ihr Netzwerk und Ihre Daten minimieren gehören ebenso zu den Lösungen, die Sie mit uns gemeinsam für Ihr Unternehmen erarbeiten können. Die notwendigen Anpassungen der Infrastruktur, sowie die Definition von notwendigen Regeln führen wir gerne in enger Zusammenarbeit mit Ihnen durch, um Ihren Workflow so wenig wie möglich zu beeinflussen und das Bestmögliche an Schutz für Ihre Daten herauszuholen.

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 Marketing-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-Service, IT-Security 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.

Unsere innovative 360°-Lösung bietet Ihnen viele Vorteile

Sie können 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. Sie stärken das Kundenvertrauen durch Sicherheits- und Datenschutzstandards nach aktueller Gesetzeslage. Ihre Probleme identifizieren und lösen wir schon im Vorfeld – bevor Sie dadurch Geld verlieren. 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

INNOVATIONSPREIS-IT
BEST OF 2018
initiative mittelstand
CONSULTING

Profitieren Sie von unserem ausgezeichneten Service!

Die Badeschlappen sind in 35 dm-Filialen in und um Karlsruhe erhältlich

Wir unterstützen das Sybelcentrum für Kinder- und Jugendhilfen

Keine kalten Füße

Je 10 Prozent der Teilnahmegebühr unseres Kongresses „Security Cruise“ auf der MS Karlsruhe im Mai 2019 spenden wir an die lokale Kampagne „Keine kalten Füße“. Erfahren Sie hier mehr über das Sybelcentrum der Heimstiftung Karlsruhe.

Das Sybelcentrum, errichtet 1913, in der Sybelstraße 11 in der Karlsruher Südstadt

Das Sybelcentrum

Das Sybelcentrum der Heimstiftung Karlsruhe bietet ca. 170 Kindern und Jugendlichen ab 6 Jahren ein vielfältiges und differenziertes Jugendhilfeangebot im stationären, teilstationären und ambulanten Bereich. Die Arbeit mit den Kindern und Jugendlichen hat das Ziel, deren individuelle Lebenssituation positiv weiterzuentwickeln, Probleme zu mindern und eine Wiedereingliederung bzw. den Verbleib in ihrer Familie zu ermöglichen.

Herausforderung: Generalsanierung

Das denkmalgeschützte Gebäude wurde 1913 gegründet. Nun ist dieser Zufluchtsort für Kinder und Jugend-

liche in die Jahre gekommen: Wasser-, Stromleitungen und Heizung sind marode. Auch sonst erfüllt der Bau die aktuellen Standards für eine zeitgemäße Kinder- und Jugendhilfe kaum noch. Doch die Trägerin des Sybelcentrums, die Heimstiftung Karlsruhe – gemeinnützig und nicht-gewinnorientiert – kann die Kosten für die Generalsanierung nicht alleine aufbringen.

Spendenprojekt: „Keine kalten Füße"

Die Sanierung des Sybelcentrums wird einen zweistelligen Millionenbetrag beanspruchen. „Keine kalten Füße" hat das Ziel, in den kommenden Jahren bis zu 3 Millionen Euro zu sammeln, um die Vision einer modernen, zeitgemäßen Kinder- und Jugendhilfe in Karlsruhe zu unterstützen. Ferner möchte die Kampagne darauf hinweisen, dass nicht alle Kinder und Jugendlichen in Karlsruhe die gleichen Startchancen erhalten und daher Einrichtungen wie das Sybelcentrum gesamtgesellschaftlich sehr wichtig und unterstützungswürdig sind.

Helfen Sie mit – Machen Sie sich mit uns auf die Socken!

Die Initiative „Keine kalten Füße" ist im November 2017 gestartet und hat das Ziel, das Sybelcentrum für Kinder- und Jugendhilfen von Grund auf zu sanieren, bauliche Schwächen und schwerwiegende Schäden zu beheben und der pädagogischen Aufgabe angemessene Rahmenbedingungen zu ermöglichen.

Auf vielseitige Weise bietet die Kampagne Unterstützungsformen an

Neben Geldspenden auf das Spendenkonto oder Barspenden in eine der über 50 Spendendosen im Karlsruher Einzelhandel, kann auch zu feierlichen Anlässen wie beispielsweise unter dem Motto „Spenden statt schenken" zum Geburtstag eine Spendenbox angefordert werden. Interessierte Bürgerinnen und Bürger können auch Zeit spenden im ehrenamtlichen KKF-Aktionsbündnis bei unterschiedlichen Karlsruher Veranstaltungen.

Heimstiftung Karlsruhe
Sybelcentrum
Projektleiterin: Anna Weißhaar
Sybelstraße 11, 76137 Karlsruhe
Tel. 0721/133-5688
www.keine-kalten-fuesse.de
info@keine-kalten-fuesse.de
Facebook: KEINEKALTENFUESSE

Spendenkonto: Sparkasse Karlsruhe
IBAN DE22 6605 0101 0108 2575 93

Spendenbox im Fachhandel „City Cosmetic"

Spendenbox für private Anlässe

Eigene „Keine kalten Füße"-Produkte: Die Socken und Backformen gibt es in der Tourist-Information am Hauptbahnhof

Oberbürgermeister Dr. Frank Mentrup, Schirmherr
Alle Kinder und Jugendlichen sollen in Karlsruhe die Chance auf einen guten Start in ihr eigenes Leben erhalten. Manche von ihnen brauchen dazu unsere Hilfe. Darum bitte ich Sie als Schirmherr um Ihre ganz persönliche Unterstützung für die Kampagne „Keine kalten Füße".

Martina Warth-Loos, Geschäftsführerin der Heimstiftung Karlsruhe
Helfen Sie uns , in unserem Sybelcentrum für Kinder- und Jugendliche gute Rahmenbedingungen zu schaffen. Wir als Trägerstiftung des Sybelcentrums sind nicht alleine in der Lage, die notwendigen Maßnahmen zu realisieren. Dafür brauchen wir Ihre tatkräftige Unterstützung.

Eva Rühle, Einrichtungsleiterin im Sybelcentrum
Jeden Tag dürfen wir rund 170 Kinder und Jugendliche begeliten und unterstützen. Damit meinen Mitarbeiterinnen und Mitarbeiter und mir die bestmögliche Arbeit im Sybelcentrum und seinen Außenstellen möglich ist, sind Baumaßnahmen unumgänglich.

Connecting Media

Bleiben Sie mit uns immer auf dem neuesten Stand:

XING	https://www.xing.com/companies/connectingmedia
LINKEDIN	https://www.linkedin.com/company/27108974/
YOUTUBE	http://youtube.connectingmedia.de
BLOG	https://www.connectingmedia.de/blog/
FACEBOOK	https://www.facebook.com/ConnectingMedia.de/
EVENTS	https://www.connectingmedia.de/event/