ICT CHANNEL SONDERHEFT SECURITY

Bring on Your Future

Werden Sie jetzt Kaspersky-Partner und profitieren Sie von hohen Margen, attraktiven MSP-Vertriebswegen, umfassendem Support und vielen weiteren Benefits.

kas.pr/compete

Sie wollen mit Sicherheit nur das Beste? Kaspersky ist die Nr. 1.

kaspersky BRING ON THE FUTURE

Profiteure der Verunsicherung

Stefan Adelmann,
Chefredakteur ICT CHANNEL

Ob Eset, G Data, Kaspersky, Sophos, Watchguard, BSI oder selbst FBI – Anbieter und Institutionen schlagen in den letzten Monaten unisono Alarm: Die Corona-Pandemie stellt nicht nur eine Bedrohung für Leib und Leben dar, sondern Cyberkriminelle nutzen die Verunsicherung der Menschen und die neuen Herausforderungen auch, um daraus größtmöglichen Profit zu schlagen. Je nach Art des Angriffs und des jeweiligen Ziels, hat sich die Zahl der Angriffe verdreifacht, vervierfacht, oder – wie im Falle der Angriffe auf Remote-Desktop-Verbindungen – sogar verzehnfacht.

In die Karten spielt den Cyber-Tunichtguten dabei vor allem der notgedrungene Trend zum Homeoffice. Zahlreiche Unternehmen mussten innerhalb kürzester Zeit die entsprechende mobile Infrastruktur errichten, um auch dezentral geschäftsfähig bleiben zu können. Was dabei jedoch oftmals im Umzugsstress auf der Strecke blieb, das waren die dringend erforderlichen Security-Vorkehrungen sowie eine Einweisung der Mitarbeiterinnen und Mitarbeiter. Mehr denn je liegt die Verantwortung der IT-Sicherheit im Homeoffice – außerhalb der Firewall und gegebenenfalls mit privaten Geräten im Einsatz – in den Händen jedes Einzelnen.

Hier ist die Unterstützung des Channels entscheidend. Vielen Unternehmen wird aktuell bewusst, dass es sowohl technisch als auch strategisch noch einiges nach-zuholen gibt, in nicht minder vielen Fällen aber schlicht das Fachpersonal oder das Know-how fehlt. Daher verwundert es kaum, dass viele Systemhäuser, IT-Dienstleister und Managed Service Provider aktuell von einer rasant steigenden Nachfrage im Cyber-Security-Bereich berichten.

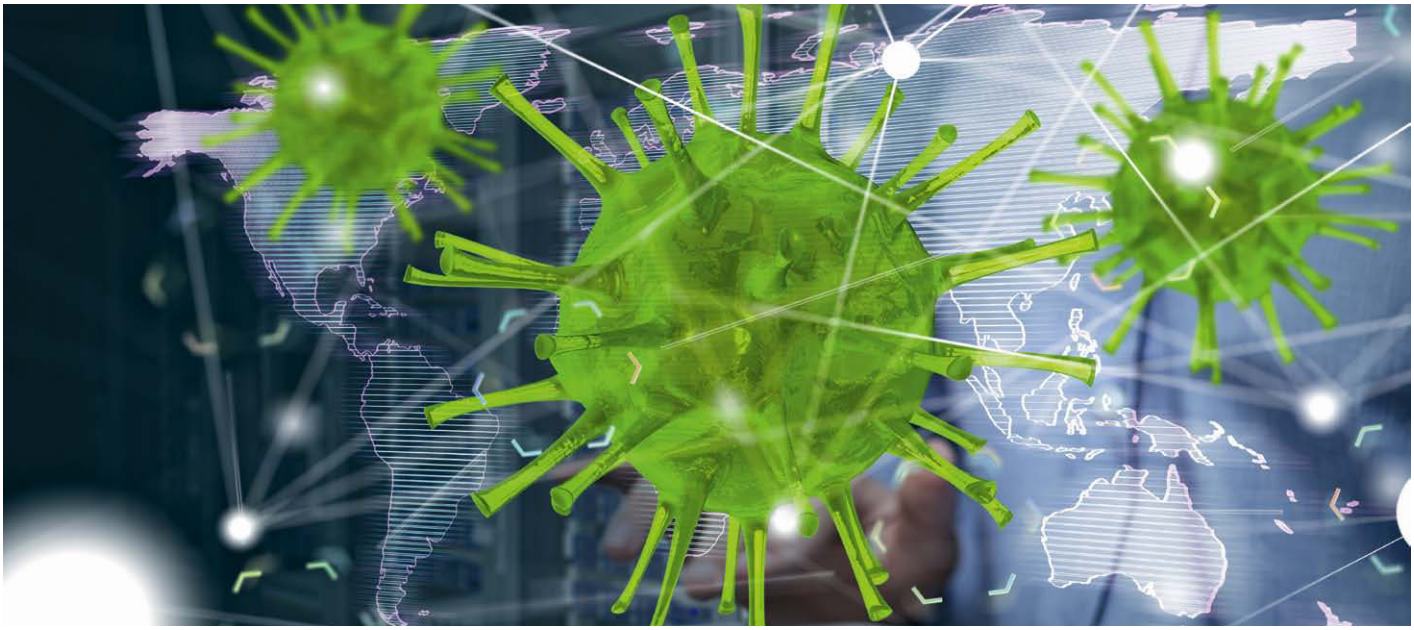
Ihr

Impressum

Chefredakteur:
Stefan Adelmann (sta), Tel. 089 25556-1352, sadelmann@weka-fachmedien.de
(verantwortlich für den redaktionellen Teil)
Editor-at-large
Martin Fryba (mf) -1559, mfryba@weka-fachmedien.de
Chefin vom Dienst:
Andrea Fellmeth (af) -1520, afellmeth@weka-fachmedien.de
Mitarbeiter dieser Ausgabe:
Antje Müller -1357, amueller@weka-fachmedien.de
Sales Director:
Eric Weis -1390, eweis@weka-fachmedien.de

Mediaberatung:
Sara Neugebauer -1574, sneugebauer@weka-fachmedien.de
Sofie Steuer -1452, ssteuer@weka-fachmedien.de
Nicole Wawrzinek -1087, nwawrzinek@weka-fachmedien.de
Anzeigendisposition: Sandra Wegner -1490
Leitung Vertrieb: Marc Schneider -1509
Layout/Grafik/Druckvorstufe:
JournalMedia GmbH, Haar
Druck: L.N. Schaffrath, Marktweg 42-50, 47608 Geldern

Geschäftsführung:
Kurt Skupin, Matthäus Hose



Quelle: vegefox.com | AdobeStock

Rapider Anstieg der Angriffszahlen

Wie die Pandemie die Cyber-Security-Landschaft verändert

Die Corona-Pandemie und der Wechsel zu dezentralen Arbeitskonzepten und Homeoffice haben auch die Anforderungen an Cyber-Security-Strategien verändert. Selten zuvor wurde so deutlich, wo Unternehmen nachbessern müssen und welche entscheidende Rolle Systemhäusern und IT-Dienstleistern zukommen kann.

Stefan Adelmann | Die Covid-19-Pandemie stellt nicht nur das Gesundheitssystem vor gewaltige Herausforderungen. Auch die Bekämpfung digitaler Viren ist aktuell mehr denn je gefordert. G Data beispielsweise ermittelte im vergangenen März einen Anstieg der Zahl an Cyberattacken um 30 Prozent. Betroffen waren nahezu alle Angriffsvektoren, ob Phising-Mails, Ransomware, DDoS-Angriffe oder aber auch vermeintliche Spendenaufrufe oder Angebote für Atemmasken, um Anwender auf Fake-Shops zu locken und zu Zahlungen zu verleiten. Auch Eset schlägt Alarm. Wie der Anbieter berichtet, hat sich im Zuge des Homeoffice-Umzugs vieler Unternehmen die Anzahl der Hacker-Angriffe auf Remote-Desktop-Verbindungen im DACH-Raum mehr als verzehnfacht. Allein im Juni 2020 verzeichnete Eset bis zu 3,4 Millionen Attacken innerhalb von 24 Stunden. Dabei gehe es den Angreifern sowohl um das Abgreifen von Daten als auch um die Verteilung von Ransomware. »Die aktuelle Verunsicherung in der Bevölkerung nutzen Cyberkriminelle schamlos aus. Wir beobachten derzeit einen sprunghaften Anstieg bei diesen Kampagnen«, erklärt Thomas Uhlemann, Eset Security Specialist. Anwender müssten in diesen Tagen unbedingt einen kühlen Kopf bewahren. Ziel der Kriminellen sei es, Nutzer zu einer unüberlegten Handlung zu verleiten, sei es das Öffnen eines Anhangs, das Anklicken eines Links oder die Überweisung von Geld.

