IT-BUSINESS SPEZIAL

Verlags-Sonderveröffentlichung 4/2018

IT-Security

BILD: RAWPIXEL – STOCK.ADOBE.COM - [M] CARIN BOEHM

Vogel Business Media

IT-SECURITY: IM SCHATTEN DES FALLBEILS

Autor: Dr. Andreas Bergler

email: andreas.bergler@it-business.de
tel: 0821 2177 141

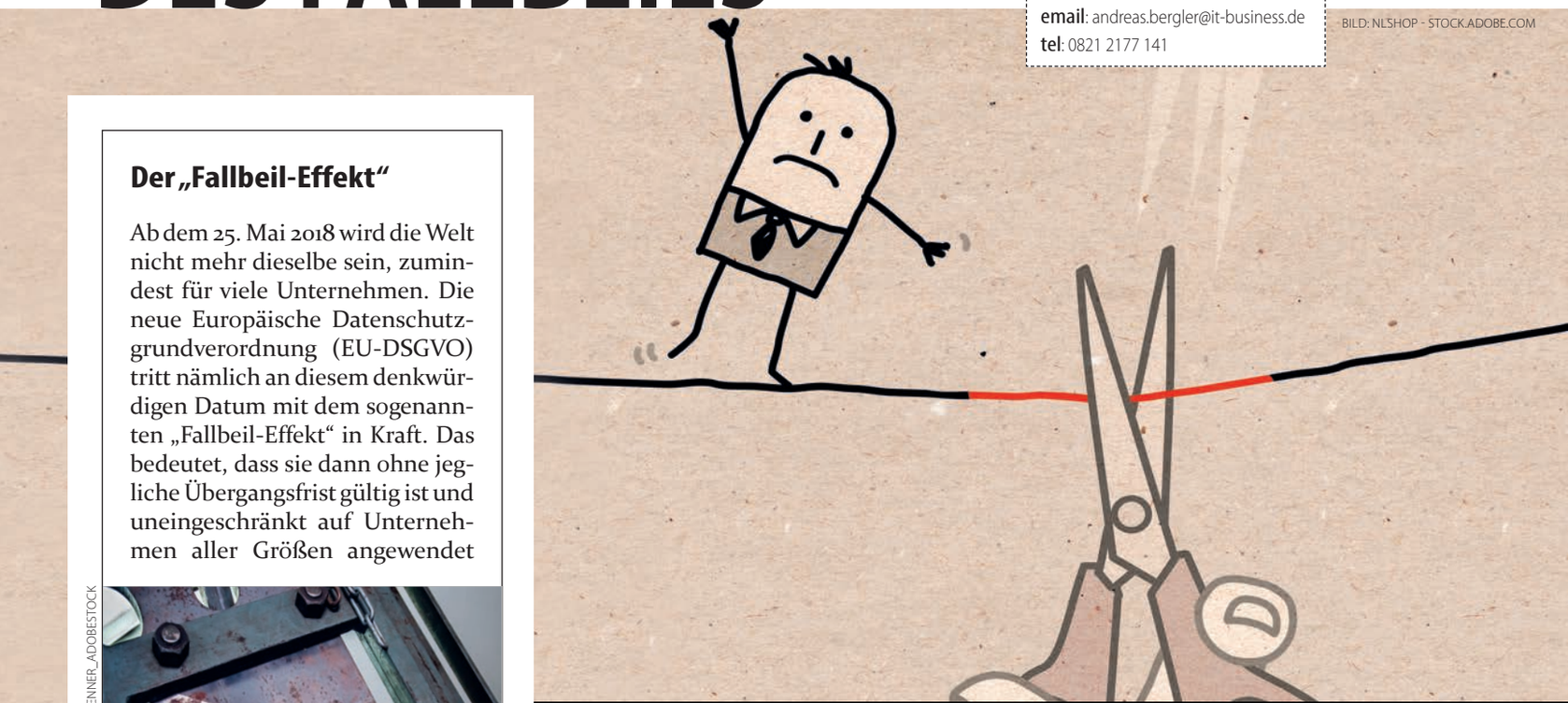


BILD: NLSHOP - STOCK.ADOBE.COM

In puncto Cyber-Security und Compliance sind deutsche Unternehmen in erschreckend geringem Ausmaß auf Probleme vorbereitet. Der „Fallbeil-Effekt" der dräuenden EU-DSGVO dürfte sie daher umso härter treffen.

Der „Fallbeil-Effekt"

Ab dem 25. Mai 2018 wird die Welt nicht mehr dieselbe sein, zumindest für viele Unternehmen. Die neue Europäische Datenschutzgrundverordnung (EU-DSGVO) tritt nämlich an diesem denkwürdigen Datum mit dem sogenannten „Fallbeil-Effekt" in Kraft. Das bedeutet, dass sie dann ohne jegliche Übergangsfrist gültig ist und uneingeschränkt auf Unternehmen aller Größen angewendet werden kann. Eine nur teilweise Anwendung des Datenschutzrechts ist ausgeschlossen. Weil die Aufsichtsbehörden das Bundesdatenschutzgesetz bei Verstößen bisher relativ moderat angewendet haben, soll die DSGVO jetzt umso strenger wirken. Bei der Verhängung von Geldbußen sollen die Behörden darauf achten, dass eine Geldbuße „wirksam, verhältnismäßig und abschreckend" (Art. 83 Abs. 1) ist.

[http://bit.ly/Feil-dsgvo]
[http://bit.ly/anwalt-dsgvo]

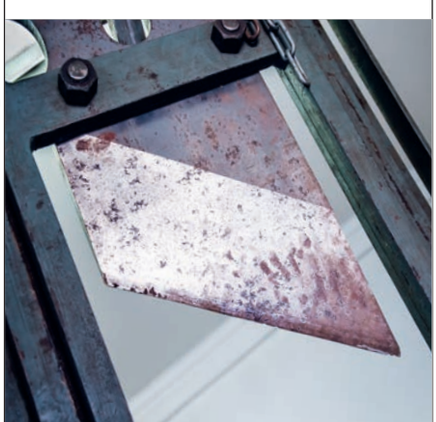


BILD: THORSTEN ZENNER_ADOBESTOCK

Bei Cyber-Vorfällen sieht die DSGVO drakonische Maßnahmen vor.

Die steigenden Kosten für einen Sicherheitsvorfall in einem Unternehmen sind ein beliebtes Beispiel, um Firmenlenkern und IT-Verantwortlichen in aller Öffentlichkeit vor Augen zu führen, warum sich Investitionen in IT-Security lohnen können. Aktuell werden diese Kosten auf die unglaubliche Summe von etwa einer halben Million US-Dollar pro Vorfall für ein durchschnittliches, großes Unternehmen geschätzt. Die Schätzung beinhaltet unter anderem verlorene Umsätze, verlorene Kundenkontakte, direkte Kosten zur Schadensbehebung und weitere Folgekosten, die durch Image-Schäden oder Kurseinbrüche entstehen. Aber trotz aller Hochrechnungen und Schätzungen des Gefahrenpotenzials in klingender Münze: Es hat sich noch nicht allzu viel geändert in der Wahrnehmung der Dringlichkeit von IT-Security. nur eine Minderheit reagiert überhaupt auf Sicherheitsvorfälle.

Das kann sich aber bald ändern. Stichtag ist der 25. Mai dieses Jahres. Ab diesem Datum tritt nämlich die Europäische Datenschutzgrundverordnung (EU-DSGVO) mit sofortiger Wirksamkeit in Kraft (siehe Kasten). Erstmalig werden dann auch staatliche Behörden bei der Ahndung von Sicherheitsvorfällen in Unternehmen kräftig zulangen. Bei Verstößen gegen die DSGVO – und nichts anderes ist ein Sicherheitsvorfall – beträgt die Geldbuße für europäische Unternehmen bis zu 20 Millionen Euro. Alternativ, das heißt je nachdem, welcher Wert höher ist, sind bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr abzutreten.
Bei kleinen und mittleren deutschen Unternehmen ist die Schadenssumme, die durch Sicherheitsvorfälle in der IT entstehen kann, deutlich geringer. Der Spezialversicherer Hiscox rechnet hier mit einem durchschnittlichen Wert von

46.000 Euro. Der liegt zwar weit unter demjenigen großer Unternehmen, dürfte aber angesichts der neuen europaweiten Regelungen durchaus existenzbedrohliche Ausmaße angenommen haben. Ein möglichst umfassendes Sicherheitskonzept mit einer Absicherung auf allen Ebenen ist daher das Gebot der Stunde. Denn die Bedrohungen wachsen...

Die größten Security-Trends haben Security-Anbieter unterschiedlicher Couleur entlang der Leitdifferenz „Cyberkriminelle versus Abwehrtechnologien" aufgeschlossen:

- Auf der **Blockchain** basierende Sicherheitstechnologien könnten Online-Umgebungen mit besserem Schutz und geringerer Anonymität schaffen.
- Andererseits verlockt die Blockchain Cyberkriminelle auch dazu, via Botnets **Cryptowährungen** schürfen zu lassen, also die Rechenkapazitäten fremder Rechner auszunutzen.
- Serverlose Sicherheits- und Analysefunktionen werden zum Standard für Funktionen wie Virenscans.
- Angreifer haben es vor allem auf **„weiche Ziele"** abgesehen. Große Schwachstellen für die Sicherheit in Firmen sind ungepatchte Systeme, aber auch arglose Mitarbeiter.
- Gefahren liegen dabei auch in – häufig schon ungesichert ausgelieferten – **IoT-Geräten und SCADA-Systemen** für die Industriesteuerung.
- **Predictive Analytics** wird zu einer grundlegenden Methode werden. Um Bedrohungen einen Schritt voraus zu sein, werden Angriffe vorhergesehen, die noch nicht stattgefunden haben.
- **Künstliche Intelligenz (KI), Machine Learning und Chatbots** werden es ermöglichen, menschliche und maschinelle Intelligenz effektiver zu kombinieren. Dadurch können Sicherheitslücken besser bewertet und priorisiert werden.
- Anderseits werden sich auch Cyberkriminelle vermehrt der **KI-Mechanismen** bedienen, um automatisierte, flächendeckende Angriffe zu lancieren.
- Der zentrale Kern der **3G- und 4G-Netze** ist laut A10 Networks meist nicht geschützt. Es sei deswegen immer wahrscheinlicher, dass Angreifer große Mobilfunkbetreiber angreifen und ihre Netze lahmlegen.
- Angriffe auf **Cloud-Anbieter:** Da deren Kunden keine Kontrolle mehr über die zugrundeliegende Infrastruktur ihrer Anwendungen haben, werden immer mehr Unternehmen auf einer Multi-Cloud-Strategie umsatteln.

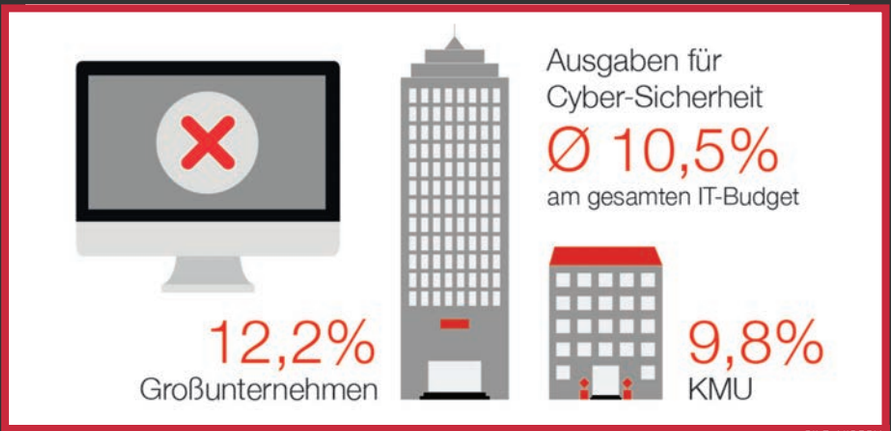


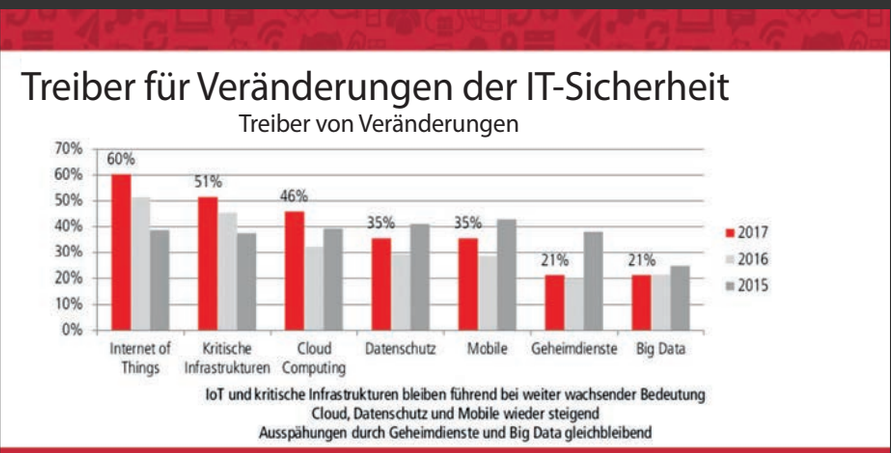
BILD: HISCOX

Unternehmen erleben regelmäßig Cyber-Zwischenfälle – und investieren in Cyber-Sicherheit.

„Die Ratlosigkeit der Betriebe zeigt, dass sie Hilfe von Profis für die Erstellung einer wasserdichten Cyber-Strategie brauchen."

Robert Dietrich, Hauptbevollmächtigter von Hiscox Deutschland

Cybersicherheit wird mehr und mehr zu einer Frage des Menschenrechts: Verbraucher sind gefährdet, da sie oft am wenigsten gegen Bedrohungen geschützt sind. Aber auch Regierungen auf regionaler und kommunaler Ebene dürfen vermehrt mit Cyberangriffen rechnen. Während die Öffentliche Hand mehr und mehr Online- und Cloud-Dienste nutzt, werden sich Budgetkürzungen hier auf die Sicherheit auswirken. Im Argen liegt die Sicherheit auch bei Unternehmen: Laut dem Versicherer Hiscox ist die Mehrheit der deutschen Unternehmen als „Cyber-Anfänger" zu klassifizieren. Mit einer kohärenten Cyber-Sicherheitsplanung im Sinne der EU-DSGVO seien die meisten Unternehmen, insbesondere KMU, schlichtweg überfordert. Gute Zeiten also für Versicherungen: Laut Hiscox plant ein Viertel aller Unternehmen, in den nächsten zwölf Monaten, eine Cyber-Versicherung abzuschließen.



IoT und kritische Infrastrukturen haben in den vergangen drei Jahren am stärksten zugelegt und gelten jetzt als die Top-Treiber im Security-Markt.

BILD: ECO VERBAND

DSGVO – DIE HEISSE PHASE HAT BEGONNEN

DAS KÖNNEN IT-DIENSTLEISTER JETZT FÜR IHRE KUNDEN TUN

Viele Unternehmen haben sich in den letzten Monaten umfassend darüber informiert, welche Neuerungen die DSGVO mit sich bringt und welche Sanktionen bei Verstößen drohen.

BILD: INFINIGATE

Nun hat die heiße Phase für die praktische Umsetzung der Vorgaben begonnen. Neben organisatorischen Anpassungen werden Unternehmen spätestens jetzt auch vermehrt nach geeigneten technischen Lösungen suchen, die ihnen dabei helfen, die Anforderungen der DSGVO zu erfüllen. Jetzt ist der perfekte Zeitpunkt für IT-Dienstleister Ihre Kunden zu geeigneten Lösungen zu beraten und bei der Umsetzung zu unterstützen.

Die Tools: Infinigate hat zusammen mit dem IT-Fachanwalt Christian R. Kast neben einem Umsetzungsfahrplan sechs Anwendungsbeispiele zur DSGVO herausgearbeitet. Diese veranschaulichen, in welchen Bereichen die Verordnung beispielsweise Anwendung findet und welche Bereiche der Architektur betroffen sind. Außerdem schlägt der Distributor konkrete Technologien vor, die in den jeweiligen Szenarien zum Schutz personenbezogener Daten eingesetzt werden können. Bei den Technologie-Empfehlungen bleibt Infinigate herstellerneutral. Die Anwendungsfälle sind ein Bestandteil des Infinigate DSGVO Guide, der unter www.infinigate.de/dsgvo kostenlos zum Download angefordert werden kann.

Infinigate bietet seinen Partnern außerdem individuelle Webinare an, um deren Endkunden zum Thema DSGVO zu informieren oder offene Fragen zu klären. Dem juristischen Teil schließt sich in der Regel die Vorstellung einer DSGVO-konformen Security-Lösung an, deren Einsatz der Reseller seinem Kunden empfiehlt. Ähnlich ist auch das Eventkonzept für Endkundenveranstaltungen aufgebaut, welches Sie kostenfrei bei Infinigate anfordern können. Ob Webinar oder Vor-Ort-Event: Als Referent für den juristischen Teil der Präsentationen empfiehlt Infinigate Herrn Christian R. Kast, Fachanwalt für IT-Recht vom anwaltscontor München. Buchen Sie den Referenten über Infinigate, dann profitieren Sie von besonderen Rahmenkonditionen.