Maßnahmen noch »verbesserungsbedürftig«

Der Homeoffice-Boom spielt den Kriminellen in die Hände. Oftmals mussten Unternehmen ihre Mitarbeiterinnen und Mitarbeiter über Nacht aus den Büros in die Heimarbeit senden, entsprechende mobile Endgeräte wurden notgedrungen und schnellstmöglich angeschafft – ohne dabei stets auf eine umfassende IT-Security-Strategie zu achten. Es ging vor allem darum, geschäftsfähig zu bleiben, alles andere folgte an zweiter Stelle. Wenn überhaupt.

Dabei können Homeoffice-Strukturen aber besonders anfällig für Cyber-Angriffe sein. Rechner befinden sich nicht mehr hinter der Firewall des Unternehmens, oftmals kommen private, ungeschützte Endgeräte zum Einsatz und längst werden nicht alle verfügbaren Sicherheitsvorkehrungen ausgeschöpft. Eine Umfrage des Bundesverbandes IT-Sicherheit (Teletrust) unter knapp 1.150 Teilnehmern aus dem vergangenen März zeigt auf, wo es technisch besonders hakt.

Backup: Lukratives Business statt lästige Pflichtaufgabe

Für die meisten Unternehmen ist Datensicherung eine lästige Pflicht. Für die meisten Systemhäuser ist es das auch. Völlig zu Unrecht. Denn richtig organisiert ist Managed Backup eine interessante Lösung für Endkunden und ein lukratives Geschäft für MSPs.

Das Angebot eines Systemhauses, die Datensicherung in Form einer Dienstleistung als Managed Service zu übernehmen, ist für viele Unternehmen attraktiv.

Als Systemhaus in Managed Backup einzusteigen ist nicht in erster Linie eine technische Herausforderung. Denn SolarWinds Backup bringt alle technischen Voraussetzungen bereits mit: Das System ist mandantenfähig, arbeitet als reines, natives Cloud Backup, ist vollständig automatisierbar und bietet verschiedene nutzungsbezogene Lizenzmodelle.

Rechenkünstler gefragt

Wichtiger als die technischen Grundlagen. Managed Backup Provider stellen ihren Kunden Angebotspakete mit überschaubaren monatlichen Pauschalen zusammen. Einige SolarWinds MSP Partner bieten ihren Kunden monatliche Flatrate unabhängig vom genutzten Datenvolumen an. Dazu ist es wichtig, die SolarWinds Backup Lizenzen mit Dienstleistungen zu kombinieren und den Betrieb effizient zu organisieren.

1. Wesentlicher Faktor ist die eigene Kostenstruktur: Was kostet eine Technikerstunde tatsächlich und wie viele benötige ich im monatlichen Betrieb. Der Vorteil: nahezu alle Tätigkeiten lassen sich automatisieren. Manuelle Eingriffe spielen eine untergeordnete Rolle.
2. Auf Basis der SolarWinds Lizenzmodelle können MSPs eigene Angebote maßgeschneidert für ihre Kunden entwickeln. Grundlage ist die Abrechnung je genutztem Server. Entscheidend ist, die eigene Kalkulation von den eingekauften Leistungen zu lösen. Die Rechnung EK + Marge = VK greift zu kurz.

Die richtige Kalkulation entscheidet

Besonders interessant für Backup im Managed Service ist das Angebot SolarWinds Backup pro Server inklusive 500 GByte lokales Datenvolumen zu einem monatlichen Pauschalpreis. Wichtig für die Kalkulation: Das Datenvolumen ist frei verfügbar.

Wer den tatsächlichen Speicherbedarf seiner Kunden kennt, ist im Vorteil. Belegen Server im Schnitt 100 GByte Daten (gerade bei kleinen und mittelständischen Unternehmen eine gängige Größenordnung), bleibt pro Server-Lizenz SolarWinds Backup ein Rest von im Schnitt 400 GByte zur freien Nutzung. Im Unterschied zu anderen Backup-Programmen belegt ein Backup mit SolarWinds im Rechenzentrum tatsächlich genau so viel Speicherplatz wie das zu sichernde Volumen.

Bei zehn Servern bedeutet das einen Verbrauch von 10x100 GByte = 1 TByte bei einem verfügbaren Volumen von 5 TByte (10x500 GByte). Eine Backup-Flatrate nach dem Vorbild von DSL-Datenverträgen ist angesichts des verfügbaren Volumens kein Problem.

Wird der Speicherplatz knapp, kann es günstiger sein, einen weiteren Server zu buchen. Belegt ein Kunde ungewöhnlich viel Speicher, empfiehlt es sich, das Gespräch zu suchen und gegebenenfalls ein angepasstes Abrechnungsmodell vorzuschlagen.

Fazit

Erfolgreiches Managed Backup Geschäft hängt von der Vorbereitung ab. Die beginnt bei Kalkulation und Angebotsdefinition, der Analyse der eigenen Tätigkeiten sowie der Kundeninfrastruktur und -daten. Die Automatisierung aller Vorgänge erhöht Sicherheit und Profitabilität.

»Wir schließen mit allen Kunden einen Backup- und RMM-Vertrag«


Quelle: Michgehl & Partner

Der Markt für Anwälte und Notare ist im Umbruch: Die Digitalisierung hält Einzug und verändert die Arbeitsweise der Akteure. »Der Schriftverkehr mit Gerichten hat elektronisch zu erfolgen«, erklärt Franz-Josef Michgehl, Geschäftsführer bei Michgehl & Partner, einem auf Anwalts- und Notarsoftware spezialisierten MSP.

Mit RA Micro vermarktet Michgehl eine renommierte Software-Lösung für Anwälte und Notare. Seine Kunden betreut der MSP ganzheitlich. »Wenn wir die Bereitstellung der Software übernehmen und die Verfügbarkeit gewährleisten, müssen wir natürlich die Infrastruktur unserer Kunden kennen«, betont Franz-Josef Michgehl. Nur so können seine Techniker Probleme und Schwächen schon im Vorfeld erkennen und ausräumen.

Der minimale Servicevertrag umfasst Monitoring, Backup und die Absicherung der Clients. »Das brauchen wir, um unseren Job machen zu können. Wir erklären den Kunden unsere Leistungen und deren Nutzen sehr genau«, sagt Franz-Josef Michgehl und empfiehlt anderen MSPs: »Sprechen Sie mit Ihren Kunden Klartext.«

Demnach sind zwar knapp zwei Drittel der eingesetzten Computer und WLANs im Homeoffice immerhin passwortgeschützt, auch ein Virenschutz kommt zumeist zum Einsatz. Eine Trennung von privaten und dienstlichen Endgeräten gibt aber nur noch die Hälfte an, eine verschlüsselte Datenübertragung oder ein VPN kommen gar nur bei 38 beziehungsweise 37 Prozent der Befragten zum Einsatz. Und eine Mehr-Faktor-Authentifizierung ist lediglich bei 27 Prozent vorhanden. »Das Ergebnis zeigt, dass durchaus Problembewusstsein besteht, die technischen Maßnahmen aber noch verbesserungsbedürftig sind«, so das Fazit von Norbert Pohlmann, Vorsitzender des Teletrust.

Oftmals keine Einweisung der Belegschaft

Aber nicht nur entsprechende Security-Lösungen sind im Homeoffice-Einsatz eigentlich unabdingbar, auch die Rolle der Mitarbeiterinnen und Mitarbeiter ändert sich, die Verantwortung für die IT-Sicherheit liegt nunmehr zu großen Teilen in ihren Händen. Eine Aufgabe, auf die nicht jedes Unternehmen in der Kürze der Zeit ausreichend vorbereitet hat, an entsprechender Awareness mangelt es in vielen Fällen. So bemängeln ganze 81 Prozent der durch Kaspersky im Rahmen einer Studie befragten Beschäftigten aus Deutschland, dass sie zu Beginn der Remote-Arbeit keine Cybersicherheitseinweisung oder -schulung erhalten hätten. Der Anbieter rät daher, nicht nur die wichtigsten Maßnahmen zum Datenschutz durchzuführen, sondern besonders auch regelmäßig die gesamte Belegschaft zu schulen.

Aufgrund der offenkundigen Risiken verwundert es kaum, dass zahlreiche IT-Dienstleister und Systemhäuser im Zuge der Corona-Pandemie gegenüber ICT CHANNEL von einer steigenden Nachfrage im Security-Geschäft berichten. Denn selten zuvor war es so eklatant, wo die Schwachstellen vieler Sicherheitsstrategien liegen. Den Unternehmen würde immer mehr bewusst, dass sie etwas tun müssten, berichtet auch Wulf Vogel, Geschäftsführer des Karlsruher IT-Dienstleisters Interconnect. Eine Entwicklung, die sich auch an den Marktzahlen ablesen lässt. Zwar sollen die Security-Ausgaben in diesem Jahr laut Canalys aufgrund der Pandemie langsamer wachsen als zuvor erwartet. Die Marktforscher gehen aber immer noch von einer Steigerung um bis zu 5,6 Prozent auf 43,1 Milliarden US-Dollar aus. Im Detail sollen 2020 besonders die Ausgaben für Endpoint Security (bis zu 8,5 Prozent), Web- und E-Mail-Security (bis zu 10,3 Prozent) sowie Schwachstellenmanagement und Security-Analytics (bis zu 10 Prozent) steigen. Ein Minus von bis zu 4,7 Prozent sieht Canalys hingegen bei Network Security, die aufgrund der Auflösung des klassischen Perimeters an Bedeutung verlieren würde.

Eine Chance in der Krise

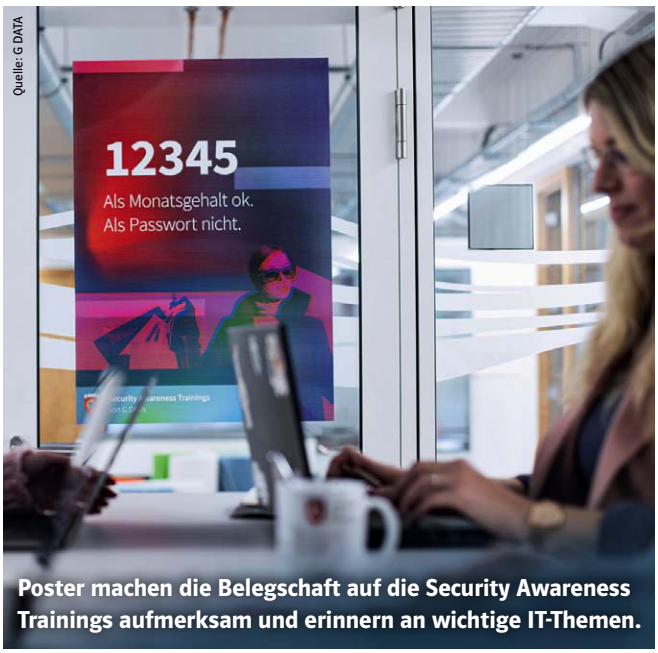
Ein Selbstläufer ist das IT-Dienstleistungsgeschäft aber auch in diesen herausfordernden Zeiten nicht. Eine Befragung des Spezialversicherers Hiscox zeigt, dass die Hälfte der befragten IT-Anbieter im Zuge der Corona-Krise Aufträge verloren hat, denn viele Unternehmen ziehen aus Vorsicht zeitunkritische Projekte zurück oder verschieben diese. Zwar würden viele Medien über einen Digitalisierungsschub sprechen, wie Hiscox-Manager Marc Thamm gegenüber der Deutschen Presse-Agentur erklärte, »aber Homeoffice oder Home Schooling sind nur eine Facette der großen IT-Landschaft. IT-Dienstleistern für die Reise- und Veranstaltungsbranche geht es beispielsweise nicht so gut, die sind genauso betroffen wie andere Unternehmen auch.«

IT-Sicherheit ist hingegen kein Thema, das Geschäftsführer in Anbetracht der steigenden Angriffszahlen auf die lange Bank schieben können. Hinzu kommt, dass vielen Unternehmen schlicht das Fachpersonal sowie das nötige Know-how fehlt, um den immer professionelleren Angriffen allein begegnen zu können. Für den Channel eröffnet sich hier mit der richtigen Strategie eine Chance, Kunden in der Krise zu unterstützen und gleichzeitig von der rasch steigenden Nachfrage zu profitieren. Wie beispielsweise Cyqueo. Der Münchner Managed Security Service Provider und Cloud-Security-Dienstleister verbuchte zuletzt eine um 70 Prozent gestiegene Nachfrage bei der Absicherung von Homeoffice-Strukturen, bei Security Awareness Trainings waren es gar 85 Prozent. »Die Corona-Krise hat viele Bereiche und Branchen hart getroffen, gleichzeitig aber auch die Digitalisierung deutlich beschleunigt. Dabei gilt es, die ständige Bedrohungsveränderung, Kostenoptimierung und die Verschiebung von Budgets ständig im Auge zu behalten«, so der Rat von Patric Liebold, CEO von Cyqueo. ■

Schulungen sensibilisieren Mitarbeiter für Cybergefahren

Cyberkriminelle gelangen nicht nur über Sicherheitslücken im System in das Unternehmensnetzwerk. Oft gehen sie den Weg des geringsten Widerstands und greifen über Mitarbeiter an. Sinnvoll ist daher der Einsatz von G DATA Security Awareness Trainings und einer Phishing-Simulation, um Mitarbeiter zu schulen und sie aktiv in die IT-Sicherheit mit einzubeziehen.

Mittelständische Unternehmen sind für Cyberkriminelle ein attraktives Ziel. Eine Umfrage von Bitkom im November 2019 ergab: 75 Prozent der Firmen sind in den vergangenen zwei Jahren Opfer von Datenmissbrauch, Industriespionage oder Sabotage geworden. Das zeigt: Unternehmen müssen sich bei der IT-Sicherheit bestmöglich aufstellen und sich Cyberkriminellen entschieden entgegenstellen. G DATA Security Awareness Trainings schulen alle Angestellten im Unternehmen in Form von E-Learnings und machen sie fit für alle wichtigen Themen der IT-Sicherheit.



Poster machen die Belegschaft auf die Security Awareness Trainings aufmerksam und erinnern an wichtige IT-Themen.

Technischen Schutz um IT-Schulungen erweitern

Neben technischen Schutzmaßnahmen ist auch der Mensch ein wichtiger Faktor für die ganzheitliche Sicherheit der Unternehmens-IT. Für die Angreifer ist es oft leichter, Mitarbeiter zu manipulieren, um Logindaten auszuspionieren oder über sie Schadcode ins Firmennetzwerk zu schleusen, als nach technischen Sicherheitslücken zu suchen. Angestellte müssen daher ein Verständnis für die IT-Sicherheit und für Cyberrisiken entwickeln. Die Security Awareness Trainings von G DATA CyberDefense umfassen über 35 Kurse mit unterschiedlichen Schwerpunkten. In kleinen Lerneinheiten kommen Videos, Texte und Multiple-Choice-Fragen zum Einsatz, um unterschiedliche Thematiken, wie das richtige Verwalten von Passwörtern oder sicheres Arbeiten im Homeoffice didaktisch ansprechend zu vermitteln. Durch Wiederholungen der Inhalte und eine kurze Auswertung zu jedem Lernblock festigt sich das Wissen langfristig und Mitarbeiter können im Ernstfall richtig reagieren. Eine Phishing-Simulation stellt dabei realistische Angriffsszenarien nach und trainiert den Umgang mit gefälschten Mails.

Phishing-Simulationen zeigen Status quo der Belegschaft

Phishing-Angriffe zu simulieren ist sinnvoll, um die Awareness im Unternehmen zu messen und langfristig zu steigern. Über einen festgelegten Zeitraum erhalten die Mitarbeiter mehrere Wochen lang Mails in unterschiedlichen Schwierigkeitsgraden. Manche Nachrichten sind aufgrund einer auffälligen Rechtschreibung direkt als Phishing erkennbar, andere wiederum erst nach genauerem Hinsehen. Auf diese Weise übt die Belegschaft den Umgang mit Phishing-Mails und entwickelt auch eine Routine, wie sie mit verdächtigen Mails im besten Fall verfahren: Sie sollten sie nicht nur erkennen, sondern auch an die zuständige IT-Abteilung weiterleiten. So lassen sich umgehend Maßnahmen einleiten, wenn sich der Verdacht bestätigt. Nach Abschluss der Simulation ist eine Einschätzung möglich, die den aktuellen Wissensstand der Mitarbeiter im Umgang mit Phishing-Mails zeigt. Ist die Interaktion mit diesen Mails sehr hoch ausgefallen und wurden sogar Daten eingegeben, besteht akuter Handlungsbedarf.