Kontakt DSGVO Kampagne:
web: www.infinigate.de/dsgvo
E-Mail: kati.rabe@infinigate.de
Telefon: +49 (0)89 89048 -229

Der Ansatz: Ganzheitlichkeit im Sinne der Datensicherheit. Die meist in den letzten 20 Jahren historisch gewachsenen IT-Infrastrukturen in Unternehmen sind oft nicht mehr zeitgemäß. Um gegen die heutigen Bedrohungen gewappnet zu sein und Sicherheitsvorfälle bestmöglich zu verhindern, bedarf es oft einer Runderneuerung. Diese sollte proprietäre Insellösungen ablösen und Platz schaffen für Systeme, die miteinander kommunizieren. „Synchronized Security" nennt der IT-Security Hersteller Sophos beispielsweise seine Antwort auf die Frage nach intelligenter, vernetzter Sicherheit.

Bis zum Erreichen des Ziels einer nahezu vollumfänglichen Sicherheit braucht es funktionierende Konzepte. Die Spezialisten von Infinigate haben für Partner ein schlüsselfertiges Modell entwickelt. In diesem Modell zeigt der Distributor das nahtlose Ineinandergreifen der Lösungen von Gemalto, HPE Aruba und Sophos.

BILD: INFINIGATE

Marco Di Filippo, IT-Sicherheitsexperte, whitelisthackers UG

„Ganzheitlich denken – das ist meine Empfehlung. Warum? Aus einem einfachen Grund: Unternehmen denken häufig zu eindimensional. Das ist ein echtes Problem. Cyberkriminelle haben dadurch noch immer ein relativ leichtes Spiel. Ein Umdenken – hin zur Ganzheitlichkeit im Sinne der Datensicherheit – bekommt durch die EU-DSGVO nun eine noch größere Bedeutung."

Kontakt NextGen Networking-Konzept:
web: www.infinigate.de/nextgen
E-Mail: musterfirma@infinigate.de
Telefon: +49 (0) 8989048-385

DSGVO – Interview mit einem Fachanwalt

Christian R. Kast, Fachanwalt für IT-Recht, kennt die Herausforderungen, vor denen viele Unternehmen und auch IT-Dienstleister in diesen Tagen stehen. Die meist gestellte Frage lautet noch immer: „Was müssen wir konkret tun?" Infinigate hat diese und weitere brennende Fragen an den Rechtsanwalt gestellt:

Herr Kast, Systemhaus-Partner werden von Kunden aus dem Mittelstand zunehmend aufgefordert, DIE DSGVO-Lösung zu installieren. Was würden Sie Kunden darauf antworten?
Die DSGVO umfasst mehr als die Installation einer oder mehrerer technischer Lösungen. Das Konzept zielt vielmehr auf einen ganzheitlichen Ansatz der Betrachtung datenschutzrechtlicher Vorgänge ab. Dafür muss sich ein Unternehmen einige Fragen stellen, nämlich erstens „Wo erhebe ich personenbezogene Daten?" bzw. „Wo kommen solche Daten in meinem Unternehmen her?". Denn die Erhebung ist der erste Schritt der Verarbeitung von Daten im Sinne der DSGVO. Bei der Verarbeitung geht es um: „Was mache ich mit diesen Daten?" – „Wo sind diese gespeichert?", wobei der zweite Punkt auch die Frage nach Rechenzentren oder länderübergreifenden Verarbeitungen umfasst.
Schließlich die letzte Grundfrage: „Wann lösche (sperre) ich personenbezogene Daten?", denn auch wenn es Aufbewahrungspflichten gibt, selbst während dieser dürfen Daten nicht für jedermann im Unternehmen zugänglich sein.

BILD: INFINIGATE

Christian R. Kast, Fachanwalt für IT-Recht

Wie können IT-Dienstleister Kunden unterstützen?
Die DSGVO hat im Rahmen des ganzheitlichen Ansatzes das „Verarbeitungsverzeichnis" entwickelt. Damit soll ein Gesamtüberblick über die Prozesse geschaffen werden, mit denen personenbezogene Daten verarbeitet werden. Dabei umfassen die zu beschreibenden Prozesse einerseits organisatorische, also insbesondere intern getroffene Maßnahmen zum Datenschutz und zur Datensicherheit, wie z.B. IT-Handbücher und Sicherheitskonzepte.
Andererseits sind die Prozesse in technischer Hinsicht zu beschreiben und die prozessimmanenten Risiken für den Datenschutz zu analysieren. Dies ist der Bereich, in dem IT-Dienstleister ihre großen Stärken einsetzen können, denn wer kennt die Systeme des Kunden üblicherweise besser als der IT-Dienstleister?

Werden konkrete IT-Maßnahmen oder Technologien von der DSGVO gefordert?
Die DSGVO ist technikneutral und beschreibt daher auch keine bestimmte Technologie, die einzusetzen ist. Allerdings gibt die DSGVO Hinweise zu Mechanismen, die beim Einsatz von Technologie in der Umsetzung der Vorgaben wichtig sind. Die Stichworte Anonymisierung, Pseudonymisierung und Verschlüsselung sind zwar nicht primär technisch zu verstehen, aber dennoch so, dass eingesetzte Technologien oder Maßnahmen diese Mechanismen nutzen sollen.

Was bedeutet „Stand der Technik" und woher weiß ich, was aktuell „Stand der Technik" ist?
„Beste am Markt verfügbare Technik" wird häufig als Umschreibung verwendet und verdeutlicht, worauf es ankommt: es muss nicht jede „denkbare" Technik eingesetzt werden, sondern die, die Risiken der konkreten Datenverarbeitung minimiert. Eine allgemeingültige „Liste des Stands der Technik" gibt es allerdings nicht, aber das BSI und branchenspezifische Sicherheitsstandards (wie sie z. B. in manchen ISO-Zertifizierungen normiert sind) helfen bei der Einordnung weiter. Daher sind ISO-Zertifizierungen bei der Einordnung der im Unternehmen eingesetzten Technologien hilfreich und liefern noch dazu durch die Erfassung der wesentlichen Unternehmensprozesse eine gute Grundlage für das Verarbeitungsverzeichnis.

Wie ändert sich die Verantwortung der IT-Dienstleister?
Wenn der Dienstleister – zum Beispiel bei der Erbringung von Managed Services – Zugriff auf personenbezogene Daten des Kunden hat, muss eine Vereinbarung zur Auftragsverarbeitung getroffen werden. Der Dienstleister muss dabei aktiv auf den Abschluss der Vereinbarung hinwirken und es müssen technische und organisatorische Maßnahmen beschrieben und ergriffen werden, um die Datensicherheit und den Datenschutz bei der Verarbeitung im Auftrag zu gewährleisten.

Die Uhr tickt. Was kann (noch) getan werden, wenn noch nichts passiert ist?
Die Aufsichtsbehörden stehen in den „Startblöcken". Es wird sicherlich zeitnah Prüfungen und Bußgelder geben, auch wenn nicht sofort alle Bereiche geprüft werden können. Falsch ist aber, abzuwarten. Starten Sie mit der Erfassung der Prozesse und wenn Risiken festgestellt werden, adressieren Sie diese unmittelbar, selbst wenn noch nicht das „große Ziel" im ersten Schritt erreicht werden kann. Einen Elefanten isst man ja auch nicht in einem Stück, sondern Scheibchen für Scheibchen.

Webinar mit Fachanwalt
Christian R. Kast zum Thema
DSGVO – Was IT-Dienstleister jetzt tun können
Termin: 13. April 2018 10 -11 Uhr
Anmeldung unter www.infinigate.de/dsgvo

DSGVO: SOPHOS HILFT IN ZENTRALEN BEREICHEN BEI DER UMSETZUNG

Seit Jahren beherrschen gravierende Datenpannen mit alarmierender Häufigkeit die Schlagzeilen. Im Rahmen der EU-DSGVO drohen betroffenen Unternehmen im Falle von Datenpannen empfindliche Geldstrafen. Die Verschlüsselungs- und Datenschutztechnologien von Sophos können Unternehmen helfen, die Anforderungen des Gesetzes zu erfüllen.

Die Entscheidung, welche technischen Sicherheitsmaßnahmen zu etablieren sind, muss auf Grundlage einer umfassenden Risikoanalyse und im Rahmen einer individuellen Sicherheitsstrategie erfolgen. Bei der Etablierung technischer Sicherheitsmaßnahmen können Sophos-Lösungen in drei zentralen Bereichen zum Einsatz kommen, um bei der Einhaltung der DSGVO zu helfen:

1. Bekämpfung der Hauptursache von Datenverlusten

Feindliche Angriffe von außen und versehentliche Offenlegungen von personenbezogenen Daten durch interne Fehler sind die zwei Hauptursachen für Datenpannen. Sophos Central Device Encryption ist die einfachste Methode zur zentralen Verwaltung Ihrer Festplattenverschlüsselung für alle PCs und Macs. Sophos Mobile bietet einen vergleichbaren Schutz für Daten auf mobilen Geräten und ermöglicht darüber hinaus eine Remote-Ortung, -Zurücksetzung oder -Sperrung verloren gegangener Geräte. Intercept X kann gemeinsam mit schon bestehenden Antivirus-Produkten genutzt werden und schützt effektiv vor Malware, Exploits und Ransomware.

2. Rechtzeitiges Stoppen von Bedrohungen

Die XG Firewall schützt Netzwerk-Geräte, indem sie die Angriffe direkt an der Netzwerkgrenze abfängt – also noch bevor sie auf Geräte gelangen können. Die Sophos Email Appliance blockiert oder verschlüsselt zudem sensible E-Mails und Anhänge automatisch. Zudem werden verdächtige E-Mails gestoppt, bevor sie in die Posteingänge der Benutzer gelangen können.

3. Fortwährender Schutz durch Verschlüsselung

Eine E-Mail kann auch ganz ohne böse Absicht schnell bei einem falschen Empfänger landen. Wenn die Mail vertrauliche Daten enthält, können harmlose Fehler schnell weitreichende Folgen haben. Die dateibasierte Verschlüsselung von Sophos SafeGuard sorgt dafür, dass Daten auch dann geschützt bleiben, wenn sie die Geräte oder das Netzwerk verlassen.

E-Mail: sophos@infinigate.de
Telefon: +49 (0)89 89048 – 381/-382

WAS BEDEUTET DIE DSGVO FÜR WLAN-HOTSPOTS?

Deutsche User checken im Schnitt 214 Mal pro Tag ihr Smartphone. Auch im Urlaub, im Krankenhaus, beim Arzt, im Shop, im Restaurant oder in der Bibliothek verzichten sie nicht gern darauf. Wer da nicht mitspielt, riskiert Kunden zu verlieren. Doch nun kommen neue Pflichten auf Betreiber zu, die am 25. Mai 2018 nach der DSGVO in Kraft treten. Es drohen nicht nur höhere Bußgelder als bisher, sondern die Ahndung von Verstößen ist keine Ermessensfrage mehr, sondern wird verpflichtend.

BILD: PEXELS

Internetzugang über WLAN zu bieten ist in vielen Branchen heute ein Standard geworden.

Was ist daher zu beachten, um auf der gesetzeskonformen Seite zu bleiben? Entscheidend ist die Anmeldung, denn dabei werden Daten verarbeitet. Hier die wichtigsten Kriterien:

1. *Rechtsgrundlage:* Ohne sie keine Datenverarbeitung! Liegt etwa die Buchung eines Zimmers mit WLAN vor, kauft der Kunde ein WLAN-Ticket oder gehört der Zugang zu einer Club-Mitgliedschaft, einem Arbeitsverhältnis oder Hochschulbesuch, liegt eine rechtliche Grundlage für die Verarbeitung der Buchungsdaten vor.
2. *Transparenz und Datensparsamkeit:* Es soll nur verarbeitet werden, was für die bestimmungsgemäße Nutzung notwendig ist, und nicht zusätzliche, etwa für Marketingzwecke gedachte Daten – schon gar nicht ohne Wissen des Betroffenen.
3. *Datenweitergabe:* Werden Daten an Dritte übertragen, muss der Betroffene informiert und einverstanden sein. Freies WLAN, etwa im SPA, nur gegen dieses Einverständnis zur Verfügung zu stellen, ist nicht zulässig. Das Opt-in, etwa in eine Mailing-Liste des angeschlossenen Kosmetikinstituts, muss unabhängig von diesem Service erfolgen.
4. *Aufbewahrungsfristen:* Der Kunde muss informiert werden, wie lange die Daten gespeichert werden, und es muss eine Möglichkeit geben, diese auf Verlangen zu löschen, zu berichtigen, zu übertragen oder einzuschränken. Jeder Betreiber ist gut beraten, persönliche Kundendaten nicht länger als notwendig oder gesetzlich vorgeschrieben aufzubewahren.
5. *Datenschutzhinweis:* Um als Betreiber seine Informationspflicht korrekt zu erfüllen, ist dies das richtige Medium. In klar verständlicher Sprache ist darzulegen, welche Daten auf welcher Grundlage wie lange gespeichert werden und ob sie an Dritte übertragen werden. Dazu ist eine Kontaktmöglichkeit zu nennen.

Mit der IAC-BOX sind Sie in Sachen Datenschutz jedenfalls auf der sicheren Seite. Datensparsame und datenschutzfreundliche Grundeinstellungen sowie Löschungs- und Anonymisierungsfunktionen bot die IAC-BOX bereits. Nun wurden zusätzlich die Datenschutzhinweise für den Endbenutzer aufbereitet und alle Anmeldeseiten mit Hinweisen zu Anonymisierungs- und Löschfristen ausgestattet. Das neue, zukaufbare Modul **Privacy Toolkit** bietet darüber hinaus Optionen, ein individuelles Datenverarbeitungsverzeichnis mit Berücksichtigung der spezifischen Anmeldemethoden und Datenbank-Anbindungen zu erstellen, sowie komfortable Möglichkeiten zu privacy by design/default Voreinstellungen, Vertraulichkeits- und Auftragsverarbeiter-Vereinbarung, Checks, Hilfetexte und Zugriffsprotokollierung.

IACBOX
Internet Access Control

Werden Sie IAC-BOX-Partner!
Näheres unter iacbox.com oder bei unserem Distributor Infinigate Deutschland unter Portfolio/Hersteller.

Privacy Toolkit Extra Bonus
Speziell für IT-Business-Leser gibt es bei einer Bestellung bis 30. April 2018 einmal je Partner 10 % Extra-Discount. Geben Sie dafür den Promotion Code #ITBIZ2018 an.

Bestellbar: ab sofort.
Auslieferung: Ende März/Anfang April.

DSGVO SETZT STANDARDS AUCH FÜR DEN CHANNEL

Mechanismen zur Pseudonymisierung und Verschlüsselung sind elementare Schritte, um den Datenschutz zu verbessern und die neuen Vorgaben zu erfüllen. In Artikel 32 der DSGVO und an weiteren Stellen wird gerade das Thema Verschlüsselung mehrfach erwähnt. Der Channel muss sich spätestens jetzt mit den Technologien hinter dem Begriff beschäftigen.

BILD: GEMALTO

Die EU-Datenschutz-Grundverordnung (DSGVO) schärft bestehende Regelungen: Verschlüsselung und Co. sind nun konkrete Themen, an denen sich der Channel orientieren muss.

Kryptografie darf dabei nicht als simple Ja/Nein- oder Checkbox-Funktion verstanden werden. Sie muss durch ineinandergreifende Schutzmechanismen über alle Ebenen gewährleistet werden. In dieser Thematik sind benutzerfreundliche Lösungen spezialisierter Anbieter gefragt. Der Verschlüsselungsexperte Gemalto hat sein Produktportfolio entsprechend ausgerichtet und kann in vielen Use Cases helfen, die DSGVO-Anforderungen einzuhalten. Die Maßnahmen umfassen dabei mehrere Bereiche – hier ein kleiner Einblick:

- Verschlüsselung auf Anwendungsebene: Schon bei der erstmaligen Erstellung oder Verarbeitung werden Daten verschlüsselt und bleiben über ihren kompletten Lebenszyklus geschützt, seien es unstrukturierte Daten oder strukturierte Dateien.
- Datenbankverschlüsselung auf Spaltenebene: Informationen müssen auch nach der Erstellung in den Datenbanken geschützt werden. Hier bietet die Spaltenverschlüsselung eine gute Kombination aus Performance und Sicherheit.
- Verschlüsselung auf Dateiebene: In jedem Fall muss man damit rechnen, dass Angreifer Netzwerke trotzdem unterwandern können. Daher sollte durch Verschlüsselung auf Dateiebene eine zusätzliche Schutzvorkehrung getroffen werden, die auch bei erfolgreichem Unterwandern anderer Segmente wirkt – ganz gleich, ob diese sich auf Servern vor Ort oder in der Cloud befinden.
- Verschlüsselung virtueller Rechner: Virtualisierte Maschinen enthalten ebenfalls sensible Informationen und müssen vor unerlaubter in Betrieb- und Einsichtnahme geschützt werden. Gerade Gastbetriebssysteme werden ohne entsprechende Sicherheitsmechanismen leicht von herkömmlichen Tools übersehen.
- High-Speed Netzwerk-Verschlüsslung: Nicht nur gespeicherte Daten, sondern auch Informationen, die innerhalb eines Netzwerkes oder zwischen Rechenzentren ausgetauscht werden, müssen auf ihrem Transportweg geschützt werden. Dafür sorgen Layer-2 High-Speed-Encryptoren (HSE), die neben effektivem Schutz auch für maximalen Datendurchsatz sorgen.
- Auf die Schlüssel kommt es an: Verschlüsselung ohne den Schutz der verwendeten Keys ist so gut wie nutzlos. Wirklich sicher kann kryptografisches Schlüsselmaterial nur in Verbindung mit spezieller Hardware erzeugt, verwaltet und aufbewahrt werden. Hier bieten sich Hardware-Sicherheits-Module (HSM) an.
- Identity- und Accessmanagement (IAM) als Verbindung zur Verschlüsselung: Es wird sichergestellt, dass nur berechtigte Benutzer überhaupt Zugriff auf geschützte Dateien erhalten. Eine Multi-Faktor-Authentisierung macht es Angreifern zusätzlich noch schwerer, Identitäten zu stehlen. Als zusätzlicher Faktor eignen sich Smartcards oder Tokens.