Security-Awareness beim Kunden steigern

Reseller können durch G DATA Security Awareness Trainings ihr Portfolio gewinnbringend und sinnvoll erweitern, um Unternehmen zu helfen, sich ganzheitlich und umfassend vor Cyberangriffen zu schützen. Die G DATA Security Awareness Trainings und die Phishing-Simulation machen Mitarbeiter zu einem Teil der Cyberabwehr. Im alltäglichen Geschäft erhält die komplette Belegschaft durch E-Learning-Kurse das nötige Wissen, um Angriffe umgehend abzuwehren. Durch flächendeckende Schulungen über einen festgelegten Zeitraum, entwickelt sich eine Sicherheitskultur. Eine Investition in das IT-Sicherheitswissen der Mitarbeiter ist auch eine Investition in die Zukunft des Unternehmens.

Mehr Informationen unter:
www.gdata.de/awareness-training

HP Laptops haben die Sicherheit bereits integriert

Gerade durch den Umzug ins Home-Office ist die Sicherheit mobiler Endgeräte wie Laptops und Tablets deutlich wichtiger geworden. Da diese Geräte bei der Arbeit in den eigenen vier Wänden nicht in die Sicherheitsarchitektur des Unternehmensnetzwerks eingebunden sind, müssen Unternehmen wie Mitarbeiter weitere Maßnahmen ergreifen, um zu gewährleisten, dass nicht nur die Hardware und Anwendungen selbst geschützt sind, sondern auch die sensiblen Firmendaten.

Quelle: HP

HP Notebooks kommen mit integrierten Sicherheitsfunktionen.

Nicht selten nutzen Cyberkriminelle schwächer geschützte Endgeräte als Einfallspforten, um unternehmenskritische Informationen und geistiges Eigentum abzuschöpfen. Der Verlust vertraulicher Daten, kundenspezifischer Datensätze oder proprietärer Informationen kann leicht Kosten in Millionenhöhe verursachen. Organisationen setzen daher so viele Ressourcen wie nie zuvor für den Schutz ihrer Daten ein. Sicherheitslücken im Druck-, Imaging- und PC-Bereich werden aber bei vielen Security-Strategien nicht berücksichtigt. Daher schützen Technologien, die HP bereits ab Werk in seinen Rechnern und Druckern integriert, Organisationen und erleichtern IT-Teams die Arbeit.

Die umfangreichen, integrierten Sicherheitsfunktionen suchen ihresgleichen. Bereits rund um das Betriebssystem hat HP Sicherheitsfunktionen und Schutzebenen aufgebaut, die Bedrohungen proaktiv verhindern und im Falle einer Sicherheitsverletzung eine schnelle Wiederherstellung gewährleisten. Darüber hinaus setzt die HP Sure Sense-Funktion proprietäre auf Deep-Learning-Algorithmen und fortschrittliche neuronale Netzwerke, um Malware instinktiv zu erkennen und Anwender vor völlig unbekannten Angriffen zu schützen. Denn immerhin entstehen pro Tag circa 350.000 neue Malware-Varianten. IT-Teams können diese Vielzahl unterschiedlicher Malware nicht manuell scannen und gleichzeitig Netzwerke, Rechner und Drucker absichern – Künstliche Intelligenz (KI) ist hier ein entscheidendes Erfolgskriterium.

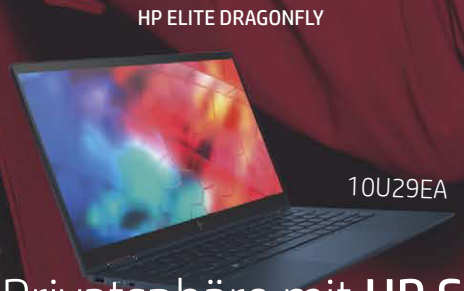
Integrierter Schutz bereits ab Werk

Eine weitere Möglichkeit, um Notebooks und damit sensible Daten zu schützen, ist etwa eine Virtualisierungslösung wie HP Sure Click Enterprise. Die Lösung isoliert jede potenziell riskante Anwenderaktivität – etwa das Aufrufen einer Webseite über Links in Dokumenten oder E-Mails, das Herunterladen einer Datei von solchen Webseiten, das Öffnen und Bearbeiten eines E-Mail-Anhangs oder der Zugriff auf die Daten eines portablen Speichermediums – in einer eigenen Micro-Virtual-Machine (Micro-VM). Der Malware-Schutz erfolgt direkt am Endgerät, mögliche Schädigungen bleiben auf das jeweilige Anwendungsfenster begrenzt. Nach Beendigung der Aktivität oder dem Schließen eines Browser-Tabs werden alle Informationen automatisch gelöscht. Eine Infizierung des Rechners selbst mit neuer, bisher unbekannter Schadsoftware – mit dem Potenzial eines Angriffs auf das komplette Netzwerk – ist nahezu ausgeschlossen.

Mitarbeiter, die von ihrem Unternehmen mit HP Notebooks ausgestattet sind, können damit aufatmen: Sie sind bereits zu einem nicht unerheblichen Teil vor Angriffen geschützt. Berücksichtigen sie jetzt noch ein paar einfache Richtlinien – zum Beispiel nicht auf Links in E-Mails mit unbekanntem Absender klicken oder verdächtig erscheinende Anhänge öffnen – können sie sicher im Home-Office arbeiten. Organisationen hingegen haben eine Sorge weniger und konzentrieren sich darauf, den Betrieb zu gewährleisten und erfolgreich am Markt zu agieren.

Quelle: HP

VERABSCHIEDEN SIE SICH VON UNGEWOLLTEM PUBLIKUM



Dank maximaler Privatsphäre mit **HP SureView Reflect.**

HP Notebooks. **Work better.**

Mehr erfahren: **hp.com/workbetter**

Intel® Core™ i5 vPro® Prozessor

Die Eröffnung des neuen Firmengebäudes von G Data fand Ende 2018 statt. Bistro, Museum, moderne Arbeitsplätze – der Anbieter hat erkannt, dass es im War for IT-Talents attraktive Anreize braucht

35 Jahre G Data

IT-Security made in Bochum

Zwei Tech-Enthusiasten, eine innovative Idee, Gartenlaube statt Garage – die G Data-Gründungsgeschichte steht denen aus dem fernen Silicon Valley in wenig nach. Ergebnis war die Entwicklung der ersten Antiviren-Software der Welt. Eine deutsche IT-Erfolgsstory, die auf einigen Produktumwegen zum heutigen Ziel kam.

Stefan Adelmann | Mehr als drei Jahrzehnte nach der Gründung von G Data musste Andreas Lüning erst einmal eine Fehlannahme ausräumen: Das Unternehmen wurde 1985 eben nicht in einer Garage gegründet, wie es der IT-Ur-Mythos aus dem Silicon Valley eigentlich vorschreibt, sondern einige Meter hinter der Garage der Familie Figge, in einer Gartenlaube. Hier begannen Lüning und Kai Figge (damals beide um die 20), erste Software für den Atari ST zu programmieren und zu verkaufen, nachdem sie sich zuvor in einem Copyshop kennengelernt hatten. Bereits zwei Jahre später sollten sie Geschichte schreiben: Die IT-Enthusiasten entwickelten 1987 das erste kommerzielle Antiviren-Programm, um mit diesem gegen – auf ihrem Feld wohl ebenso Pionierarbeit leistende – Bootsektor-Viren vorzugehen. »Wir haben diese zwei Viren in meiner Diskettenbox gefunden«, blickt G Data-Mitgründer Lüning im Gespräch mit ICT CHANNEL zurück. »Da war es logisch, etwas dagegen zu tun.« Zwar hatten die beiden Entwickler bereits damals die Befürchtung, dass noch weitere Schädlinge folgen könnten, Sorge vor einer größeren Bedrohung in diesen frühen Tagen der Malware-Historie jedoch noch nicht. Immerhin waren Viren Ende der 80er Jahre nicht unbedingt gefährlich, viel mehr lustig, wie Figge sich erinnert. »Das haben ein paar Kids entwickelt, das war noch keine Computerkriminalität wie heute.«

Zugespitzt hat sich die Bedrohung für Nutzer und Wirtschaft dann vor allem

mit der zunehmenden Vernetzung und dem Erfolg des Internets. Nichtsdestotrotz konnten die Bochumer Pioniere bereits 1987 den Grundstein der modernen Cyber Security legen – schreckten im Zuge ihres Unternehmenswerdegangs, vor allem noch vor der Jahrtausendwende, aber auch nicht vor Ausflügen in andere Software-Bereich zurück. Ob Routenplaner, Brennprogramm, digitales Telefonbuch oder Diktier-Tool, längst war durch die Jahrzehnte nicht alles aus dem Hause G Data IT-Security. »Wir haben in all den Jahren sehr viele verschiedene Produkte angeboten«, sagt Figge im Gespräch mit ICT CHANNEL, »das war teils ein Bauchladen«.