Die Herausforderungen rund um die DSGVO sind groß, denn die Kunden vertrauen bei der Wahl der richtigen Tools auf die Beratung durch Systemhäuser und Reseller. Schlecht geplante oder unzureichende Schutzmechanismen sind im Ernstfall unzuverlässig und ziehen trotz umfangreicher Vorbereitung Strafen nach sich. Organisationen müssen sich auf allen Ebenen überprüfen und nach dem „Stand der Technik" absichern. Welchen „Fahrplan" Unternehmen dabei nehmen können und in welchen Beispielfällen welcher Handlungsbedarf entstehen kann, können Sie im herstellerneutralen DSGVO Guide von Infinigate nachlesen (kostenloser Download unter www.infinigate.de/dsgvo).

E-Mail: gemalto@infinigate.de
Telefon: +49 89 89048 383

CYBER-ANGRIFFE ENTWICKELTEN SICH 2017 ZUM GRÖSSTEN GESCHÄFTSRISIKO

BILD: SONICWALL

Der Sicherheitsspezialist SonicWall hat die Ergebnisse seines jährlichen Sicherheitsberichts präsentiert. Der Cyber-Threat-Report zeigt den intensiven Wettlauf um IT-Sicherheit. Demnach erfassten die Sicherheits-Experten 9,32 Milliarden Malware-Angriffe, sowie mehr als 12.500 neue Sicherheitslücken im Jahr 2017.

Der Wettlauf um die IT-Sicherheit betrifft alle Unternehmen, Behörden, Organisationen und Anwender", sagt Bill Conner, CEO von SonicWall. „Unsere aktuellen Erhebungen zeigen eine Reihe strategischer Angriffe und Gegenmaßnahmen, der Wettlauf um IT-Sicherheit eskaliert weiter. Mit unseren in der Praxis anwendbaren Informationen möchten wir dabei helfen, die allgemeine Sicherheitslage zu verbessern."

Zu den wichtigsten Ergebnissen zählen:

- Cyberangriffe werden zum größten Geschäftsrisiko für Marke, Betrieb und Geschäftsergebnis
- Die Anzahl der Malware-Angriffe stiegen von 2016 bis 2017 um 18,4 Prozent auf 9,32 Milliarden
- Die Zahl der Ransomware-Attacken sank zwar von 638 Millionen auf 184 Millionen, doch die Anzahl an Varianten nahm um 101,2 Prozent zu
- Durch SSL/TLS verschlüsselter Datenverkehr wuchs um 24 Prozent, dies entspricht 68 Prozent des gesamten Datenverkehrs

Den Fortschritten der Cyberkriminellen – wie beispielsweise die Verdoppelung unterschiedlicher Ransomware-Varianten, Malware-Cocktails, dass sich Cyberangriffe weiterhin in SSL-Daten verstecken sowie Chip-Prozessoren und IoT als neue Angriffsfelder – stehen die Fortschritte der Security-Branche gegenüber.

Fortschritte der Security-Branche:

Gesamtvolumen der Ransomware-Angriffe sinkt: Obwohl WannaCry, Petya, NotPetya und Bad Rabbit für Schlagzeilen sorgten, trafen die Voraussagen über zunehmende Ransomware-Attacken nicht ein. Das Gesamtvolumen der Ransomware-Angriffe reduzierte sich 2017 um 71,5 Prozent zum Vorjahr, auf 184 Millionen. 37 Prozent der weltweiten Ransomware-Attacken im vergangenen Jahr wurden in Europa verzeichnet.

Nutzung von SSL/TLS-Verschlüsselung nimmt um 24 Prozent auf 68 Prozent zu: Verschlüsselung und die zu wenig verbreitete Untersuchung des verschlüsselten Datenverkehrs eröffnet Cyberkriminellen die Möglichkeit, Schadprogramme in verschlüsseltem Datenverkehr zu verstecken und ins Netzwerk einzuschleusen. Immerhin, eine immer größere Anzahl an Unternehmen implementiert zunehmend Sicherheitslösungen wie Deep Packet Inspection (DPI), um in verschlüsseltem Datenverkehr versteckte Angriffe zu erkennen und abzuwehren.

Effektivität von Exploit Kits reduziert: Da die meisten Browser inzwischen Adobe Flash nicht mehr unterstützen, wurden 2017 keine neuen kritischen Flash-Sicherheitslücken mehr entdeckt. Doch Angreifer probieren nun neue Strategien aus. Zu den verstärkt attackierten Zielen gehören Anwendungen wie Apple TV oder Microsoft Office, die erstmals in die Top 10 kamen.

BILD: SONICWALL

Strafverfolgung immer erfolgreicher: Die Verhaftung wichtiger Cyberkrimineller führte zu empfindlichen Störungen der „Malware-Lieferkette" und beeinträchtigte den Aufstieg neuer Hacker. Die Zusammenarbeit von nationalen und internationalen Strafverfolgungsbehörden verstärkt somit den Kampf gegen weltweite Cybergefahren.

Der jährliche Cyber Threat Report von SonicWall beschreibt auch Best Practices und Sicherheitsprognosen für 2018. Sie werden im vollständigen Bericht ausführlich thematisiert. Weitere Informationen gibt es unter: SonicWall Annual Threat Report 2018 [www.sonicwall.com/de-de/lp/2018-cyber-threat-report]

Aktuelle Daten zu Cyberangriffen – inklusive weltweiter Trends, Varianten und Zahlen – gibt es im SonicWall Security Center.

[securitycenter.sonicwall.com]

EU-DSGVO: WIRD E-MAIL-VERSCHLÜSSELUNG ZUR PFLICHT?

Die EU-DSGVO fordert in Art. 32 Abs. 1, dass personenbezogene Daten „unter Berücksichtigung des Stands der Technik" zu schützen seien.

BILD: SEPPMAIL DEUTSCHLAND GMBH

Stephan Heimel, Sales Director der SEPPmail Deutschland GmbH

> **„ZURZEIT SETZEN VOR ALLEM DATENSENSIBLE BEREICHE VERSTÄRKT AUF E-MAIL-VERSCHLÜSSELUNG.**

BILD: SEPPMAIL DEUTSCHLAND GMBH

Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH

Vielen Verantwortlichen ist durch diese Formulierung nicht ganz klar, ob die Verschlüsselung von E-Mail-Kommunikation ab Mai sogar zur Pflicht wird. Ein genauer Blick in den Gesetzestext bringt Klarheit.

Denn in Art. 32 fordert die EU-DSGVO ganz konkret die „Pseudonymisierung und Verschlüsselung" personenbezogener Daten. „Aus unserer Sicht ist an dieser Stelle kein Raum für Interpretationen", sagt Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH. „Vielmehr wird sogar eine Verschlüsselungspflicht eingeführt. Und die gilt meines Erachtens nicht nur für die Verarbeitungen von Daten innerhalb einer Organisation, sondern vor allem auch für den E-Mail-Versand. Denn hier verlassen sensible Daten die Organisation. Entsprechend beobachten wir seit einiger Zeit gerade in Branchen wie Gesundheit, Recht und Finanzen einen Trend hin zu sicherer Kommunikation."

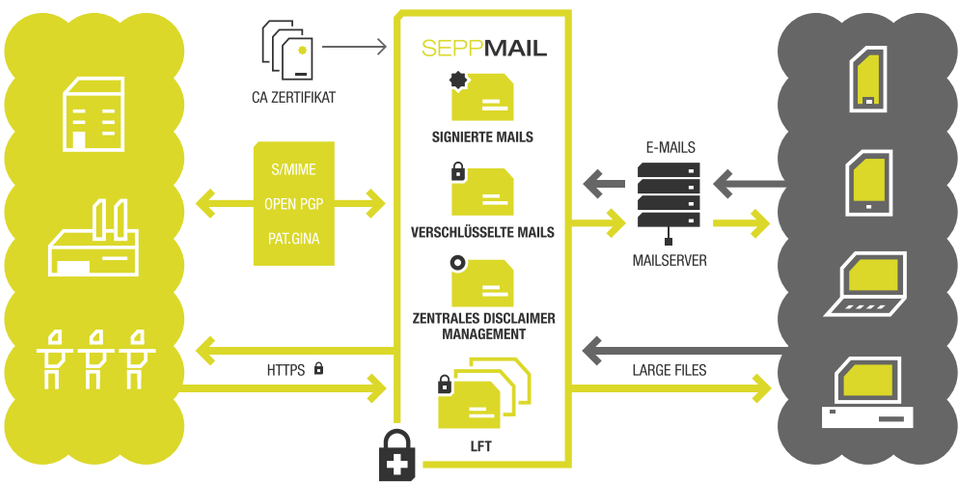


BILD: SEPPMAIL DEUTSCHLAND GMBH

E-Mails einfach und sicher: Vor allem für Unternehmen ist eine benutzerfreundliche und einfach zu integrierende Lösung besonders wichtig; gerade auch in Hinsicht auf die Kommunikation mit Partnern, die selbst noch keine Verschlüsselungslösung einsetzen. SEPPmail hat dazu ein Gateway und die patentierte Verschlüsselungsmethode GINA entwickelt. GINA nutzt HTML-Container, um die Nachrichten verschlüsselt an den Empfänger auszuliefern. Diese Methode erfordert beim Empfänger keine zusätzlichen Softwareinstallationen. Er benötigt lediglich Standardkomponenten wie einen Mailclient, einen Internetzugang und einen Browser, um verschlüsselte Mails auf einem beliebigen Endgerät zu empfangen und zu lesen. Nutzt er keine eigene Verschlüsselung, kann er über das Gateway bequem verschlüsselt antworten. Der Nachrichtenversand erfolgt extrem ressourcenschonend, da die verschlüsselte Mail nicht vorgehalten, sondern samt Anhang ausgeliefert wird. Lediglich bei großen Anhängen (Large File Transfer – LFT) wird die Nachricht samt Anhang für einen gewissen Zeitraum zwischengespeichert.

„Dieses Thema wird in vielen Unternehmen immer wichtiger", sagt Stephan Heimel, Sales Director der SEPPmail Deutschland GmbH. „In allen Branchen, in denen Vertrauen eine zentrale Rolle spielt oder in denen der wirtschaftliche Erfolg eines Unternehmens von seinem technologischen Vorsprung abhängt, beobachten wir eine zunehmende Sensibilisierung für das Thema. Der Sicherheitsgedanke überträgt sich sogar auf die gesamte Wertschöpfungskette. So erhalte ich immer häufiger Anfragen von Firmen, die von ihren Partnern einen verschlüsselten E-Mail-Versand verlangen. Das geht soweit, dass bei der Auftragsvergabe Unternehmen, die verschlüsselt kommunizieren, den Vorzug erhalten."

Kontakt

Telefon: +49 (0)89 89048 -383
Email: seppmail@infinigate.de

ZWEI- ODER MULTIFAKTOR-AUTHENTIFIZIERUNG?

In vielen Fällen ist zudem auch eine Multifaktor-Authentifizierung zwingend erforderlich. Jedes Unternehmen sollte eine adaptive Vorgehensweise bei der Einführung einer Authentifizierungslösung wählen, die eine optimale Balance zwischen Sicherheit und Benutzerkomfort gewährleistet.

Jedes Unternehmen hat ein individuelles Anforderungsprofil und es kann keine One-size-fits-all-Lösung für die sichere Authentifizierung geben. Deshalb kann die Zweifaktor-Authentifizierung in einigen Fällen auch zu kurz greifen: Das betrifft zum Beispiel Anwendungen und Transaktionen im Bankenbereich, hier reichen zwei Faktoren nicht für einen adäquaten Schutz vor externen Gefahren aus. Eine starke Authentifizierung ist allein schon aufgrund aktueller und künftiger Rechts- und Verwaltungsvorschriften unerlässlich. Ein Beispiel hierfür ist die von der EU verabschiedete und am 13. Januar 2018 in Kraft getretene „Payment Services Directive 2" (PSD2). Die Richtlinie regelt nicht nur den Internet-Zahlungsverkehr, sondern führt auch die starke Multifaktor-Authentifizierung für das Online-Banking als obligatorisch ein.

Einige Unternehmen arbeiten mit Daten, die nicht sicherheitskritisch sind, ein Datenverlust hätte dann nicht unmittelbare finanzielle oder geschäftliche Auswirkungen. Für solche Unternehmen ist eine Zweifaktor-Authentifizierung in der Regel ausreichend. Da allerdings immer mehr Unternehmen mit Kunden über Online- oder mobile Kanäle interagieren, sind zunehmend persönliche, vertrauliche Daten zu berücksichtigen, die entsprechend geschützt werden müssen. Ein Datendiebstahl kann hierbei aufgrund unzureichender Authentifizierungsverfahren ernste Folgen haben, sowohl unter finanziellen als auch unter Reputationsgesichtspunkten. Aus diesen Gründen sollten diese Unternehmen eine Multifaktor-Authentifizierung nutzen. Bei der Multifaktor-Authentifizierung werden üblicherweise traditionelle besitz- und wissensbasierte Faktoren um eine weitere Komponente aus den Bereichen Eigenschaft oder Verhalten ergänzt, ein Beispiel hierfür sind biometrische Merkmale.

BILD: HID GLOBAL

Das einfache Passwort zum Schutz von Daten hat ausgedient. Die Zweifaktor-Authentifizierung ist ein Kernelement jeder Sicherheitsstrategie.

Der Vorteil einer Multifaktor-Authentifizierung hinsichtlich Sicherheit ist offensichtlich. Eine Frage stellt sich dabei aber: Wenn eine Multifaktor-Authentifizierungs-Lösung eine effiziente Möglichkeit darstellt, Bedrohungen zuverlässig auszuschließen, warum sollte sie dann nicht von allen Unternehmen und durchgängig eingesetzt werden? Die Antwort liegt in der Bedeutung einer positiven User Experience. Eine Authentifizierungsprozess muss nicht nur zu einer hohen Sicherheit beitragen, er muss auch für Kunden und Mitarbeiter so einfach wie möglich sein.

Aus diesem Grund ist ein adaptiver Sicherheitsansatz extrem wichtig, das heißt, die richtige Balance zwischen positiver User Experience und hoher Sicherheit zu finden, ist von essenzieller Bedeutung. So ist es beispielsweise einerseits auf jeden Fall sinnvoll, eine Zweifaktor- oder sogar Multifaktor-Authentifizierung für die Mobile-Banking-Sicherheit zu nutzen, andererseits ist aber zu berücksichtigen, dass der Anwender auch nicht zu viel Zeit für die Überprüfung seiner Identität und Zugriffsrechte bei der Abfrage seines Kontostands oder bei der Durchführung einer Überweisung verlieren will. Die Kundenbeeinträchtigung kann ohne Abstriche hinsichtlich der Sicherheit etwa minimiert werden, indem die Anmeldung des Nutzers durch Verfahren wie Geolokation, verhaltensbasierende Authentifizierung oder Geräteidentifikation unterstützt wird, die transparent für den Nutzer im Hintergrund ablaufen und eine zusätzliche Sicherheitsebene bieten.

Insgesamt muss jedes Unternehmen im Hinblick auf die Einführung eines Authentifizierungsverfahrens die konkreten eigenen Anforderungen ermitteln und davon abgeleitet einen individuellen Lösungsansatz finden. Die Herausforderung für Unternehmen liegt dabei darin, eine Lösung zu finden, die einerseits hohe Sicherheit garantiert, andererseits aber auch eine positive User Experience bietet.

Fragen zu HID Global
E-Mail: hid@infinigate.de
Telefon: +49 89 89048-395

HPE ARUBA SICHERHEITSLÖSUNGEN FÜR DIE DSGVO

EINE 360 GRAD SICHT AUF PERSONEN, PROZESSE UND TECHNOLOGIEN

Um sensible Daten zu sichern, sind eine Reihe von organisatorischen Maßnahmen notwendig. Damit kann man feststellen, welche Daten verwendet und wo diese gespeichert werden. Es sind aber auch einige technische Lösungen notwendig, um die Anforderungen der Richtlinie im Unternehmen umzusetzen.

Insbesondere wurden 4 Bereiche identifiziert, wo HPE Aruba Produkt-Vorteile bietet:
- Zugang zu den Daten
- Datensicherheit
- Erkennung von Gefährdungen
- Reaktion auf Gefährdungen

Absicherung des Zugangs zum Netzwerk (Network Access Management): Die markt- und technologieführende Network Access Management Lösung Aruba Clearpass hilft als zentrales Authentifizierungs (AAA)– und Richtlinienwerkzeug den sicheren Zugang zum Netzwerk für Personen, Smart Devices und IoT-Geräte zu ermöglichen. Clearpass stellt durch Profile von Endgeräten sicher, dass Geräte und Personen den notwendigen Zugang im richtigen Ausmaß erhalten.

Mit Clearpass Exchange werden eine Vielzahl von Fremdherstellerlösungen aus den Bereichen WLAN, LAN, VPN, Firewall, SIEM, Endpoint Protection, MDM und EMM in dieses zentrale Produkt mit eingebunden. So sind informationsbasierte automatisierte Entscheidungen abhängig vom Kontext (Ort, Uhrzeit, Betriebssystem, Anwendergruppe…) jederzeit möglich. Werden Gefährdungslagen festgestellt, können mit Clearpass sofort Maßnahmen, wie zum Beispiel Quarantäne oder Abschalten des Zugangs, durchgesetzt werden.

Datensicherheit durch sichere Übertragung und Sichtbarkeit: Viele Unternehmen sind mittlerweile international verteilt und verfügen über Zweigniederlassungen und mobile Mitarbeiter. Hier ist es die besondere Aufgabe, die sichere Übertragung von Daten im WLAN, LAN und mittels VPN sicherzustellen. Aruba Produkte für die Vernetzung von Niederlassungen sowie Anbindung von Heimarbeitsplätzen und mobilen Mitarbeitern sorgen für die nötige Sicherheit und einfache Implementierung. Eine neue Generation von Core Switchen (Aruba Secure Core) sorgt mit einer Security Analytics Engine für die notwendige Sichtbarkeit von Vorgängen im Netzwerk und erzeugt Entscheidungsgrundlagen im Gefahrenfall.

BILD: HPE/ARUBA

Die Europäische Datenschutz-Grundverordnung ist ab 2018 die neue Grundlage für den Datenschutz. Sie wird kurz „DSGVO" oder aus dem Englischen „General Data Protection Regulation" („GDPR") genannt.

Erkennungen von Gefährdungen und Reaktionen auf Gefährdungen: Aruba Introspect bedient sich der neuesten Technologien wie Machine Learning und Big Data Analysis, um normales Verhalten von Benutzern und Geräten (UBEA User and Entity based Behavior Analysis) zu erkennen und kann bei abweichendem Verhalten die Risiken bewerten und alarmieren. Durch die Integration mit Aruba Clearpass kann dieses Verhalten automatisiert sichtbar gemacht und auch unterbunden werden. Natürlich stehen dann auch genaue Dokumentationen zur Verfügung, um im Fall einer Sicherheitsverletzung, wie von der Sicherheitsrichtlinie gefordert, sowohl die Behörden als auch die betroffenen Personen im vollen Umfang in kürzester Zeit informieren zu können.

HPE Aruba 360 Secure Fabric – Netzwerk-Sicherheit in Zeiten von Mobile, Cloud und IoT: Mit 360 Secure Fabric verändert HPE Aruba den Security Markt. Dabei handelt es sich um ein Sicherheitsframework für Unternehmen, das den Sicherheits- und Netzwerkteams eine integrierte, umfassendere Methode zum Erreichen vollständiger Transparenz und Kontrolle über ihre Netzwerke bietet.

Infinigate und HPE Aruba unterstützen unsere Partner bei der Weiterentwicklung ihres Geschäftes mit Hilfe der Infinigate TechServices (Presales und Professional Service), Marketing-Services und DistributionServices.

WIE SECURITY-TECHNOLOGIEN DIE DSGVO-COMPLIANCE UNTERSTÜTZEN KÖNNEN

CIOs und CISOs haben nun genug Argumente, Ressourcen für wichtige Sicherheitstools zu erhalten, die dem ganzen Unternehmen einen größeren Schutz versprechen sowie „fast nebenbei" die Compliance für die neue Datenschutzverordnung unterstützen. Allerdings gilt es zu beachten, dass es nicht DIE EINE Lösung für Compliance gibt.

BILD: MCAFEE

Die EU-Datenschutzgrundverordnung bedeutet für Unternehmen einen enormen Schub in Sachen IT-Sicherheit und eine große Chance, eine Kultur der Datensicherheit zu etablieren.

Das neue DSGVO-Regelwerk setzt voraus, dass Unternehmen jederzeit wissen, wo ihre Daten lagern und wer darauf zugreifen kann. Im Rahmen der Datenstrukturierung und Protokollierung empfiehlt sich daher eine Lösung zur Data Loss Prevention (DLP). Diese erfasst die unternehmensweiten Daten, erkennt, wo diese lagern und ermöglicht des weiteren eine Festlegung, wer darauf zugreifen kann. Dadurch unterstützt sie die Kontrolle darüber, wer berechtigt ist, auf Daten zuzugreifen und diese weiterzuleiten. Ebenso ermöglichen DLP-Lösungen, Datenströme zu filtern und zu schützen. Allerdings gilt es, andere Technologien wie das Identity Management oder Verschlüsselung zu integrieren. Zusätzlich können Database Security-Lösungen zur Datenbanksicherheit beitragen. Ein Vulnerability Manager for Databases erkennt beispielsweise automatisch alle Datenbanken im Netzwerk, ermittelt, ob die neuesten Patches installiert wurden, prüft die Datenbanken auf häufige Schwachstellen und bietet so einen vollständigen Überblick über deren Sicherheitslage. Unternehmen sind so in der Lage, Transparenz herzustellen und ihre Datenmengen zu lokalisieren, zu strukturieren sowie Zugriffsberechtigungen zu verteilen.

Neben dem Schutz von Daten besteht ein weiterer Teil der DSGVO-Vorschriften darin, Kompromittierungen zu erkennen und an die zuständigen Behörden weiterzugeben. Das Security Information and Event Management (SIEM) ist in der Lage, komplexe, weitverzweigte Infrastrukturen zu kontrollieren, zentral zu verwalten und Richtlinien zu implementieren. Auf einem Dashboard erhalten Mitarbeiter Echtzeit-Einblicke in die IT-Systeme. So lässt es sich Sicherheitsverletzungen und Datenverlusten schneller auf die Spur kommen, weil das System automatisiert Vorfälle meldet, protokolliert und nach Priorität ordnet. IT-Mitarbeiter müssen daraufhin feststellen, ob es sich bei dem Vorfall um ein Ereignis handelt, das laut DSGVO-Richtlinien weitergegeben werden muss. Dies entlastet die IT-Teams und erlaubt ihnen, sich ganz auf sogenanntes Threat Hunting, also die Identifizierung von potentiellen Gefahren, zu fokussieren.

Wer seine Anwendungen aus On-Premises-Umgebungen in die Cloud migrieren möchte, kommt auch hier nicht umhin, seine Datenschutz-Richtlinien auf „as-a-Service"-Angebote auszuweiten. Cloud Access Security Broker (CASB), wie von der kürzlich von McAfee akquirierten Firma Skyhigh Networks, erfreuen sich in diesem Zusammenhang großer Beliebtheit. Als Zugriffskontrolle zwischen Cloud und Nutzer kontrollieren CASBs Zugriff auf Cloud-Dienste. Mit ihrer Hilfe lassen sich Sicherheits- und Compliance-Richtlinien aus dem Unternehmen auf Cloud-Dienste ausweiten. Zudem erlauben sie das Zuweisen von Zugriffsautorisierungen und eine automatisierte Bedrohungserkennung in Cloud-Diensten.

Im Bereich DSGVO unterstützt McAfee die gestärkten IT-Sicherheitsbereiche Integrität, Verfügbarkeit sowie Vertraulichkeit und bildet mit einer gesamtheitlichen Sicherheitsarchitektur die Basis für einen umfänglichen IT-Grundschutz. Die offene Sicherheitsplattform ermöglicht Unternehmen eine gesamtheitliche Sicht auf deren komplette IT-Sicherheitsinfrastruktur, indem sich nicht nur McAfee-Lösungen, sondern auch Technologien anderer Hersteller einbinden lassen. Auch wenn sie vielen noch wie ein vielköpfiges Monster erscheint, ist DSGVO für Unternehmen unter dem Strich doch ein Segen: Wer weiß, wie er mit den persönlichen Daten von Mitarbeitern und Kunden umzugehen hat und dies konsequent in die Tat umsetzt, braucht sich keine Gedanken über schwer einzuschätzende Risiken machen, die in personenbezogenen Datenbeständen lauern könnten.

BullGuard auf Partnersuche

Der renommierte Experte für Cybersecurity, BullGuard, hat sich in den letzten zwei Jahren zum Komplettanbieter für IT-Sicherheit im vernetzten Zuhause entwickelt. Für den weiteren Wachstumskurs sucht das Unternehmen aktuell weitere Fachhändler. Wir sprechen mit Stefan Wehrhahn, Country Manager DACH.

BILD: BULLGUARD

Ansprechpartner

Stefan Wehrhahn
Country Manager DACH
Mobile: 0173 3 64 74 89
Email: stefan.wehrhahn@bullguard.com

Oktay Cayiroglu
Senior Sales Manager DACH
Mobile: 0160 1 67 72 31
Email: oktay.cayiroglu@bullguard.com

Herzlichen Glückwunsch zum Erfolg von BullGuard bei Stiftung Warentest. Was tut sich gerade bei BullGuard?
Wir haben im letzten Jahr basierend auf dem Feedback unserer Kunden und auf den neuesten Entwicklungen im Bereich Cybersicherheit unsere Lösungen komplett überarbeitet: Wir haben nicht nur eine neue Firewall entwickelt, sondern zum Beispiel auch unsere verhaltensbasierte Anti-Malware-Engine neu aufgesetzt. All diese Innovationen haben dazu geführt, dass wir in diversen Tests von unabhängigen Instituten mit Bestnoten ausgezeichnet wurden: AV Comparatives aus Österreich hat uns den Gold-Award für besonders starken Malware-Schutz verliehen. Stiftung Warentest hat uns mit der Gesamtnote 1,9 zu den drei besten Sicherheitsprogrammen gewählt. Und ComputerBILD zählte BullGuard kürzlich zu den ‚Trusted Solutions 2018'.

Wie wirken sich diese Ergebnisse auf die Zusammenarbeit mit dem Channel aus?
Lösungen, die von unabhängiger Stelle gut bewertet werden und bekannt sind für ihre Zuverlässigkeit, sind für unsere Partner natürlich besonders attraktiv. Die Zusammenarbeit ist dabei ein Erfolg für beide Seiten: Wir profitieren vom umfassenden Netzwerk, während unsere Partner ausgezeichnete Produkte vertreiben können. Ein weiteres Plus ist unser lukratives Partnerprogramm: Jede Handelsstufe – egal welcher Größe – profitiert dabei. Distributionspartner erhalten 15 Prozent, Wiederverkäufer 25 Prozent Umsatzbeteiligung, auch wenn die einmal verkaufte Lizenz online direkt bei BullGuard verlängert wird. Bis zu 85 Prozent unserer Kunden verlängern ihre installierte Sicherheitssoftware.
Eine einmal verkaufte Lizenz läuft im Durchschnitt 4,5 Jahre, da können Sie sich vorstellen, wie erfolgreich das für unsere Partner ist.

Wie sehen Ihre Fachhandelspläne aus?
Wir konnten in den vergangenen Monaten einige neue Distributoren an Bord holen, die der Grundpfeiler für unsere Zusammenarbeit mit dem Channel sind, darunter Siewert & Kau, ALSO oder Avanquest. Gleichzeitig bauen wir gerade unser Geschäft in der Schweiz und Österreich aus. Da wir in der gesamten DACH-Region auf Wachstumskurs sind, freuen wir uns natürlich über weitere Partner. Wir setzen voll auf den Fachhandel!

Wie geht es bei BullGuard in den nächsten Monaten weiter? Was ist geplant?
Wir haben uns in den letzten zwei Jahren von einem traditionellen Virenschutz-Anbieter für Privatanwender zu einem führenden Unternehmen im Bereich Cybersecurity entwickelt. Über den klassischen Virenschutz hinaus haben wir heute Lösungen für die Sicherheit im Smart Home in unsere Produkte integriert, wie etwa den Heimnetzwerk-Scanner in der Software ‚BullGuard Premium Protection'. Damit haben wir uns an die Spitze der Cybersecurity-Komplettanbieter im Privatanwenderbereich positioniert.
Darüber hinaus wird es im Laufe des Jahres auch eine weitere Neuerung im Produktsegment geben: Zusammen mit unserem Partner Dojo Labs arbeiten wir an der Sicherheit im Internet der Dinge. Demnächst werden wir auch hier in Deutschland eine entsprechende Hardware-Lösung vorstellen, um das vernetzte Zuhause vor Angriffen von außen zu schützen. Dafür haben wir Ende Februar auf dem Mobile World Congress in Barcelona den Preis „Best Connected Consumer Electronic Device" bekommen.

[www.bullguard.com]

WIR WOLLEN SIE!

- Haben Sie ein Ladengeschäft?
- Haben Sie einen Online-Shop?
- Wollen Sie BullGuard zu Ihren Hardware-Produkte bundeln?

DANN SCHREIBEN SIE UNS EINE NACHRICHT:
sales_de@bullguard.com

AV comparatives MALWARE PROTECTION 2017 GOLD

Stiftung Warentest test GUT (1,9) Ausgabe 3/2018 www.test.de 18RY14

Computer Bild TRUSTED SOLUTIONS ★★★★★ 2018 BullGuard IN DER KATEGORIE INTERNET & CYBER SECURITY

Neben den einfach anzuwendenden, preisgekrönten Produkten, die Ihre Kunden lieben werden, profitieren BullGuard-Vertriebspartner auch von einem einmaligen Partner-Programm, das Sie zum Umdenken anregen wird:

- Hohe Gewinnspannen
- 25 % Umsatzbeteiligung auf sämtliche Lizenzverlängerungen
- Partner- und Kunden-Support in deutsch
- Direkte Ansprechpartner bei BullGuard
- Kostenlose POS-Materialien für Ihr Geschäft oder Ihren Online-Shop

JETZT anmelden!

www.bullguardadvantage.de

www.facebook.com/bullguarddeutschland/

BullGuard®

Erhältlich bei folgenden Distributoren

ALSO api COMPUTERHANDELS GMBH Avanquest® CES wir machen IT möglich! Siewert & Kau Distribution – live THALI

Micron NVMe SSDs bei dexxIT

NEUE SPEICHERLÖSUNGEN REVOLUTIONIEREN DEN STORAGEMARKT

BILD: DEXXIT

Die Nachfrage nach leistungsstarken Speichern mit hoher Kapazität steigt auch in 2018 rapide an. Bislang sorgten traditionelle Storagelösungen in unzähligen Racks für die notwendige Speicherkapazität, zusammen mit Hochleistungs-SSDs für den schnellen Zugriff auf ausgewählte Daten.

Mit innovativen NVMe SSDs der Micron 9200er Serie bietet dexxIT Fachhandel und Benutzern nun auch flashbasierte Technologien mit großer Kapazität an, die bis zu 11 TB Daten bei geringem Platz- und Energiebedarf umfassend und schnell speichern, verwalten und bereitstellen.

Jeden Tag werden weltweit 2,5 Exabyte Daten produziert, bearbeitet und vertrauensvoll genutzt. Rechenzentren, Systemdesigner und Geschäftskunden benötigen leistungsstarke Speicherlösungen, die auch große Datenmengen sicher verwalten und schnell zur Verfügung stellen. „Bis 2017 lag der Fokus beim Einsatz von Flash- und SSD-Speichern auf der richtigen Balance zwischen Kapazität, Performance und den Kosten", so Hans-Jürgen Schneider, Vertriebsleiter dexxIT „Die Zukunft wird jedoch NVMe gehören, da diese Technologie den Datenspeicher-Engpass beendet."


BILD: DEXXIT

Hans-Jürgen Schneider, Vertriebsleiter dexxIT

Die Vorteile von NVMe: Während in den Jahren 2011 bis 2015 die Kapazität einer einzelnen PCIe SSD jährlich von 0,7 auf 3,2 TB verdoppelt werden konnte, sprang dank der Kombination von 3D NAND und Architekturinnovationen mittlerweile die maximale Kapazität einer NVMe SSD mit U.2-Formfaktor (2,5 Zoll) mittlerweile auf 11 TB. Da seit 2015 Standardserver problemlos 24 U.2 NVMe SSDs in einem 2U-Design unterstützen, steigern diese die Workload-Leistung für das Rechenzentrum durch die Bereitstellung von großer Bandbreite und geringer Latenz erheblich. Gleichzeitig verringern sich Platzbedarf und Energiekosten, wie das folgende Rechenbeispiel aufzeigt:

- Um in einem Rechenzentrum beispielsweise einen großen Datendurchsatz von 50 PB schnell und sicher zu gewährleisten, waren in den vergangenen Jahren bis zu 510 Racks mit PCIe SSDs notwendig. Bei der Verwendung einer 11 TB NVMe SSD beispielsweise von Micron werden nur noch 9,5 Racks benötigt. Somit lassen sich mehr Daten auf deutlich weniger Platz speichern.