Kai Figge (links) und Andreas Lüning im sogenannten War Room in der Bochumer Zentrale. Die beiden IT-Enthusiasten haben G Data in 35 Jahren zu einem Unternehmen mit 500 Mitarbeitern und zu einem der wenigen erfolgreichen deutschen Cyber-Security-Anbieter entwickelt

Die große Stärke der Bochumer blieb jedoch stets Cyber-Sicherheit und so folgte 2006 eine Rückbesinnung und eine Refokussierung des eigenen Portfolios. »Das war eine sehr gute Entscheidung«, bekräftigt Figge rückblickend. »Wir hätten sie nur noch früher treffen können.«

Der heutige Erfolg gibt der Einschätzung des Mitgründers recht. Die Mitarbeiterzahl der Nordrhein-Westfälischen Softwareschmiede hat sich seit der strategischen Richtungsfindung verfünffacht, der Umsatz ist stetig gewachsen und G Data entwickelte sich zu einem der wenigen erfolgreichen Cyber-Security-Anbieter aus Deutschland.

Bochum, ein Glücksfall

Aktuell wird der globale Markt vor allem von US-amerikanischen Anbietern dominiert, besonders aus dem Silicon Valley, aber auch aus Tel Aviv kommen wegweisende Entwicklungen. Um hier auf europäischer Bühne mitspielen zu können, benötigt es ein starkes Netzwerk und den richtigen Standort. In Deutschland denkt man dabei zuerst an Berlin, vielleicht München oder Hamburg – und doch sprechen sich Figge und Lüning auch nach 35 Jahren klar für Bochum aus. »Der Standort ist ein Glücksfall«, unterstreicht Figge. Immerhin sei das Görtz Institut nur wenige Minuten entfernt, hier werden die IT-Security-Fachkräfte der Zukunft ausgebildet. Natürlich, auch fernab der großen deutschen IT-Cluster in Berlin und München spürt man den Wettbewerb um vielversprechende Nachwuchskräfte, dennoch muss sich G Data in Bochum nicht so ungefiltert mit Digital-Goliaths wie Google und Microsoft messen, wie es beispielsweise in der Bundeshauptstadt der Fall wäre. Daher hat sich wohl auch die Frage eines Standortwechsels nie gestellt. »Wir kämen gar nicht auf die Idee, wie andere Softwareentwickler nach Rumänien umzuziehen«, so Figge.

Im Gegenteil. Statt sich vor dem starken Wettbewerb in der IT zu verstecken, hat G Data 2014 ein 2,3 Hektar großes Gelände – ein Komplex des ehemaligen »Konsumverein Wohlfahrt« – an der Königsallee in Bochum gekauft und aufwendig zu einem modernen Firmen-Campus inklusive Museum und Bistro mit österreichischem Sternekoch umgebaut. Der Anbieter hat erkannt, was es im heutigen War for Talents braucht, um sich auch gegen die US-amerikanischen Digitalgiganten durchsetzen zu können.

Ein Cyber-Sicherheitsgurt

Und die so gewonnen Fachkräfte sind auch dringend notwendig. Nicht nur, um in Zukunft den eingeschlagenen Wachstumskurs weiter beibehalten zu können. Vor allem auch, um mit den immer professioneller arbeitenden Cyberkriminellen Schritt halten zu können. Denn zu leisten gibt es für die Bochumer hierzulande noch einiges – trotz oder auch gerade wegen der wachsenden Aufmerksamkeit, die dem Thema IT-Security in den vergangenen Jahren zuteilwurde. »Die Lage im deutschen Mittelstand ist weiterhin prekär, die Unternehmen sind sehr lückenhaft geschützt«, so das wenig positive Urteil von Figge. Viele Firmen hätten noch nicht einmal einen Notfallplan in der Schublade. Daher wünscht sich der Security-Experte mehr Bewusstsein für die sich zuspitzende Bedrohungslage und dass entsprechende Vorkehrungen Teil des Alltags werden. Immerhin habe das in den 70er Jahren auch mit dem Sicherheitsgurt im Auto geklappt, wie der Vorstand im Interview sagt. »Das mag unbequemer sein als ohne, ist aber heute eine Selbstverständlichkeit.« In der digitalen Welt sei dieses Denken, das Wissen um die Notwendigkeit eines IT-Sicherheitsgurtes, jedoch vielerorts schlicht noch nicht angekommen.

Es ist ein Rennen mit der Zeit. Einerseits Unternehmen aufmerksam machen, überzeugen und Mitarbeiter regelmäßig schulen. Und andererseits mit den Cyberkriminellen technologisch stets auf Augenhöhe bleiben. Denn auch diese investieren, arbeiten mit immer mächtigeren Werkzeugen und professionelleren Netzwerken, während die IT-Systeme stetig komplexer und somit schwerer zu schützen sind. »In 5.000 Zeilen Code findet sich im Schnitt ein Fehler. Beispielsweise Windows 10 hat aber mittlerweile 50 Millionen Code-Zeilen«, erklärt Figge. Entsprechend nimmt die Angreifbarkeit der IT zu, die Anforderungen an die entsprechenden Sicherheits-Lösungen steigen. Laut den Vorständen darf es daher jetzt nicht mehr nur darum gehen, Malware nur zu entdecken und zu neutralisieren, sondern präventiv gegen sie vorzugehen. Ein Beispiel dafür ist die kürzlich von G Data vorgestellte Technologie »Beast«. Sie soll nicht nur bereits bekannte Schadsoftware erkennen, sondern vielmehr deren Verhalten verfolgen, indem die Lösung das gesamte System und dessen Aktivitäten betrachtet. So entdecke man laut dem Anbieter auch bisher unbekannte oder stark spezialisierte Angriffe.

»Das hat immerhin in den 70er Jahren auch mit dem Sicherheitsgurt im Auto geklappt. Das mag unbequemer sein als ohne, ist aber heute eine Selbstverständlichkeit.«

Katz- und Maus-Spiel

Es ist aber ein Katz-und-Maus-Spiel zwischen den Cyberkriminellen und den Security-Anbietern. Mal die Katz, mal die Maus. Die Tage der technikaffinen Kids, die sich mit Viren einen augenzwinkernden Spaß erlauben, sind wohl unwiederbringlich vorbei. Heute stehen ganz andere, weitaus kriminellere Interessen hinter Malware und der stetig wachsenden Zahl an Cyber-Angriffen auf die Unternehmenswelt.

Gleichzeitig haben aber auch die beiden Herzblutprogrammier aus Bochum ihr Unternehmen in 35 Jahren erfolgreich weiterentwickelt. Für den Standort Deutschland, die hiesige Cyber-Security-Landschaft und vor allem auch den Channel ist G Data ein wichtiger Player im Markt, der auch fernab von Garagengründung und Valley-Mythos aufzeigt, dass aus Deutschland wettbewerbsfähige Security-Technologien kommen können. Dass das Unternehmen mit seinem hiesigen Standort Nähe zu Partnern und Kunden beweist und darüber hinaus einzig den deutschen sowie europäischen Datenschutzvorgaben unterworfen ist, kann darüber hinaus in diesen Zeiten kaum ein Nachteil sein. ■

ICT CHANNEL Interview

»Wenn es zu schön ist, um wahr zu sein, ist es das auch nicht«

Die Zahl der Cyber-Angriffe hat in den vergangenen Monaten massiv zugenommen, im Homeoffice kommen auf Unternehmen und ihre Belegschaft neue Risiken zu. Im Interview mit ICT CHANNEL erläutert Stefan Dydak, Sicherheitsexperte bei HP, wo aktuell die größten Gefahren lauern und warum die Angriffsfläche drastisch zugenommen hat

Stefan Adelmann

ICT CHANNEL: *Herr Dydak, im Zuge des Homeoffice-Booms ist die Zahl der Cyberangriffe auf Unternehmen und Privatpersonen teils deutlich gestiegen. Was genau ist der Grund dieser Zunahme?*

Stefan Dydak: Diese Entwicklung haben wir ebenfalls beobachtet. Viele Cyber-Kriminelle nutzen die Angst der Menschen vor Covid-19 aus. Sie senden E-Mails und versprechen Schutzmaßnahmen, Geld, oder sonstige medizinische Dienstleistungen, wenn man auf bestimmte Links klickt oder Dokumente öffnet. Diese Links und Dokumente können Computer infizieren. Gerade in der Hochphase hat sich gezeigt, dass auch häufig Krankenhäuser Ziel der Hackerangriffe wurden. Bei diesen Angriffen verschlüsseln Cyber-Kriminelle Daten mithilfe von Ransomware und legen somit die Infrastruktur lahm. Das passiert gleichermaßen auch bei Unternehmen – immer mit dem Ziel, das Geld gezahlt wird, damit Daten oder der Zugriff auf das gekaperte Netz wieder freigegeben werden.