- Parallel zur Kapazitätssteigerung der einzelnen SSDs verringert sich der Gesamtenergiebedarf beim Speichern der 50 PB von 1.828,6 kW auf gerade einmal 139,9 kW, was knapp 7,7 Prozent der früheren Kosten entspricht. Hinzu kommen die reduzierten Kühlkosten.

Einsatzmöglichkeiten für NVMe Lösungen: NVMe SSDs wie die Micron 9200-Serie eignen sich für Rechenzentren, große Unternehmensorganisationen, öffentliche Einrichtungen sowie Anbieter von Cloud-Diensten. Sie können als neue, modular ausbaubare Storage-Lösung eingesetzt werden oder bestehende IT-Altsysteme mit voluminösen Racks voller HDDs modernisieren, konsolidieren und vereinfachen. Sie bieten eine zukunftsorientierte Plattform, mit der Nutzer die kombinierten Anforderungen des Datenwachstums und des Echtzeit-Zugriffs zuverlässig erfüllen können.

Schneller Speicher – positiver ROI: Die Investition in innovative NVMe SSDs zahlt sich schnell aus. Statt wie bisher kleine Teile von Daten durch traditionelles Caching zu beschleunigen, bieten NVMe SSDs mit hoher Kapazität die Möglichkeit, ganze Datensätze in Echtzeit zu verarbeiten. Die Beschleunigung der Anwendungen und Datenlieferung sorgt für ein besseres Endergebnis und reduziert die Ressourcenverschwendung bei alten, langsamen Speichersystemen sowie das Arbeitsaufkommen der IT-Mitarbeiter. Statt zeitaufwändig den reibungslosen Betrieb riesiger Serverfarmen aufrecht zu erhalten, können die IT-Experten sich um geschäftskritische Projekte kümmern. Weitere, dauerhafte Einsparungen bieten die einfache Systempflege und Implementierung von verteilten Anwendungen sowie der geringere Stellplatz- und Energiebedarf.

[www.dexxit.de]

dexxIT

Ihr kompetenter Enterprise SSD-Partner!

DIGITAL IMAGING | TV & AUDIO | COMPUTER & CO | STORAGE | HOME & LIVING | DIGITAL SIGNAGE

ChannelPartner Preferred Distributor 2017 – Spezial-Distribution

CRN 2018 Excellent Distributor

IT-BUSINESS DISTRI AWARD 2018 GOLD – KOMPONENTEN

www.dexxit.de

Bestellung und Beratung unter Tel. 0931 9708 496

dexxIT GmbH & Co. KG | Alfred-Nobel-Straße 6 | 97080 Würzburg

ECTACOM UND KASPERSKY LAB:
SENSIBILITÄT IST GEFRAGT!

Cyber-Angriffe auf Unternehmen sind nicht immer nur neuesten Hacker-Methoden geschuldet, sondern auch dem eigenen Verhalten. Wer nicht sensibel mit Passwörtern umgeht, öffnet Tür und Tor für jeden, der spionieren oder zerstören möchte. Security Awareness ist von der Geschäftsführung bis hin zum Mitarbeiter unumgänglich.

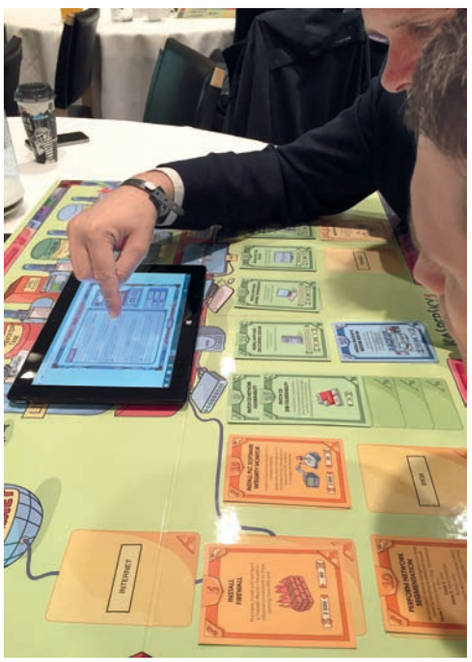


BILD: KASPERSKY LAB

Immer mehr Cyber-Angriffe erfolgen unter Zuhilfenahme gestohlener Passwörter. Geschuldet ist das der Annahme, dass klassische und teure Sicherheitslösungen hier Abhilfe schaffen würden. Wer Standardpasswörter, Zahlenkombinationen wie den eigenen Hochzeitstag oder andere leicht zu erratende Pins nutzt, überschätzt die Fähigkeiten der IT und unterschätzt böswillige Angreifer. Eine weitere Schwachstelle: Gutgläubigkeit. Zu häufig vertrauen wir E-Mails scheinbar bekannter Absender, ohne nach der Legitimation zu fragen.
Der aufmerksame und sensible Umgang mit der IT genügt, um die Anzahl der Sicherheitsvorfälle zu reduzieren. Security Awareness muss jedoch geschult werden. Schließlich arbeiten auch Mitarbeiter innerhalb des Unternehmens, die sowohl beruflich als auch privat kaum Berührungspunkte mit IT-Sicherheit haben.

Kaspersky Lab bietet eine Schulungsplattform, auf der der sichere Umgang mit IT-Security aufgezeigt und neues Wissen aufgebaut wird. Dabei muss kein technologisches Know-how vorliegen, denn es geht um ganz Grundlegendes.

- Passwortsicherheit: Tipps und Tricks zum Erstellen und zur sicheren Aufbewahrung von Passwörtern.
- Social Engineering: Mitarbeiter lernen, wie sie häufige Social-Engineering-Taktiken erkennen und Angriffe vermeiden.
- E-Mail-Sicherheit: Benutzer lernen, wie sie Phishing-Fallen wie betrügerische Links, Anhänge und Informationen in E-Mails erkennen.

Dabei unterstützt eine Online-Schulung von ectacom und Kaspersky Lab. In über 27 Modulen werden Mitarbeiter in Unternehmen spielerisch und anschaulich mit dem Thema Sicherheit betraut, um effektiv und interaktiv Wissen aufzubauen. Zunächst wird ein Cyber-Strength-Assessment durchgeführt, bei dem der Kenntnisstand jedes Nutzers und somit sein Schulungsbedarf ermittelt werden. Dieser variiert häufig, denn je nach Position ist anderes Wissen gefragt. Führungskräfte, Bereichsleiter, Belegschaft oder Security Officer können zusätzliche Intensiv-Schulungen von den Kaspersky-Trainern erhalten. Ist diese Basis geschaffen, werden mithilfe der Online-Trainingsplattform Schulungspläne erstellt, die einzelnen Nutzern oder Gruppen zugewiesen werden. So werden innerhalb der Online-Schulungsmodule von Passwort-Sicherheit und Anti-Phishing über Datenschutz und Datenzerstörung bis hin zum Umgang mit sozialen Netzwerken oder dem sicheren Browsen sämtliche Szenarien durchgespielt. Individuelle Lehrpläne sind darüber hinaus möglich – gemäß Sicherheitsbereichen, Bedrohungslandschaften und Kenntnisstand.

Kaspersky CyberSafety Awareness Trainings structure

BILD: KASPERSKY LAB

Um den Lernfortschritt der Nutzer zu überprüfen, können simulierte Phishing-Attacken durchgeführt werden, die eine schnelle Reaktion erfordern. Dazu greifen Unternehmen auf anpassbare Vorlagen für Phishing-E-Mails zurück. Wird geklickt? Dann ist weiterer Schulungsbedarf vorhanden und dem Mitarbeiter kann automatisch das entsprechende Modul zugewiesen werden. So wird er sensibilisiert und vertrauenswürdige Daten werden effizienter geschützt. Dies ist auch im Hinblick auf die DSGVO wichtig. Und auch dafür gibt es ein gesondertes Modul.

Wo Mitarbeiter durch modulare Schulungen für Cyber-Gefahren sensibilisiert werden, wird auf der Führungsebene mit Unternehmensplanspielen gearbeitet. Hierbei wird ein technologischer, realitätsnaher Prozess dargestellt und unter dem Aspekt der Cybersecurity betrachtet. Mögliche Attacken, Handlungsempfehlungen, Budget, Best-Practice-Ansätze: All dies sind Bestandteile des Trainings-Angebots. Mithilfe der Cybersecurity-Awareness-Schulungen von Kaspersky Lab erhalten Führungskräfte die Möglichkeit, sich auf einen Cyber-Angriff vorzubereiten, Maßnahmen zu simulieren und Incident-Response-Konzepte zu erarbeiten.

ectacom GmbH
[www.ectacom.com/Security-Awareness]

ectacom
trusted it-advisor – anywhere and anytime

KASPERSKY lab
DISTRIBUTOR

UPPS!

Sie sind auf einen **Phishing-Angriff hereingefallen!**

Schulen Sie Ihre Mitarbeiter und Kunden, damit Ihnen das nicht passiert!

KASPERSKY SECURITY AWARENESS

Interaktive Schulungsprogramme,
die den Aufbau einer sicheren Cyberumgebung
im Unternehmen ermöglichen.

Hier die Broschüre laden:

www.ectacom.com/Security-Awareness

EIN SICHERES GESCHÄFT FÜR DEN CHANNEL:

ESET MANAGED SERVICES

BILD: ESET

Die Nachfrage nach Managed Services boomt – vor allem im Bereich IT-Sicherheit. Der europäische Security-Hersteller ESET gehört mit seinem MSP-Programm zu den Top-Anbietern auf dem Markt. Das Unternehmen bietet ein lukratives Geschäftsmodell und setzt sich damit erfolgreich von den Mitbewerbern ab. Mit seiner „Add-On-Philosophie" und Mehrwertstrategie erhalten bestehende und neue ESET MSPs kräftig Rückenwind.

IT-Security wird immer komplexer und zunehmend zum Schlüssel für geschäftlichen Erfolg von Firmen. Folglich wächst bei Unternehmensentscheidern der Bedarf an individuellen IT-Sicherheitskonzepten. Mit klassischem Produktverkauf stoßen herkömmliche Systemhäuser im traditionellen Hardware-Geschäft langsam aber sicher an ihre Grenzen. Sie verlieren mittlerweile massiv Kunden und erleiden finanzielle Einbußen. Neben einem stetig wachsenden Kundenkreis, mehrfach ausgezeichneten Produkten und schnellem Return on Investment profitieren angehende und bestehende ESET MSPs vom kompletten Leistungs- und Serviceumfang, von Allianzen, jahrelangen Erfahrungen im IT-Markt sowie professioneller Marketing- und Vertriebsunterstützung seitens ESET.

5 gute Gründe, MSP-Partner bei ESET zu werden:

1. Breites Produkt- und Service-Portfolio

Managed Service Provider haben vollen Zugriff auf die individuellen Dienste und Lösungen des Herstellers. Neben Antimalware-Produktklassikern für Unternehmen stellt ESET auch ein Mobile Device Management für mobile Geräte sowie eine Reihe an zeit- und kostensparenden Administrations- und Verwaltungstools bereit. In 2018 wird sich das MSP-Portfolio in Richtung Softwareauthentifizierung und Verschlüsselung erweitern.

2. Höhere Wettbewerbsfähigkeit

Mit Zugriff auf das komplette ESET Produkt- und Service-Portfolio sind Fachhändler in der Lage, Ressourcen und Knowhow verfügbar zu machen, um kompetent auf den Bedarf im Markt zu reagieren. Kleinere und mittelgroße Reseller oder Systemhausverbünde mittelständischer Systemhäuser können auf diese Weise neben den großen Platzhirschen interessante, wettbewerbsfähige Konzepte und Lösungen entwickeln.

3. Dynamisches Lizenzmodell

Im Gegensatz zu vielen anderen Anbietern am Markt setzt ESET auf ein dynamisches Lizenzmodell. Vor allem für kleinere und mittelgroße Partner ist das ein Gewinn, da das Einstiegsrisiko minimal bleibt. An Stelle von statischen Volumenlizenzmodellen und Mindesteinstiegsgrößen zahlen Partner nur tatsächlich genutzte Lizenzen Ihrer Kunden. Durch die fehlende Vorfinanzierung und ohne Vertragsbindung bleiben die kommerziellen Risiken für Reseller extrem überschaubar.

4. Tschüss Einmalumsätze, hallo Kundenbindung

Als ESET Managed Service Provider sind Fachhändler in der Lage, als professionelle Dienstleister die komplette oder teilweise Abwicklung Ihrer IT-Security zu übernehmen. Statt einmaliger Lizenzverkäufe wie im klassischen Produktverkauf wird Managed Services zum Instrument der Kundenbindung und regelmäßiger Umsätze. Denn Unternehmen lassen den Betrieb ihrer IT-Security über MSPs abwickeln, um die Verantwortung für Support, Ressourcen und Haftungsrisiken abzugeben. Aus Firmensicht ist der Aufbau einer eigenen IT-Abteilung in vielen Fällen weitaus teurer als Outsourcing.

Vom tagesgenauen Abrechnungsmodell von ESET profitieren beide Seiten: Channel und Kunde zahlen nur für in Anspruch genommene Leistungen. So bleiben Kosten für alle transparent und kalkulierbar.

5. Individual Security: Maßgeschneiderte Produkte und Services vom Spezialisten

Wie schnell und in welche Richtung sich die Bedrohungslage auch ändert: Managed Service Provider haben die Malware-Trends im Blick und können so die Netzwerke ihrer Kunden optimal schützen. Hinzu kommen die enge Zusammenarbeit zwischen Partner und Hersteller und der direkte Zugriff auf dessen Knowhow, Dienste und Lösungen.

Mit der 30-jährigen Erfahrung, mehr als 1500 Mitarbeitern und 110 Millionen geschützten Anwendern gehört ESET zu den Top-Anbietern im Bereich Technologie und Gefahrenabwehr.

Weitere Informationen zum ESET MSP-Programm finden Sie hier:
[www.eset.de/msp]

ESET MSP PROGRAM

www.eset.de

Automatisierung der Extraklasse

Wir bieten die Tools und das Know-how, mit denen Sie noch erfolgreicher werden! Lehnen Sie sich zurück und verdienen Sie Geld – wir machen die Arbeit!

Warum bei ESET? Weil es sich lohnt.

- Tools zur Automatisierung und Steigerung Ihrer Effizienz
- Tagesgenaue Abrechnung, nachträgliche monatliche Rechnung
- Pausieren von Lizenzen
- Einfache Integration von API & RMM Plug-ins
- Kostenfreier Support aus Deutschland
- Privatgeführter europäischer Hersteller
- Beste Performance auf allen Systemen
- Problemlose Bedienbarkeit dank innovativer GUI

Wir haben Ihr Interesse geweckt? Weitere Infos finden Sie unter: www.eset.de/msp oder schreiben Sie eine E-Mail an: partner@eset.de

Plugins und Integrationen:

Kaseya · ConnectWise · Autotask · Tigerpaw · ConnectWise AUTOMATE formerly LabTech · salesforce

BESSERE BETREUUNG, NOCH NÄHER AM PARTNER:

G DATA VERDOPPELT SEINE AUSSENDIENSTMANNSCHAFT IN DEUTSCHLAND

G DATA setzt seit langem auf dieses Erfolgsrezept und verstärkt sein Engagement jetzt deutlich mit dem Ziel, die Fachhandelspartner noch besser zu unterstützen und ihnen zu mehr Umsatz zu verhelfen. Der Hersteller von IT-Security-Lösungen „Made in Germany" steht weiterhin klar zum indirekten Vertriebsmodell.

100-prozentig partnerorientiert: Eine optimale Betreuung der Fachhandelspartner vor Ort erfordert viel Zeit. Daher verdoppelt G DATA seine Außendienstmannschaft in Deutschland, um noch besser auf die Bedürfnisse der Partner eingehen zu können. Künftig sind die Kundenakquise und das Partnermanagement voneinander getrennt. In jeder der sechs Vertriebsregionen ist jetzt ein „Partner Sales Manager" unterwegs. Dieser besucht nicht nur die großen Systemhäuser, sondern auch speziell die kleinen Fachhändler, die in Vergangenheit insbesondere durch den Innendienst versorgt und beraten wurden. So profitieren auch diese Partner von einer bedarfsorientierten Vor-Ort-Betreuung direkt durch den Hersteller und können sich beispielsweise die Unterstützung bei Kundenprojekten sichern – so ist ein noch größerer Erfolg im Markt vorprogrammiert.

Die Neukundenakquise wird jetzt durch spezielle „Corporate Sales Manager" durchgeführt. Diese generieren hierdurch neue Aufträge, die ausnahmslos an qualifizierte Partner zur Umsetzung weitergegeben werden. Fachhandelspartner, die die nötigen Voraussetzungen mitbringen, haben von der Zusammenarbeit mit G DATA so einen weiteren Vorteil.

Qualifizierungsangebote für Partner: Fachhändler sind insbesondere dann erfolgreich, wenn sie über das nötige Wissen und die Qualifikationen verfügen. Genau damit stattet G DATA seine Partner aus und versorgt sie mit Hilfe eines umfangreichen Angebots von Online-Trainings und Zertifizierungen mit dem nötigen Rüstzeug für Kundenprojekte.
Darüber hinaus unterstützt der deutsche IT-Security-Hersteller Händler durch seinen 24-Stunden-Support an sieben Tagen in der Woche und lässt sie so beispielsweise bei der Implementierung am Wochenende außerhalb normaler Betriebszeiten nicht im Regen stehen.

BILD: G DATA

Eine umfassende Betreuung und Unterstützung direkt vom Hersteller ist für Systemhäuser und Fachhändler entscheidend, um im Channel zu punkten und Endkundenprojekte erfolgreich durchzuführen.

G DATA-Garantie: Fachhandelspartner und Unternehmen können sich auf G DATA verlassen: Der deutsche IT-Security-Hersteller tritt für höchste Sicherheitsstandards ein und garantiert, dass alle Informationen ausschließlich in Deutschland verbleiben und vor dem Zugriff Dritter geschützt sind. Dabei wird die Erhebung von Telemetriedaten auf ein Minimum reduziert. Dafür steht G DATA mit „Meine Daten bleiben in Deutschland".

Gerade für mittelständische Unternehmen ist dies besonders wichtig, wie das G DATA Business IT-Security Barometer ergibt: Neun von zehn deutsche Mittelständler finden es wichtig oder sehr wichtig, dass ein IT-Security-Hersteller die Daten ausschließlich in Deutschland verarbeitet. Entscheidend ist außerdem, dass die Sicherheitslösungen des Bochumer IT-Security-Experten keine Hintertüren für Geheimdienste oder andere Behörden enthalten – für einen umfassenden und effektiven Schutz vor Online-Bedrohungen.

Meine Daten bleiben in Deutschland.

gdata.de/virenschutz

Und nirgendwo sonst. Deutscher Hersteller, deutsche Datenschutzgesetze. G DATA hat sich dazu verpflichtet, keine Hintertüren für Geheimdienste offen zu lassen. Wir geben eine No-Backdoor-Garantie. Für echten Schutz vor Cyberkriminellen und Spionage. Ohne Kompromisse.

Setzen Sie jetzt auf die vielfach ausgezeichneten G DATA Businesslösungen
Mehr Infos auf **www.gdata.de/business** oder unter **0234 9762-170**

G DATA

TRUST IN GERMAN SICHERHEIT

DEM MSP-GESCHÄFT GEHÖRT DIE ZUKUNFT

Immer mehr Unternehmen investieren in Managed Services – besonders im Bereich Security. Diese Umsatzchance gilt es jetzt zu nutzen: Kaspersky Lab ermöglicht bestehenden und neuen Partnern einen schnellen Einstieg ins MSP-Geschäft.

Die Prognosen zeigen steil nach oben: Laut einer Studie von Market Research Future ist zu erwarten, dass der MSP-Markt im Zeitraum 2016 bis 2022 jährlich um durchschnittlich elf Prozent wächst und Ende 2022 einen Wert von etwa 245 Milliarden USD erreichen wird.

Kein Wunder, denn Entwicklungen wie die Verlagerung von Daten in die Cloud oder die zunehmende Virtualisierung sorgen für komplexere IT-Strukturen und treiben den MSP-Markt voran. Aber besonders Cybersicherheit kommt eine Schlüsselrolle zu. Denn täglich neue Bedrohungsfälle und gesetzliche Vorschriften – allen voran die DSGVO – stellen IT-Verantwortliche im Unternehmen vor enorme Herausforderungen. Für MSPs ist diese „Belastung" in der Sicherheitsverwaltung ein großes Umsatzpotenzial.

Leichter Einstieg ins MSP-Geschäft: Doch wie viele Fachhändler setzen bereits auf Managed Security Services und wie schätzen sie den Trend für die nächsten Jahre ein? Um darauf eine Antwort zu finden, führten Kaspersky Lab und Business Advantage eine Studie durch. Das Ergebnis zeigt, dass Sicherheitsleistungen mit 92 Prozent bereits heute am häufigsten Teil des Portfolios sind.

Es gilt also für Reseller und Fachhändler, möglichst bald ins MSP-Geschäft einzusteigen, wenn sie die Potenziale des Marktes ausschöpfen möchten. Hierbei unterstützt das MSP-Partnerprogramm von Kaspersky Lab. Es hilft bestehenden und neuen Vertriebspartnern, ihr Business auszubauen sowie neue Umsätze zu generieren.

Partnervorteile: MSP-Partner profitieren von der Kumulierung der Lizenzen, d.h. je mehr Lizenzen sie insgesamt verkaufen, desto geringer wird für sie der Einzelpreis. Dadurch lassen sich schnell und einfach höhere Roherträge erzielen.

Um im Security-Geschäft zu wachsen und flexibel auf Kundenbedürfnisse einzugehen, bietet das Kaspersky-Programm noch viele weitere Vorteile:

- Bessere Einkaufskonditionen durch Partnerstatus (Silver, Gold, Platinum)
- Flexible Lizenzierung: Wahl zwischen Monatsabonnements und Jahreslizenzen
- Pay per use: Rechnungsstellung nur für aktiv genutzte Lizenzen
- Einfache Erweiterung der Kundenbasis und Einsparung beim Vor-Ort-Service: Zentrale, remote Administration aller Lösungen über Web-basierte Konsole (mehrmandantenfähig)
- Schneller Einstieg mit KES Cloud: Keine zusätzlichen Infrastrukturkosten, vorkonfigurierte Standardrichtlinien, einfache Administration, 30-Tage-Trial, kostenfreie NFR-Lizenzen für Eigenbedarf
- Technischer Support: Kostenloser technischer Premium-Support für fünf Vorfälle inklusive, höchste Priorität bei schwerwiegenden Anfragen
- Sales- und Marketing-Unterstützung: Breit gefächertes Angebot an Vertriebs- und Techniktrainings, Bereitstellung von Marketingmaterial, Zertifizierungen für Servicetechniker

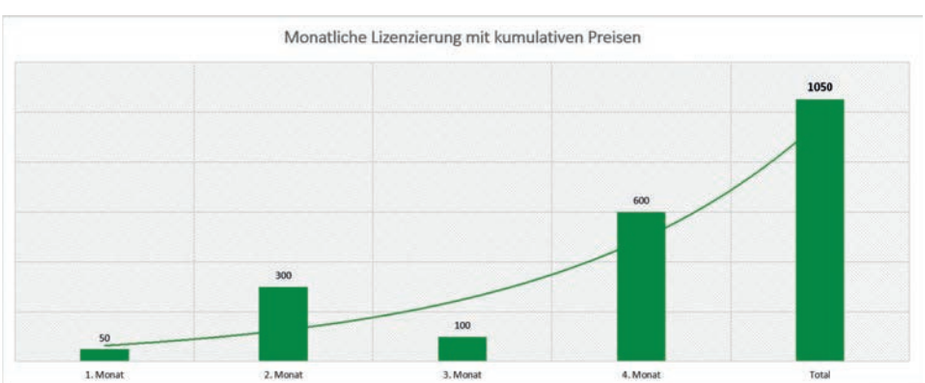


BILD: KASPERSKY LAB

MSP-Lizenzmodell mit volumenbasierten Rabatten

Distributionspartner: Der Lizenzeinkauf erfolgt über zertifizierte Kaspersky B2B Distributoren: 8Soft, acmeo, Also Deutschland, ectacom und Wick Hill.

KASPERSKY lab

In 3 Schritten zum MSP-Partner:

Mit nur drei Schritten können neue Partner am MSP-Programm von Kaspersky Lab teilnehmen:

1. Im Partnerportal registrieren
2. Distributor auswählen und
3. Technische Schulung absolvieren.

Wer bereits Partner ist, kann eine **MSP-Spezialisierung** beantragen.

Werden Sie MSP-Partner von Kaspersky Lab!

Weitere Informationen:

[www.kaspersky.de/partners/managed-service-provider]
[go.kaspersky.com/MSP_Partner.html]

Distributionspartner: acmeo cloud-distribution, ALSO, ectacom, NUVIAS, 8SOFT

Maximaler Profit. Minimales Risiko.

Werden Sie MSP Partner von Kaspersky Lab

Das MSP-Programm von Kaspersky Lab wurde entwickelt, um einen schnellen Einstieg in dieses attraktive Geschäftsfeld zu ermöglichen, Umsätze zu steigern und neue Kunden zu gewinnen. Ihre Vorteile:

- **Außergewöhnliche Margen**
- **Technischer Support für MSP-Partner**
- **Automatisiert verwalten mit RMM & PSA**
- **Vertriebs- und Marketingunterstützung**
- **Technik- und Vertriebsschulungen, Webinare und Support**

Mehr Informationen finden Sie unter: www.kaspersky.de/MSP

Zertifizierte MSP-Distributionspartner

**WIR SCHÜTZEN,
WAS IHNEN WICHTIG IST
-SEIT 20 JAHREN!**

DIE NEUE XANTO-USV: MEHR SICHERHEIT MIT DYNAMIC POWER TECHNOLOGY (DPT)

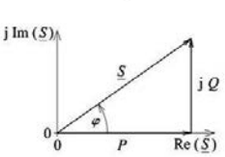
Die neue XANTO-Serie ist das Ergebnis der konsequenten Weiterentwicklung bewährter ONLINE USV-Konzepte. Mit ihrer Doppelwandler-Technik garantiert XANTO den höchsten Schutz vor Stromausfall und Datenverlust in Industrie und Rechenzentrum.

DPT
DYNAMIC
POWER
TECHNOLOGY

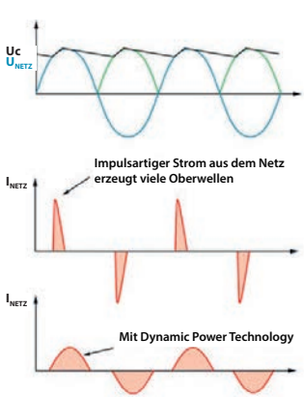
BILDER: ONLINE USV

XANTO ist von 700 VA bis 20.000 VA bei allen führenden Distributoren verfügbar. Als bahnbrechender Wandel in der USV-Branche gilt die neue und zukunftsweisende DYNAMIC POWER TECHNOLOGY (DPT) von ONLINE USV-Systeme.

Mehr Leistung mit DPT: Die DYNAMIC POWER TECHNOLOGY (DPT) passt die Leistung der USV-Anlage flexibel den angeschlossenen Verbrauchern an und stellt eine bis zu 54 Prozent höhere Wirkleistung (Watt) zur Verfügung als herkömmliche USV-Anlagen.
Hierdurch kann mit XANTO ein kleineres USV-Modell mit geringeren Anschaffungskosten eingesetzt werden. Gleichzeitig erreicht die USV-Anlage ihren optimalen Arbeitsbereich und reduziert Wärmeverluste. Dies schont die Umwelt und den Geldbeutel des Betreibers. Mit der DYNAMIC POWER TECHNOLOGY gibt es erstmals keinen Unterschied mehr zwischen der Nennleistung der USV-Anlage in VA und ihrer Wirkleistung in Watt.



Die Theorie: In Stromversorgungseinrichtungen wird zur Vermeidung von Übertragungsverlusten ein möglichst hoher Leistungsfaktor angestrebt. Im Idealfall beträgt er genau 1.
Häufig tritt trotz sinusförmiger Wechselspannung infolge nichtlinearer Verbraucher wie zum Beispiel Schaltnetzteilen in Servern ein „verzerrter" sinusförmiger Wechselstrom auf. Die Scheinleistung gliedert sich in einen Wirkleistungsanteil P und einen zusätzlichen Blindleistungsanteil Q. Der Blindleistungsanteil



Gewöhnliche Gleichrichterschaltungen erzeugen sehr viele Oberwellen.

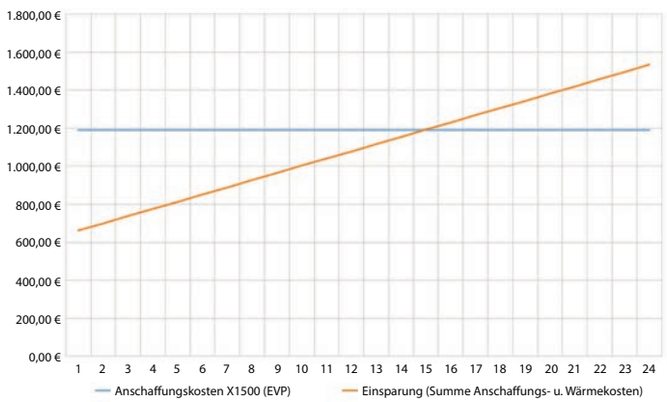
wird durch die Phasenverschiebung cos phi zwischen Strom und Spannung der Induktivität beziehungsweise der Kapazität verursacht.

Zusammen mit der Phasenverschiebung zwischen Spannung und Strom erzeugen diese Oberwellen eine Scheinleistung, für deren Erzeugung eine Überdimensionierung der Baugruppen notwendig ist.
Damit die Kosten für die Überdimensionierung und die Rückführung der unerwünschten Blindleistung nicht explodieren, hat die EU in mehreren Richtlinien eine Begrenzung vorgeschrieben. Diese regulieren eine zeitliche Verlängerung der Stromaufnahme aus dem Netz. Hiermit verringern sich Höhe und Geschwindigkeit des Stromanstieges, was gleichzeitig Anzahl und Höhe der Oberwellen reduziert. Dem Stromversorgungsnetz wird annähernd reine Wirkleistung entnommen.

Musterrechnung Kostenreduktion: Aufgrund der gesteigerten Wirkleistung kann meistens ein kleineres USV-Modell eingesetzt werden. Der Vorteil für den Anwender ist eine Einsparung bei den Anschaffungskosten von bis zu 34 Prozent gegenüber konventionellen USV-Anlagen. Zusätzliches Einsparpotenzial ergibt sich aus dem optimierten Wirkungsgrad mit einer Reduktion der Verlustleistung und der geringen Baugröße.

	Konventionelle USV	Moderne XANTO mit DPT
Leistung	2.200 VA / 1.540 W	1.500 VA / 1.500 W
Anschaffungskosten	**1.814,- €**	**1.190,- €**
Verlustleistung/Wärme	308 W	135 W
Jährliche Wärmekosten (Verlustleistung x t x 0,3 €/ kWh)	**809,- €**	**354,- €**

Kostenvorteil:	
Anschaffungskosten konventionelle USV	1.814,- €
./. Anschaffungskosten moderne XANTO mit DPT	-1.190,- €
Kostenvorteil Anschaffungskosten	**624,- €**
Wärmekosten konventionelle USV/ Jahr	809,- €
./. Wärmekosten moderne XANTO mit DPT/ Jahr	-354,- €
Kostenvorteil Wärmekosten/ Jahr	**455,- €**

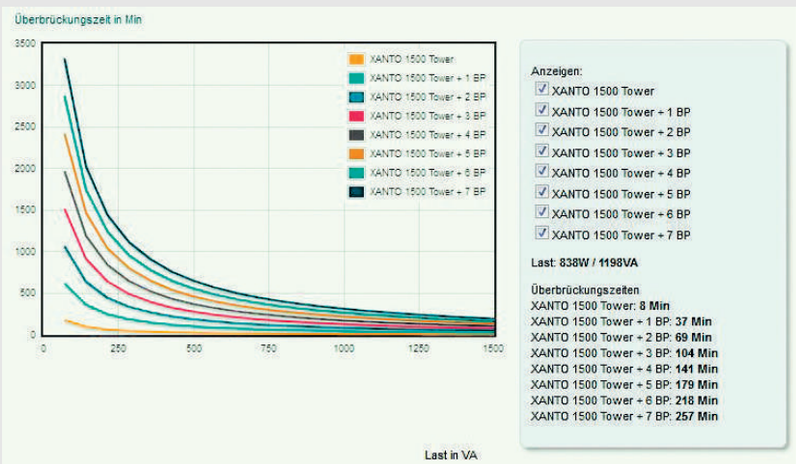


Aus der Summe beider Kostenvorteile resultiert eine Amortisation von 15 Monaten und damit weit vor Ablauf der Standard-Garantie.

Flexible Installation und vollumfängliche Information: Die innovative Geräteklasse von XANTO ist wahlweise als klassischer Tower oder im Rack-Tower-Kombidesign mit nur zwei Höheneinheiten erhältlich. Das Rack-Tower-Kombidesign ermöglicht flexible Installation, speziell nach Umzug oder Systemerweiterung. Das große Flüssigkristalldisplay von XANTO zeigt alle relevanten Informationen des Stromversorgungsnetzes und der USV-Anlage an. Die intuitive Menüführung ermöglicht eine einfach Programmierung. Alle USV-Anlagen von ONLINE USV beinhalten zwei Jahre Garantie inklusive Akku und 24-Stunden-Vorab-Austausch gegen Neugerät!

Für Beratung und Vertriebsunterstützung
steht das ONLINE USV-Team in München gerne direkt unter 089 / 242 3990 10 zur Verfügung.

Xanto 1500 Tower



Eine weitere Neuheit von XANTO

ist die Überbrückungszeit von bis zu 650 Minuten. Hiermit kann die USV-Anlage flexibel an die spezifischen Kundenbedürfnisse angepasst werden. Damit stellt auch das Herunterfahren großer Netzwerke oder die Sicherung umfassender Datenbestände kein Sicherheitsrisiko dar. Für diese hohe Überbrückungszeit können an eine XANTO bis zu sieben Batteriepakete angeschlossen werden.
Detaillierte Angaben zu den exakten Überbrückungszeiten bei individuellen Lasten finden Sie in den interaktiven Batteriekennlinien.