ICT CHANNEL: *Welche – gegebenenfalls neu entstandenen – Schwachstellen nutzen die Cyberkriminellen dabei genau?*

Dydak: Ein Fokus im Angriffsszenario ist immer der Mensch. Phishing-E-Mails, bei denen auf einen Link zu einer mit Malware gespickten Website geklickt wird, sind beispielweise eine beliebte Attacke von Cyber-Kriminellen. Dabei ist die Qualität der Angriffe deutlich gestiegen – Rechtschreibfehler oder schlechtes Deutsch als Erkennungsmerkmal werden immer seltener.

Quelle: HP

»

Durch die aktuelle Entwicklung sind die Aufgaben der IT-Verantwortlichen dramatisch gestiegen. Zudem hat die Komplexität deutlich zugenommen.

Stefan Dydak
Senior Security Advisor, HP Deutschland

ICT CHANNEL: *Und wie steht es gleichzeitig um die technischen Sicherheitsvorkehrungen der Unternehmen?*

Dydak: Einige Unternehmen waren auf die Dezentralisierung ihrer Mitarbeiter ins Homeoffice schlecht vorbereitet. In den besten Fällen war die VPN-Bandbreite plötzlich zu niedrig, in den schlimmsten mussten die Mitarbeiter auf Privatgeräte zurückgreifen – Wartungs- und Sicherheitslevel ungewiss. Klassische Sicherheitsparadigmen reichen zudem nicht aus, um Geräte und Mitarbeiter in Heimnetzwerken zu monitoren oder zu sichern. Die Angriffsfläche hat durch diese Dezentralisierung drastisch zugenommen – beispielsweise durch den heimischen Router und Drucker. Heimdrucker sind nur in den seltensten Fällen sicher konfiguriert oder mit Sicherheitstechnologie ausgerüstet. Somit sind sie ein gutes Angriffsziel.

ICT CHANNEL: *Sind im Zuge der Corona-Pandemie also die Anforderungen an die Sicherheit gestiegen oder sind bestehende Schwachstellen schlicht offensichtlicher als zuvor?*

Dydak: Wenn ein Großteil der Unternehmens-Hardware außerhalb der Unternehmensmauern genutzt wird, stellt dies Security- oder IT-Teams vor völlig neue Aufgaben. Auch heute noch berücksichtigen viele Firmen beispielsweise Endgeräte nicht ausreichend in ihren Sicherheitskonzepten. Durch die aktuelle Entwicklung sind die Aufgaben der IT-Verantwortlichen dramatisch gestiegen. Zudem hat die Komplexität deutlich zugenommen. Wichtig ist eine detaillierte Analyse des Unternehmens. Welche Prozesse sind kritisch, welche Teile der Infrastruktur müssen unbedingt verfügbar sein. Welche Mitarbeiter spielen zen-

trale Rollen? Und wo sind hier die größten Risiken? Erst wenn man dies weiß, kann man sich auf die relevantesten Risiken konzentrieren.

ICT CHANNEL: *Sie haben bereits erwähnt, dass den Mitarbeiterinnen und Mitarbeitern in den Angriffsszenarien eine zentrale Rolle zukommt. Können technisch unerfahrene Mitarbeiter heute überhaupt noch ausreichend für die oft komplexen und professionell umgesetzten Bedrohungen geschult werden?*
Dydak: Mitarbeiter sollten sich mit den Bedrohungen nicht im Detail auseinandersetzen müssen. Hier sind technische Lösungen gefragt. Wichtig ist die Sensibilisierung der Mitarbeiter auf ein paar kritische Faktoren – beispielsweise dazu, wie ich eine kritische E-Mail oder einen Link erkenne. Zudem sollten Mitarbeiter die wichtigsten Security-Richtlinien kennen und befolgen. Schlussendlich lässt sich auch viel mit gesundem Menschenverstand machen. Wenn es zu schön ist, um wahr zu sein, ist es das wahrscheinlich auch nicht

ICT CHANNEL: *Was sind hingegen die wichtigsten Sercurity-Aspekte, die Unternehmen ins Auge fassen müssen?*
Dydak: Klare Sicherheitsrichtlinien zum Thema Zugangskontrolle und Identitätsmanagement sind essenziell. Eine zentrale Frage ist: Wer benötigt welche Anwendungen und Daten? Schränkt man den Zugriff des Mitarbeiters auf die Anwendungen und Daten ein, reduziert man gleichzeitig das Risiko. Ein Identity- und Access-Management (IAM)-System leistet hier gute Dienste, muss aber natürlich regelmäßig aktualisiert werden. Dies gilt nicht nur für die Zeit im Homeoffice, sondern generell. Prinzipiell sehen wir eine Bewegung von der klassischen Perimetersicherheit zur Identitätssicherheit: Egal, wo der Mitarbeiter ist, das Unternehmen muss diesen sicher authentifizieren und autorisieren können.

Obwohl es selbstverständlich klingt, ist das fehlende Aufspielen aktueller Patches durch die IT-Teams noch immer eines der größten Sicherheitsrisiken. Cyber-Kriminelle dringen nicht selten über bekannte Schwachstellen in das Unternehmensnetzwerk ein. Dazu ist es auch kritisch, defensive Maßnahmen zu ergreifen: Die Überwachung kritischer IT-Instanzen ist wichtig, um potenzielle Angriffe möglichst rasch zu registrieren, sie rechtzeitig einzudämmen und zu eliminieren.

Und wie bereits erwähnt, aber enorm wichtig, sind regelmäßige Schulungen der Mitarbeiter, um sie kontinuierlich hinsichtlich des Themas Sicherheit zu sensibilisieren. Dazu gehören auch Trainings rund um Datenschutzgesetze und -richtlinien, die sich kontinuierlich verändern. ■

Das gesamte Interview mit Stefan Dydak finden Sie online auf ict-channel.com.

Umfrage von Eset

Die gefragtesten Security Services

Firewall, Threat Management and Defense, Verschlüsselung, 2FA oder Patch Management: IT-Security hat sehr viele Facetten. Je nach Größe und Branche sehen Kunden dort Probleme, wo andere sie bereits gelöst haben.

Martin Fryba | 25 Seiten, die tiefen Einblick in das Investitionsverhalten von Unternehmen bezüglich IT-Security geben. ICT CHANNEL zitiert auszugsweise die wichtigsten Ergbnisse aus der Eset-Studie 2020: »Quo Vadis, Unternehmen?« nach einzelnen Security-Aufgaben.