GEDEIHEN IN EINER UNSICHEREN, RISIKOREICHEN WELT

BILD: RSA

Trotz aller Bemühungen ist es schwierig, Sicherheitsdetails schnell genug in Geschäftszusammenhänge zu bringen, um Auswirkungen auf Businesskontinuität, persönliche Daten, geistiges Eigentum und Reputationsschäden ermitteln zu können. Bis jetzt.

RSA liefert anhand der „Business-Driven Security Strategie" transformative, geschäftsorientierte Sicherheitslösungen, die über 30.000 Kunden helfen, Sicherheitsvorfälle umfassend und schnell mit Geschäftskontexten zu verknüpfen, um effektiv zu reagieren und das Wichtigste zu schützen.

Mit preisgekrönten Lösungen für Identity & Access Management, Business Risk Management, Threat Detection & Response und Consumer Fraud Protection können RSA-Kunden in einer unsicheren und risikoreichen Welt weiter erfolgreich sein.

RSA-Lösungen halten Führungspositionen in vier Gartner Magic Quadrants und schützen über 50 Millionen Identitäten und über eine Milliarde Verbraucher weltweit. Mit über 700 engagierten Sicherheitsexperten und einer globalen Zusammenarbeit mit über 400 Partnern bietet RSA einheitliche Funktionen in den wesentlichen Bereichen einer effektiven, geschäftsorientierten Sicherheitsstrategie.

Das RSA-Lösungsportfolio umfasst wie folgt:

- Mit der **RSA SecurID® Suite** können Unternehmen jeder Größe ihr Geschäft beschleunigen und gleichzeitig das Identitätsrisiko minimieren, während sie modernen Mitarbeitern gleichzeitig einen bequemen und sicheren Zugang zu ihren wertvollen Ressourcen

bieten. Risikoanalysen und kontextbasiertes Bewusstsein werden wirksam eingesetzt, um sicherzustellen, dass die richtigen Personen von überall und von jedem Gerät aus den richtigen Zugriff haben.

- **Die RSA Archer® Suite** ist die führende Business-Risk-Management-Suite der Branche, die Kunden dabei unterstützt Risikobewältigung sicher voranzutreiben und zu verstehen, welche Risiken sich zu nehmen lohnen.

- **Die RSA NetWitness® Suite,** welche die Wirkung von Sicherheitsteams nahezu verdreifacht, indem sie die notwendige Transparenz bietet, Advanced Threats frühzeitig zu erkennen und in bereits wenigen Minuten entsprechend darauf reagieren zu können.

- **Die RSA® Fraud & Risk Intelligence Suite** ermöglicht Unternehmen, ihre digitale Multi-Channel-Strategie dadurch zu transformieren, dass sowohl Verbraucher vor Betrug geschützt sind wie auch deren Benutzerfreundlichkeit durch Reduzierung von Transaktionsproblemen erhöht wird.

- **Die RSA® Risk & Cyber Security Practice** bietet essentielle Beratungs-, Support- und Incident-Response-Expertise, so dass Unternehmen die Kontrolle über ihre sich entwickelnde Sicherheitslage übernehmen können.

Im Hinblick auf die DSGVO bietet RSA einen ganzheitlichen Ansatz zur Gewährleistung von Datenschutz. RSA bietet Lösungen für Business-Driven Security, die den geschäftlichen Kontext auf einzigartige Weise mit Sicherheitsprozessen verknüpfen, damit Unternehmen Risiken managen und die wichtigsten Ressourcen schützen können. RSA-Lösungen unterstützen Unternehmen bei der effektiven Erkennung und Abwehr von Angriffen, dem Management von Benutzeridentitäten und -zugriff sowie der Reduzierung geschäftlicher Risiken – all das sind wichtige Schritte, damit Unternehmen eine ganzheitliche Strategie als Reaktion auf die DSGVO entwickeln können.

ZEIT, IN EINER UNSICHEREN WELT ERFOLG ZU HABEN

ES IST ZEIT FÜR BUSINESS-DRIVEN SECURITY.

30.000+ Kunden (B2B)

1 Mrd. Consumer (B2C)

50 Mio. Identitäten

$ 60+ Mrd. geschützte Transaktionen – pro Jahr

$ 8+ Mrd. betrügerische Verluste verhindert – pro Jahr

1+ Mio. erweiterte Angriffe aufgespürt und beendet

400.000+ Malware-Abfragen analysiert – pro Woche

500+ Patente

Lassen Sie uns mit den DSGVO-Anforderungen als Kontext einen genaueren Blick auf das Produkt- und Serviceportfolio von RSA werfen und erläutern, wie diese Angebote Unternehmen bei der Vorbereitung auf die DSGVO-Compliance unterstützen können:

Die RSA Archer® Suite wird als konfigurierte, integrierte Softwareplattform bereitgestellt und umfasst zwei spezifische Anwendungsbeispiele; RSA Archer Data Governance stellt ein Framework bereit, mit dem Unternehmen geeignete Kontrollen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten identifizieren, managen und implementieren können. Mit RSA Archer Privacy Program Management können Unternehmen Verarbeitungsaktivitäten gruppieren, um Bewertungen der Auswirkungen der Data Protection durchzuführen und Mitteilungen an Datenschutzbehörden bezüglich Vorschriften und Datenschutzverletzungen zu überwachen.

Mit der RSA NetWitness® Suite können Unternehmen die DSGVO-Anforderungen zum Schutz von Benutzerdaten in den Bedrohungserkennungs- und Reaktionsaktivitäten selbst erfüllen. Im Gegensatz zu herkömmlichen Abwehrsystemen unterstützt die RSA NetWitness Suite Unternehmen bei der Suche nach Bedrohungen, die erfolgreich in Unternehmen eingedrungen sind. Werden sie nicht erkannt, können solche Exploits verheerend für Infrastrukturen und geistiges Eigentum sein und zu der Art von Datenschutzverletzungen führen, auf die die DSGVO speziell ausgerichtet ist.

Für die DSGVO ist die Pünktlichkeit bei der Erfüllung der Anforderung zur Benachrichtigung innerhalb von 72 Stunden absolut entscheidend. Mit RSA NetWitness können der Umfang und die Art von Sicherheitsverletzungen dank besserer Einblicke in die Angriffssequenz schneller erkannt werden. Darüber hinaus ist die Plattform mit einer Reihe von Kontrollmaßnahmen wie Verschleierung ausgestattet, die Sicherheitsanalysten für den Schutz von datenschutzsensiblen Daten nutzen können, ohne die Analysefunktionen zu verringern.

Die RSA SecurID® Suite nutzt Risikoanalysen und kontextbezogene Informationen, die dafür sorgen, dass den richtigen Personen von überall und auf jedem Gerät ein angemessener Zugriff bereitgestellt wird.
Im Zentrum der DSGVO steht die Anforderung, Data-Governance-Praktiken (technisch und organisatorisch) einzurichten, um den Zugriff auf personenbezogene Daten zu sichern. Das bedeutet die Implementierung von Technologie und Policies für das Identitäts- und Zugriffsmanagement, um sicherzustellen, dass Benutzer, die auf personenbezogene Daten zugreifen, dazu auch berechtigt sind.

Zusammenfassend unterstützt RSA Unternehmen dabei, das erforderliche Framework für die Vorbereitung auf diese Verordnung einzurichten, indem ein geschäftsorientierter Ansatz für Sicherheitsmaßnahmen implementiert und sichergestellt wird, dass ihr Risiko- und Kontroll-Framework präzise, vollständig und auf Herausforderungen rund um behördliche Auflagen und geschäftliche Risiken vorbereitet ist. RSA kann mit seinem einzigartigen Umfang von Produkten und Services, die Risikobewertung, Bereitstellung und Management von Sicherheitskontrollen sowie das laufenden Compliance-Management abdecken, als strategischer Partner auftreten, der jedes Unternehmen auf seinem Weg zur DSGVO-Compliance unterstützt.

Kontakt: Arrow ECS AG
web: www.arrowecs.de/rsa.html
Telefon: 089 93099 0
mail: rsa.ecs.de@arrow.com

NEURONALES DEEP LEARNING – DER ENDPOINT LERNT AUS ERFAHRUNG

Der Security Heartbeat lässt Endpoint- und Firewall-Lösungen miteinander reden.

BILD: SOPHOS

Heutige IT-Sicherheit ist meist reaktiv und viel zu langsam. Gleichzeitig nehmen Endpoint-Angriffe stetig zu und werden immer raffinierter. Daher stoßen herkömmliche Abwehrmechanismen zusehends an ihre Grenzen.

Die SophosLabs analysieren täglich mehr als 400.000 neue Malware-Samples. 75 Prozent dieser Malware wurde gezielt für bestimmte Unternehmen entwickelt. Deep Learning, eine Weiterentwicklung des Machine Learning, revolutioniert die Endpoint-Sicherheit. Intercept X steht an der Spitze dieser Revolution. Durch die Integration von Deep Learning verwandelt sich reaktive Endpoint-Sicherheit in prädiktive Endpoint-Sicherheit und schützt vor unbekannten Bedrohungen.

Viele Anbieter werben damit, dass ihre Produkte auf Machine Learning basieren. Machine Learning ist jedoch nicht gleich Machine Learning. Bei Sophos setzen wir zur Erkennung von Malware auf das sogenannte „Deep Learning" – oft auch als „neuronale Deep-Learning-Netzwerke" oder „neuronale Netzwerke" bezeichnet. Es ist von der Funktionsweise des menschlichen Gehirns inspiriert.

Es handelt sich um dieselbe Art des Machine Learning, die auch häufig zur Gesichtserkennung, zur natürlichen Sprachverarbeitung, bei selbstfahrenden Autos und in weiteren anspruchsvollen Bereichen der Computerwissenschaft zum Einsatz kommt. Deep Learning war anderen Machine-Learning-Modellen in der Vergangenheit durchweg überlegen, ist jedoch zur Erstellung eines effektiven Modells auf riesige Datenmengen und eine hohe Rechenleistung angewiesen. Unsere SophosLabs sammeln und analysieren zum Beispiel bereits seit 30 Jahren Malware-Daten und unsere mehr als 100 Mio. Endpoints liefern uns täglich Telemetriedaten.

Deep Learning hat wesentliche Vorteile gegenüber anderen Arten des Machine Learning, die gewöhnlich in Endpoint-Security-Produkten zum Einsatz kommen: die Modelle verarbeiten Daten über mehrere Analyseebenen – genau wie Neuronen im menschlichen Gehirn.
Jede Ebene trägt zu einer erheblichen Performance-Steigerung des Modells bei. Deep Learning ermöglicht die automatische Erkennung relevanter Eigenschaften und von deren Abhängigkeiten untereinander, was in dieser Komplexität von Menschen nicht bewältigbar wäre. Auf diese Weise kann das Sophos Deep-Learning-Modell auch Malware erkennen, die andere Machine Learning Engines übersehen.

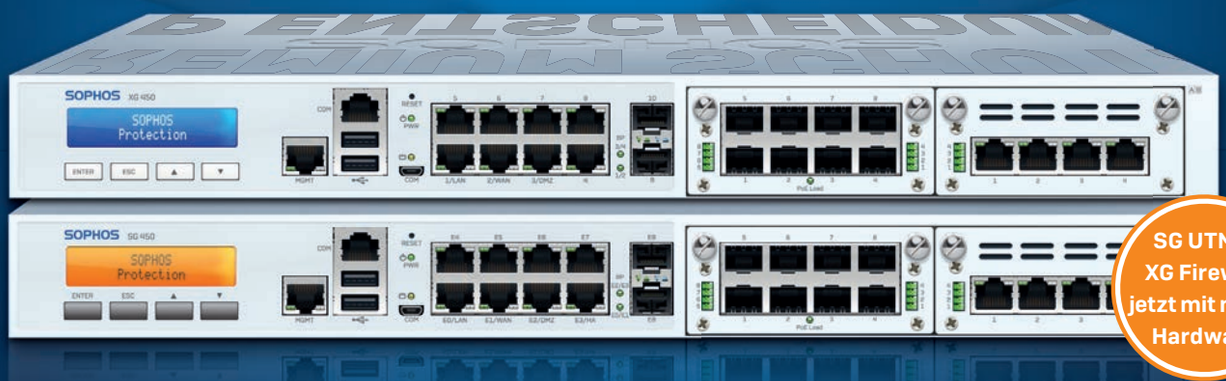
Deep Learning lässt sich problemlos auf Hunderte Millionen Training-Samples skalieren. Dieser Punkt ist entscheidend, weil die SophosLabs wöchentlich 2,8 Mio. neue Malware-Samples analysieren. Unser Modell kann unbegrenzt riesige Mengen von Trainingsdaten aufnehmen und ist so in der Lage, sich im Rahmen des Trainingsprozesses die gesamte beobachtbare Bedrohungslandschaft einzuprägen. Da das Modell weit mehr Eingaben verarbeiten kann, sagt Deep Learning Bedrohungen heute genauer vorher und bleibt auch in Zukunft immer auf dem neuesten Stand. Das Sophos-Trainingsmodell ist dabei kleiner als 20 MB und benötigt nur selten Updates. In der Cloud trainieren die SophosLabs das Modell kontinuierlich weiter und prüfen diese Entscheidungsgrenze mit neuen, unbekannten Malware-Samples.

Die richtige Schlagkraft erhält jede Technologie allerdings erst durch die nahtlose Einbindung in ein Gesamtsystem. Genau hier setzt Sophos Central mit einer zentral gesteuerten Managementplattform an. Mit dieser Security-Plattform können Unternehmen ihre gesamte Sicherheit an einem zentralen Ort verwalten: Endpoint, Mobile, Server, Web, Email, Wireless und Firewall Security sowie Verschlüsselung. Dabei handelt es sich nicht bloß um eine zentrale Management-Konsole.

Synchronized Security bietet wesentlich mehr: Dutzende Technologien arbeiten auf koordinierte Weise zusammen, um bestmöglichen Schutz vor koordinierten Angriffen zu bieten. Der Security Heartbeat reduziert zudem den Zeitaufwand für Bedrohungserkennung, Schutz und Reaktion von Stunden, Tagen oder sogar Wochen auf Sekunden.

[www.sophos.de]

MAXIMALE LEISTUNG.
PREMIUM SCHUTZ.
TOP ENTSCHEIDUNG.



SG UTM & XG Firewall jetzt mit neuer Hardware

SG UTM und XG Firewall:

Jetzt mit Deep Learning – integriert in Sophos Sandstorm.

- Weitaus effektiver als herkömmliches Machine Learning
- Erkennt Malware komplett ohne Signaturen
- Schützt selbst vor völlig unbekannten Bedrohungen

www.sophos.de/firewalls

SOPHOS

Prämierte Firewalls mit Spitzentechnologie

Enterprise Firewalls – PLATIN – Readers' Choice Security Insider AWARD 2017
Platin-Award „Enterprise Firewalls" von SecurityInsider

Readers' Choice eGovernment COMPUTING AWARDS 2017 Identität & Sicherheit – PLATIN –
Platin-Award „Identität und Sicherheit" von eGovernment Computing

SOPHOS NSS RECOMMENDED
Sophos XG Firewall – Beste Firewall im Test der unabhängigen NSS Labs

Produkt des Jahres
ITK-Produkt des Jahres im Bereich „Cybersecurity" von der Funkschau

CRN 2017 Bester Hersteller
„Security-Hersteller des Jahres" vom Channel-Fachmagazin CRN

TRANSFORMATION ALS TAGESGESCHÄFT

BILD: TAROX

TAROX-TRENDS IM JUBILÄUMSJAHR

Die fortschreitende Digitalisierung macht vor der IT-Branche nicht halt. Für die Unternehmensführung bedeuten die Veränderungen, die eigene Transformation täglich mit Tempo voranzutreiben.

Wie Tarox sich selbst und als Unterstützer seine Systemhauspartner für den Wandel zur Zukunft befähigt, zeigen Kristian Krause als Leiter Tarox Data und Patrick Andreas als Leiter IT-Security auch außerhalb ihrer Bereiche.

Denn die gemeinsame Zukunft gehört dem ganzheitlichen Zusammenwachsen. Als die Verantwortlichen der Tarox AG zuletzt für ihre Road Show durch Deutschland die dabei adressierten Systemhausinhaber via „Open Space"-Methode selbst bestimmen ließen, über welche Top-Themen sie informiert werden wollen, fiel die Entscheidung eindeutig zugunsten von Cloud-Diensten und IT-Sicherheit. Nicht die Wahl an sich, sondern ihre Klarheit überraschte etwas beim ganzheitlichen IT-Lösungsanbieter aus Westfalen. Denn traditionell packen zumindest Techniker und Vertriebler im Channel genau solche Themen nicht so gerne an, weil sie durch die Einführung bei gewerblichen Kunden den Verlust von Arbeit im eigenen Tagesgeschäft fürchten. „Dabei entsteht damit nachgewiesen ein großes Spektrum neuer Aufgaben, die zum Teil wegen des Fachkräftemangels kaum noch als Systemhaus allein bewältigt werden können. Die Nachfrage im Mittelstand nach Cloud-Diensten und IT-Sicherheit steigt. Wir registrieren beispielsweise im Bereich von Backups schon ein natürliches Wachstum von zehn Prozent. Schließlich bewegen wir uns alle in digitalen Prozessen, wodurch sich die zu verarbeitenden Datenmengen vergrößern und sich der Bedarf an Sicherung und an Sicherheit erhöht", betont Kristian Krause als Leiter von Tarox Data.

Wandel der Geschäftsmodelle: Durch die Digitalisierung entstehen in Unternehmen zunehmend „hybride Strukturen", beschreibt er, für die sich IT-Technologien „stetig und rasant" verändern und sich Angebote weiter hin zu „Geschäftsmodellen nach dem Prinzip pay per use" verschieben. Krause belegt dies allgemein an verstärkt verlangten Diensten wie Managed Service Providing (MSP). Oder an konkreten Beispielen wie Workplace as a Service, bei dem der Kunde zur Kaufoption von IT-Infrastruktur pro Arbeitsplatz alternativ ein Mietmodell als Angebot erhält. „Mit der wachsenden Vielfalt geht einher, dass Systemhäuser immer mehr Knowhow für verschiedene Anforderungen aufbauen müssten. Oder die Inhaber konzentrieren ihr Portfolio auf Kernkompetenzen und erweitern es dadurch, dass sie den Sachverstand von Tarox-Teams aufsatteln", rät Kristian Krause zur effizienten Transformation als Aufgabe im Tagesgeschäft.

Das Unternehmen sehe dabei die Rolle als Bindeglied zwischen Hersteller und Sytemhauspartnern. Dafür halte Tarox Data etwa Spezialisten vor für leistungsfähige hybride Backup-Lösungen, für zuverlässige Veeam Online-Speicher inklusive Veeam Backup & Replication, für effiziente IP-Telefonie oder für komfortable Managed Security aus der Cloud.

Ganzheitliche IT-Sicherheit: „Für die ganzheitliche IT-Sicherheit von Unternehmensnetzwerken ihrer Geschäftskunden sind Systemhäuser heute in der Bringschuld", bringt Patrick Andreas als Leiter der Tarox Security den Druck auf den Punkt. Denn der Mittelstand habe sich mittlerweile zwar „intensiv mit Informationssicherheit auseinandergesetzt", aber mit dem Umsetzen der Vorgaben aus der ab Mai greifenden EU-Datenschutz-Grundverordnung (DSGVO) „benötigen viele Unternehmen offensichtlich im Endspurt dringend Unterstützung." Der Information Security Manager konstatiert: „Der IT-Branchenverband Bitkom hat zuletzt in einer repräsentativen Umfrage ermittelt, dass nur jede zweite Firma mit 20 Mitarbeitern und mehr bislang externe Hilfe von Fachleuten in Anspruch genommen hat, um ihre DSGVO-Verpflichtungen rechtzeitig zu erfüllen. Entsprechend wird nur jedes achte Unternehmen nach eigener Einschätzung rechtzeitig zum Stichtag die Vorgaben umgesetzt haben." Dieser Nachholbedarf eröffne Tarox-Partnern große Chancen.

Die richtige Geräteverschlüsselung einrichten, dazu die passende Sicherheitssoftware vermarkten, den verlässlichen Schutz vor Malware gewährleisten – Systemhäuser seien vielseitig gefragt. Neben zuverlässigen Techniken gehe es „deutlich umfangreicher vor allem um organisatorische Maßnahmen", um ein Höchst-

BILD: TAROX

Kristian Krause,
Leiter Tarox Data

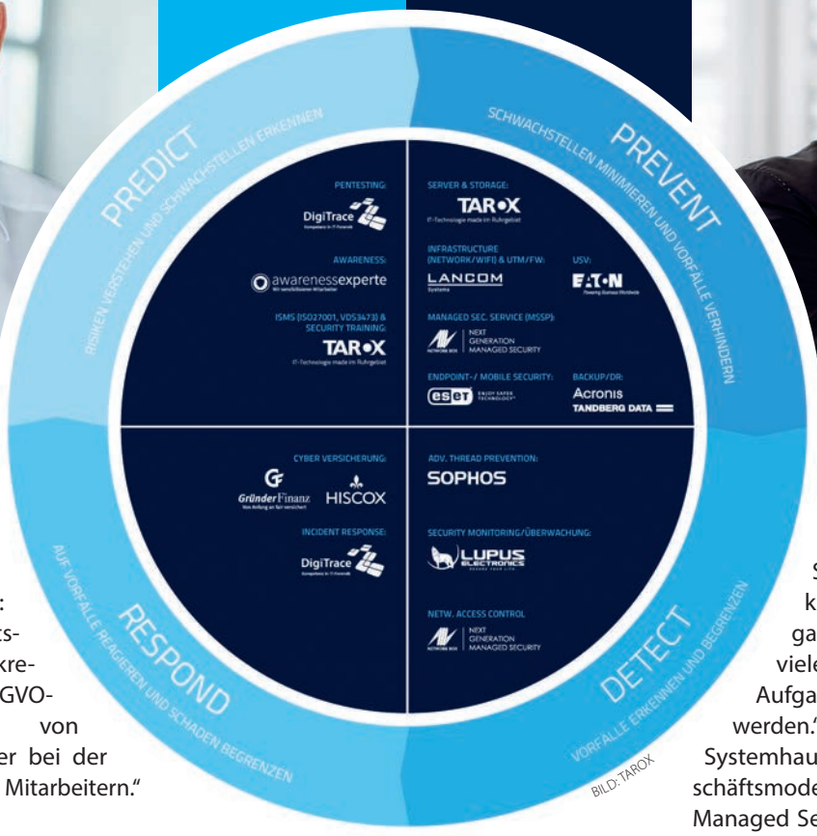


BILD: TAROX

Patrick Andreas,
Leiter IT-Security

maß an Sicherheit zu garantieren, unterstreicht der Experte: „Das Schließen von Sicherheitslücken scheitert oft an der konkreten Umsetzung – ob beim DSGVO-konformen Überarbeiten von Unternehmensrichtlinien oder bei der Datenschutzunterweisung von Mitarbeitern."

Als „Kernthemen" für IT-Sicherheit im Mittelstand registriert Patrick Andreas die stimmige Dokumentation und die präzisen Prozessketten, wofür spezielle Kompetenzen aufgebaut gehören. „Entsprechend stark ausgebucht sind unsere Workshops für Systemhauspartner", sagt er und verweist auf das in der Tarox Security Allianz gebündelte Wissen der zahlreichen Fachfirmen mit Expertise. Der Kreis aus Spezialisten für frühzeitige Schwachstellen-Erkennung bis zur wirkungsvollen Schadensbegrenzung streben als Einheit den vollen Schutz im Lebenslauf schützenswerter Daten und Infrastrukturen an. Und alle Tarox Systemhauspartner können dieses Knowhow nach Bedarf abrufen, um bei Geschäftskunden den Sachverstand für ganzheitliche IT-Sicherheit mitzubringen.

Zukunft der Systemhauspartner: Tarox verfolgt angesichts der digitalen Transformation für Systemhauspartner und ihre Firmenkunden das Ziel, das große Ganze für IT-Lösungen im Blick zu behalten. Dafür bündelt Tarox Technik und Knowhow, spürt aufkommende Trends und Entwicklungen auf und leitet daraus zukunftsträchtige Geschäftsmodelle her.

Die Herausforderungen nehmen künftig eher noch an Geschwindigkeit und an Schärfe zu, ist Kristian Krause überzeugt: „Im Mega-Markt IT beobachten wir eine Zunahme des Wettbewerbsdrucks durch den Direktvertrieb von Herstellern und starke Verschiebungen innerhalb der Handelsketten. Viele Veränderungen fordern vermehrt umfassendes Wissen von neuen technologischen Möglichkeiten, aber auch von neuen Vermarktungsstrategien oder ebenso von neuen Rahmenbedingungen gesetzlicher Natur." Deshalb gilt seine Devise, verstärkt Allianzen zu bilden und Kompetenzen zu bündeln.

Systemhäuser erkennen diesen Vorteil und nutzen das Tarox Consulting, um mit speziellem Knowhow bei Unternehmenskunden vor Ort aufzuwarten. Diese zeitgemäße Zusammenarbeit verlange zwar mehr Offenheit und Vertrauen, rentiere sich jedoch für alle Beteiligten. Kristian Krause spricht vom „neuen Arbeiten", das allein kaum noch zu bewältigen sei, wenn hinter dem „Top-Thema Office 365" beispielsweise 65 Einzelprojekte aufpoppen können: „Heute entwickeln wir hier mit dem Systemhaus und seinem Firmenkunden gemeinsam jeweils in ganztägigen Workshops, welche der vielen Applikationen für effiziente Aufgabenerfüllung wirklich benötigt werden." Das Unternehmen erarbeitet mit Systemhauspartnern komplett neue Geschäftsmodelle und Konzepte für umfassende Managed Services für Cloud-Dienste und IT-Security. „Onboarding"-Programme gezielt abgestimmt auf das betreffende Systemhaus schulen heute Partner nicht nur technisch, sondern auch in Vertrieb und Marketing.

Tarox trägt der Digitalisierung, mit der schnellere Prozesse einhergehen, künftig noch mehr Rechnung. Das digitale Tool „Tarox Pro" stellt Systemhäusern nicht nur den Konfigurator zum zügigen Zusammenstellen von IT-Lösungen zur Seite, sondern auch einen virtuellen Assistenten. Geräte-Order, Bundles, Software-Zukauf, Zusatz-Services für Partner, Ticketing zum fixen Austausch gehören zum neuen Partner-Portal, das jüngst an den Start ging. Der Tarox plus Agent stellt zudem ab April vielfältige Systemhaus-Unterstützung in den Fokus mit digitalem Agent und raschen Prozessen. Das Zusammenrücken und Zusammenwachsen zählt zur Zukunftsstrategie von Tarox, denn von der guten Auswahl qualifizierter Hersteller und von der kräftigen Unterstützung seiner Systemhauspartner profitieren neben Unternehmenskunden alle Beteiligten. Erfolgserlebnisse also, mit denen auch die Ergebnisse stimmen, wie das Unternehmen jetzt seit 25 Jahren beweist.

TAROX empfiehlt Microsoft® Software

Schichtwechsel!

Windows Server

TAROX SecurityAllianz

Mehrfach ausgezeichnete Serversysteme

25 IT. JUBILÄUM. TAROX. 1993 – 2018.

Wenn Unternehmen bessere Sicherheit, Effizienz und Innovationen benötigen, empfehlen wir Windows Server 2016.

- Maximale Performance für Ihre Applikation mit hoch skalierbarer Architektur
- Flexible interne Datenspeicherkonfigurationen
- Integrierte Sicherheitsfunktionen zum Schutz der Hardware
- Neuste Generation der Netzwerkkomponenten für einen effizienteren Datentransfer
- Optimiertes Energie- und Temperaturmanagement
- Verbessertes Ressourcenmanagement

Diesen Artikel finden Sie unter **www.tarox.de**

TAROX Aktiengesellschaft | Stellenbachstr. 49 – 51 | 44536 Lünen | Telefon: +49 (0)231/98 98 0-300 | vertrieb@tarox.de

IT-BUSINESS

Vogel IT-Medien GmbH

August-Wessels-Str. 27, 86156 Augsburg
Tel. 0821/2177-0, Fax 0821/2177-150
eMail: redaktion@vogel-it.de
Internet www.it-business.de

Geschäftsführer: Werner Nieberle (-100)

Co-Publisher: Lilli Kos (-300; verantwortlich für den Anzeigenteil)

Chefredakteur: Wilfried Platten

CvD: Dr. Andreas Bergler

CvD-Online: Sylvia Lösel

Redaktion: Michael Hase (Ltd.), Dr. Stefan Riedl (Ltd.), Sarah Böttcher, Sarah Gandorfer, Klaus Länger, Sarah Nollau, Heidi Schuster, Ira Zahorsky

Weitere Mitarbeiter dieser Ausgabe: Dr. Rudolf Aunkofer, Sebastian von Bomhard, Harald Knapstein

Media/Sales: Besa Agaj / International Accounts (-112), Stephanie Steen (-211), Hannah Lamotte (-193), eMail: media@vogel-it.de

Anzeigendisposition: Dagmar Schauer (-202)

Grafik & Layout: Johannes Rath, Udo Scherlin, Carin Boehm

Titelbild: © beebright-stock.adobe.com / Juniper - [M] Carin Boehm

EBV: Carin Boehm

Anzeigen-Layout: Johannes Rath, Carin Boehm, Michael Büchner, Udo Scherlin

Leserservice / Mitgliederbetreuung: Sabine Assum (-194), Fax (-228) eMail: vertrieb@vogel-it.de

Fragen zur Abonnement-Rechnung: Marcus Zepmeisel DataM-Services GmbH, 97103 Würzburg Tel.: 0931/4170-446 (Fax -494) eMail: mzepmeisel@datam-services.de

Erscheinungsweise: 14-täglich

Abonnement: Zeitschrift IT-BUSINESS: Der regelmäßige Bezug ist fester Bestandteil der Mitgliedschaft IT-BUSINESS PLUS Preise und weitere Informationen unter : http://www.it-business.de/plus

Druck: Vogel Druck- und Medienservice GmbH, Leibnizstr. 5, 97204 Höchberg

Verbreitete Auflage (IT-BUSINESS): 26.156 Exemplare (IVW Q4 / 2017)

Vogel Business Media

IVW EDA

Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Business Media**, Würzburg, einer der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt der Verlag Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an. Die wichtigsten Angebote des Verlages sind: **IT-BUSINESS, eGovernment Computing, BigData-Insider.de, CloudComputing-Insider.de, DataCenter-Insider.de, Dev-Insider.de, IP-Insider.de, Security-Insider.de** und **Storage-Insider.de.**

Nächste Ausgabe

IT-BUSINESS 5 / 2018 erscheint am 26.3.2018

IT-BUSINESS Spezial: Education

Druckunterlagenschluss am 20.3.2018

Anzeigenhotline 0821 / 2177 - 300

Lesertelefon 0821 / 2177 - 194

BILD: .SHOCK - STOCK.ADOBE.COM

Inserenten

Firma	Seite	Firma	Seite
api Computerhandels GmbH	100, 105	Kodak Alaris Germany GmbH	35
BullGuard Deutschland GmbH	68, 69, 94	Michael Telecom AG	103
DexxIT GmbH & Co. KG	70, 71	ONLINE USV-Systeme AG	3, 13
ECOM Electronic Components Trading GmbH	107	REWE Digital GmbH	21
ectacom GmbH	72, 73	RSA The Security Division of EMC Deutschland GmbH	82, 83
Eset Deutschland GmbH	74, 75	Siewert & Kau Computertechnik GmbH	92, 93, 96, 97
Exclusive Networks Deutschland GmbH	5	Sophos Technology GmbH	84, 85
Extreme Networks GmbH	33	Targus Deutschland GmbH	11
Fujitsu Technology Solutions GmbH	108	TAROX AG	86-89, 91, 98
G DATA Software AG	76, 77	TDT AG	101
Herweck AG	9	Toshiba Electronics Europe GmbH	2
Infinigate Deutschland GmbH	58-67	Vogel IT-Akademie	15, 27, 37-40
INGRAM MICRO Distribution GmbH	95	ZOTAC International (MCO) Ltd	99
Kaspersky Labs GmbH	78, 79		

Redaktionell erwähnte Unternehmen

Firma	Seite	Firma	Seite	Firma	Seite
Acer Group	32	Fujitsu	42	Nvidia	10, 48
Acmeo	20	G Data	31	PWC	22
ADP	31	Gartner	31, 32	Reiner SCT	13
Alpha 11	18	GfK	28	Ricoh	17
Also	7	Gigabyte	10	Riverbed	16
AMD	10, 43	HGST	8	Samsung	8, 10, 20, 44, 48, 102
Asus	10, 32	HMD Global	44	Scanblue	6
Axians	21	HP Inc.	32	SeeTec	18
Benq	10	Huawei	22	Siewert & Kau	8
BHE Bundesverband Sicherheitstechnik		i3D.net	22	SolarWinds	7
e.V.	18	IBM	6	Sony	44
Bitkom	30	IDC	22	Sophos	106
Cat Phones	44	IHS Markit	22	StepStone	36
Cirosec	7	IHS Research	18	Tech Data	8
Cisco	22	Infinigate	20	Techconsult	22
Dell	32	Intel	10, 42, 48	Telcat	8
Deloitte	31	International Ferdaration of Robotic	46	Toshiba	10
DHL	25	IQITS	41	TP-Link	10
Dimension Data	30, 22	IT-Cube Systems	6	Veeam	12
DXC Technology	31	IT-On.Net	41	Viewsionic	42
Ebertlang	7	Juniper	22, 25, 26	VMware	30
Ecom	10	Kaspersky	10	Westcon Security	7
Edimax	10	Lenovo	32, 44	Westcon-Comstor	25
ElectronicPartner	104	LG	44	Western Digital	10, 42
Elo	7	Liyama	10	Xantaro Group	26
EuroCIS	6	Microsoft	7, 10, 48	Zotac	48
Exclusive Networks	20	MSI	10	Zyxel	44
F5 Networks	26	Nokia	22		
Fast LTA	6	Nuvias	25		