Vier von zehn Unternehmen: »Wir schaffen das«

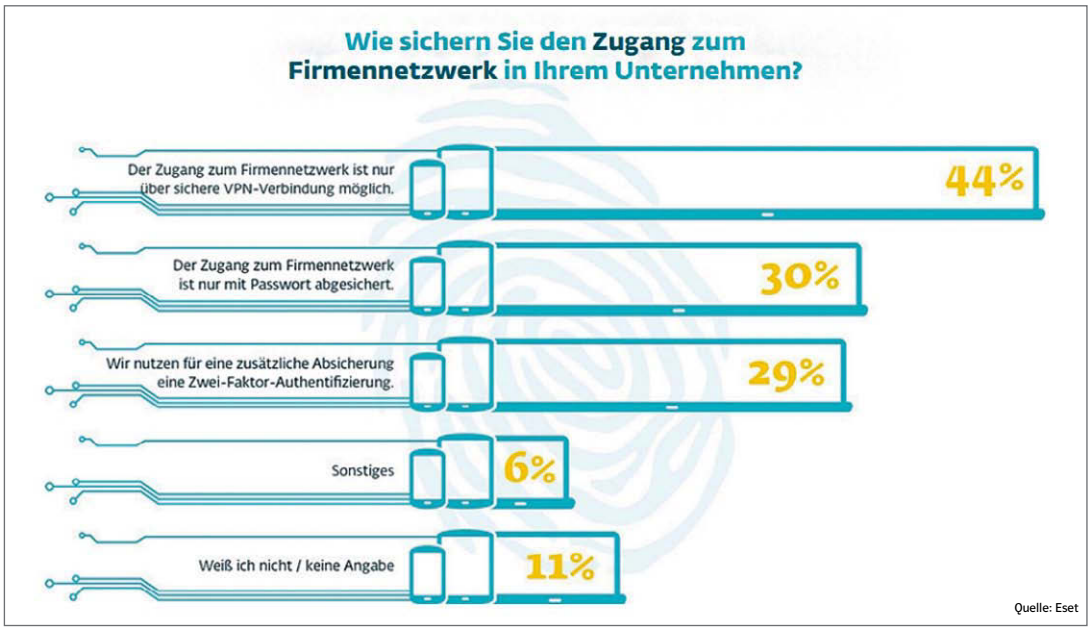
Die Eset-Umfrage unter 520 deutschen und 106 Schweizer Unternehmen, Behörden und Non-Profit-Organisationen ergab, dass 39 Prozent der Studienteilnehmer keine Herausforderung bei IT-Sicherheit sehen. Das gelte vor allem für die Privatwirtschaft: 41 Prozent trauen sich zu, ihre Systeme intern umfassend zu sichern, gefolgt vom Öffentlichen Dienst (36 Prozent) und Non-Profit-Organisationen (31 Prozent). Das Gleiche gelte auch für über die Hälfte der Organisationen im Rechtswesen und unternehmensbezogene Dienstleistungen. Nur das Bauwesen sehe mit Abstand (20 Prozent) die größten Probleme bei der Betreuung.

Firewall

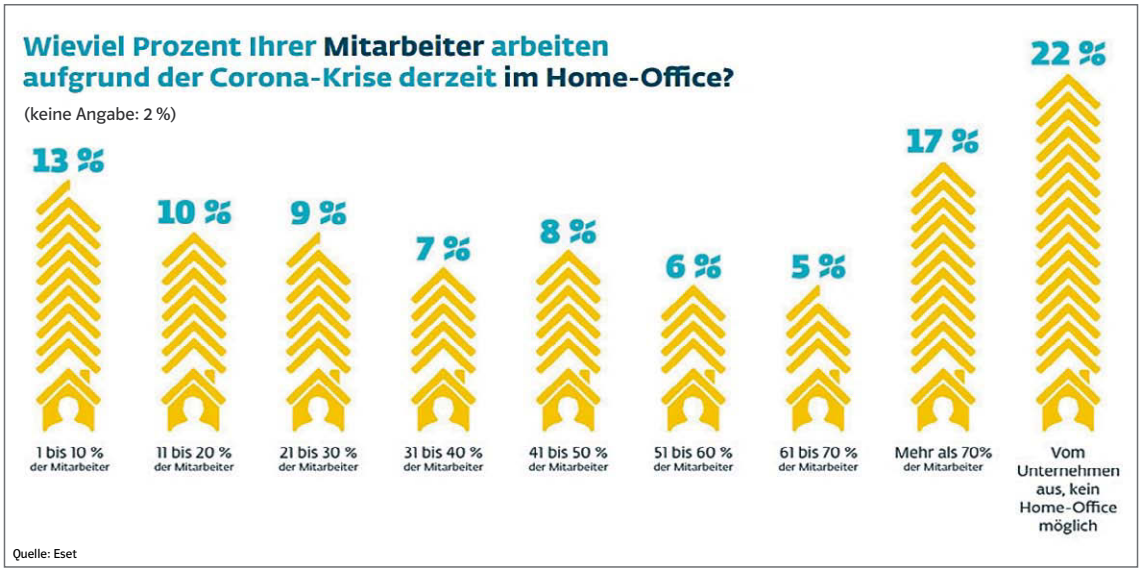
Dennoch habe generell rund jedes sechste Unternehmen am meisten mit der Verwaltung der Firewall zu kämpfen, gefolgt von Penetration Tests und Threat Management (jeweils 16 Prozent), so die Eset-Studie. Im Enterprise-Segment sei die Firewall das geringste Problem (13 Prozent), anders als in den weiteren Umsatzklassen: Hier betreffe es rund jedes fünfte Unternehmen. Auch ein Viertel der kleineren Firmen von 20 bis 49 Mitarbeitern und ein Fünftel der größeren Organisationen mit 250 bis 499 Beschäftigten erachteten das Thema Firewall als zu komplex. Das treffe vor allem für die Branchen Bauwesen (26 Prozent) und Finanzwesen (20 Prozent), am wenigsten auf Dienstleistungsunternehmen (12 Prozent) und den Bildungsbereich (13 Prozent) zu. Letztere fühlten sich ebenso beim Thema Sicherheitstests (27 Prozent) und Gefahrenanalyse (23 Prozent) am meisten überfordert, gefolgt von Unternehmen mit 50 bis 99 sowie 100 bis 249 Mitarbeitern.

Auch Konzerne sehen hier eine Schwachstelle: Ein Fünftel habe weitaus mehr damit zu kämpfen als Firmen, die weniger erwirtschaften. Die höchsten Werte in der Branche verzeichneten laut Eset das Gesundheitswesen (21 Prozent); dicht gefolgt von Gastronomie sowie vom Bildungs- und Rechtswesen (19 Prozent).

Verschlüsselung



Auch Encryption, Patch Management, Multi-Faktor-Authentifizierung und Security Operations werde insgesamt von jedem siebten Unternehmen als zu vielschichtig erachtet, um eine umfassende Betreuung sicherzustellen. Beim Öffentlichen Dienst gebe es in puncto Encryption (23 Prozent) und Security Operations im Vergleich zu den anderen Sektoren (18 Prozent) Ausreißer nach oben. Die Unternehmen mit einem Jahresumsatz von einer bis zehn Millionen würden den Bereich Verschlüsselung (21 Prozent) mit dem größten Aufwand verbunden



sehen, gefolgt von Unternehmen mit höheren Umsätzen (17 Prozent). Dies gelte auch für Firmen mit einer Mitarbeiterzahl von 100 bis 249 sowie 250 bis 499: Ein Fünftel davon würde hier »schneller die Übersicht verlieren«.

Encryption-Lösungen seien vor allem im Gesundheits- und Rechtswesen (26 und 24 Prozent) ein größeres, im Bauwesen (7 Prozent) und in der Unterhaltungsbranche das kleinste Problem.

2FA und Patch Management

Das Thema Multi-Faktor-Authentifizierung (11 Prozent) und Patch Management (12 Prozent) würde bei Behörden und Co. dagegen die Tiefstwerte erreichen, vor allem im Vergleich zu den Non-Profit-Organisationen. Hier verzeichnen MFA (35 Prozent) und Patch Management (20 Prozent) die höchsten Werte von allen Sektoren – in der Privatwirtschaft sind es nur 16 und 15 Prozent. Bis auf das Thema Verschlüsselung (21 Prozent) seien die Ergebnisse (20 bis 24 Prozent) bei gemeinnützigen Organisationen deutlich höher als bei Behörden und Privatunternehmen. Bei ihnen sind auch die Werte im Bereich EDR fast dreimal so hoch (28 Prozent) wie bei den anderen und das Thema sei damit »ein großes internes Problem«, heißt es in der Eset-Studie.

Beim Patch Management seien Unternehmen mit weniger Umsatz überforderter (28 Prozent) als der Rest (12 und 16 Prozent). Allerdings würden beim Patch Management vor allem Unternehmen mit 250 bis 499 Angestellten die größte Komplexität (27 Prozent) sehen, gefolgt von Firmen mit 100 bis 249 und 50 bis 99 Beschäftigten. Mit Blick auf die Umsatzklassen sei das Thema Multi-Faktor-Authentifizierung recht ausgeglichen: Hier lägen alle in einem ähnlichen Bereich (zwischen 17 bis 19 Prozent). Das Gleiche gelte für Security Operations, wobei das Kleinstgewerbe (19 Prozent) und Konzerne (18 Prozent) am meisten damit zu kämpfen hätten, genauso wie Unternehmen mit 100 bis 249 (23 Prozent) und 250 bis 499 Angestellten (21 Prozent).

Eset befragte im April 2.045 Beschäftigte online, das zweite Panel, an dem 520 deutsche und 106 Schweizer Firmen teilnahmen, fand zwischen April und Juli 2020 statt. ■

Ablösung der bestehenden Produkte

Trend Micro modernisiert Endpoint-Security-Portfolio

Trend Micro will sein Angebot an Suiten für Endpoint Security erneuern, übersichtlicher gestalten und Partnern unter anderem im Managed-Services-Bereich neue Werkzeuge an die Hand geben. Das alte Portfolio soll schrittweise abgelöst werden, spätestens aber im zweiten Halbjahr 2021.

Stefan Adelmann | Trend Micro stellt sein Portfolio an Produkten für Endpunktscherheit neu auf, will dieses verschlanken und modernisieren. So sind mit »Apex One SaaS« und »Apex One On-Premise« zwei neue Enterprise-Suiten erhältlich, die das bestehende Portfolio laut Hersteller schrittweise ablösen werden. Beide Suiten basieren auf einem Suscription-Modell, laut Trend Micro reagiere man mit diesem Schritt auf den Wunsch vieler Kunden nach verminderten Investitionshürden. Darüber hinaus können Kunden optional die SaaS-Plattform »XDR« – Extended Detection & Response – hinzubuchen, sowohl Apex One SaaS als auch Apex One On-Premise sind mit ihr entsprechend erweiterbar.

Christina Decker, Head of Channel & Alliances bei Trend Micro Deutschland

Neben den neuen Suiten führt Trend Micro mit »Worry-Free XDR« zudem eine Lösung für Detection & Response ein, die vor allem auf KMU abzielt. Sie soll Erkennungs-, Reaktions- und Ermittlungsfunktionen in einem Agenten bündeln und ist auch als sogenanntes »Co-Managed«-Angebot für MSPs verfügbar. Den Service betreibt dabei Trend Micro selbst, in den Händen der Partner liegen Alarmüberwachung, Incident Response und personalisierte Abhilfemaßnahmen für ihre Kunden. Zudem soll sich für MSPs die Möglichkeit unternehmensübergreifender Analysen bieten, um gegebenenfalls den gesamten Kundenstamm vor ähnlichen Angriffen zu schützen. »Unsere Partner sind die erste Anlaufstelle für viele Unternehmen, die Schwierigkeiten haben, immer mehr Cyberangriffe mit überlastetem Personal und einer großen Anzahl verschiedener Tools abzuwehren«, erklärt Christina Decker, Head of Channel & Alliances bei Trend Micro Deutschland. Mit dem neuen Portfolio möchte der Hersteller ihnen Lösungen bieten, um Unternehmen jeder Größe mit »modernstem Standard« schützen zu können.

Die neuen Suiten sind bereits verfügbar, die bisherigen Produkte werden schrittweise vom Markt genommen. Neugeschäft soll laut Trend Micro noch bis spätestens März 2021 mit bestimmten Suites möglich sein, Renewals teilweise bis zum zweiten Halbjahr 2021. ■

Bullguard VPN

Bullguard erweitert Channel-Angebot um VPN-Lösung

Nicht zuletzt im Homeoffice ist ein VPN (Virtual Private Network) für Unternehmen und Nutzer unerlässlich. Auf die zuletzt gestiegene Nachfrage reagiert Cyber-Security-Anbieter Bullguard nun mit der Erweiterung seines Channel-Portfolios um eine entsprechende Lösung.

Antje Müller, Stefan Adelmann | Mit der Einführung von »Bullguard VPN« in das eigene Channel-Portfolio reagiert Bullguard laut eigenen Angaben auf die gestiegene Nachfrage und Bedeutung von VPNs. Mit der Lösung können Nutzer ihre IP-Adresse verbergen und ISPs, Social-Media-Plattformen und Regierungsorganisationen daran hindern, ihre Online-Aktivitäten nachzuverfolgen. Vollständig privat bleiben darüber hinaus Websites, die ein Anwender besucht, sowie genutzte Anwendungen und Dienste. Außerdem ist eine automatische Verbindung für offene WLAN-Netzwerke enthalten, wie sie in Flughäfen, Hotels und Cafés üblich sind. Seinen Kunden garantiert der Anbieter zudem einen Rund-um-die-Uhr-Support, regelmäßige Software-Updates und eine »No-Logs-Politik«.

Für Reseller soll sich wiederum die Möglichkeit bieten, den schnell wachsenden VPN-Markt auszuschöpfen und gleichzeitig von den Vorabmargen sowie, im Rahmen des Advantage-Partnerprogramms, von einem Umsatzanteil von 25 Prozent bei Lizenzverlängerungen zu profitieren. »Indem wir Bullguard VPN zu unserem Channel-Portfolio hinzugefügt haben, können Reseller jetzt die vollständige Palette an Bullguard-Produkten anbieten und ihren Kunden so einen umfassenden Schutz vor der anhaltenden Flut cyberkrimineller Bedrohungen zur Verfügung stellen«, so Stefan Wehrhahn, Country Manager DACH bei Bullguard.

Bullguard VPN ist für Reseller ab sofort verfügbar und wird in ein-, zwei- und dreijährigen Lizenzpaketen angeboten. Jede Lizenz sichert bis zu sechs Geräte (Desktop-PC, Laptop, Smartphone oder Tablet). Nutzer können dabei zwischen Servern in 16 Ländern wechseln. ■

Datenverlust verhindern

Proofpoint stellt neue Enterprise-DLP-Lösung vor

Proofpoints neue personenbezogene Enterprise-DLP-Lösung (Data Loss Prevention) soll Unternehmen helfen, Datenverlust durch fahrlässige oder böswillige Benutzer zu verhindern sowie kompromittierte Accounts zu erkennen und schnell darauf zu reagieren. Ebenfalls neu ist der »Bexus People Risk Explorer«.

Stefan Adelmann | Proofpoint hat eine neue Enterprise-DLP-Lösung vorgestellt. Sie ist personenbezogen und fasst Inhalte, das Nutzerverhalten und die Bedrohungstelemetrie in einem Interface zusammen. Mithilfe der Lösung können Unternehmen laut dem Anbieter Risiken im Umgang mit Daten, die durch fahrlässige oder böswillige Nutzer oder kompromittierte Accounts entstehen, identifizieren und schnell darauf reagieren. Die Plattform vereint dabei die bestehenden Cloud-, E-Mail- und DLP-Lösungen von Proofpoint. »Daten verlieren sich nicht von selbst – es ist immer ein nachlässiger beziehungsweise böswilliger Benutzer involviert oder sein Account wurde kompromittiert«, erklärt Ryan Kalember, Executive Vice President, Cybersecurity Strategy bei Proofpoint. »Da wir den Menschen in den Mittelpunkt stellen, kann unser personenbezogener Ansatz dort erfolgreich sein, wo frühere Lösungen versagt haben«, so das Versprechen.

Risikomodell auf ML-Basis

Ebenfalls neu im Programm des US-amerikanischen Cyber-Security-Anbieters ist das Tool »Nexus People Risk Explorer«. Es soll Sicherheitsverantwortlichen eine ebenfalls personenbezogene Möglichkeit bieten, besonders gefährdete Benutzer, einschließlich der am intensivsten angegriffenen, verwundbarsten und privilegiertesten Personen einer Organisation, zu identifizieren. Zudem empfehle die Lösung laut dem Anbieter Maßnahmen, um das Risiko anschließend zu verringern. Als Beispiel nennt Proofpoint die Isolierung von URLs in E-Mails von Anwendern, die sowohl häufig Angriffsziel sind als auch bei Phishing-Simulationen gezeigt haben, dass sie wenig sicherheitsbewusst handeln. Das zugrundliegende Risikomodell nutzt dabei maschinelles Lernen und führt die Echtzeit-Bedrohungstelemetrie des hauseigenen Cloud App Security Brokers mit Informationen von E-Mails und Security-Awareness-Trainings zu einem Bedrohungsdiagramm zusammen. ■

Managed Threat Response

Andere informieren Sie nur über Bedrohungen. Wir werden aktiv.

Mit Sophos MTR erhält Ihr Unternehmen 24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service.

JETZT INFORMIEREN
www.sophos.de/mtr

SOPHOS

Die Evolution der Cybersecurity.