www.channelpartner.de 31.1.2017 / 23. Jahrgang / B 13743 / Euro 5,20 IDG 1-2/2017

ChannelPartner

VON IDG

Netzwerke vor unbefugtem Zugriff schützen

CYBER SECURITY

Außerdem:

ISSN 1864-1202

Postvertriebsstück B-13743 Entgelt bezahlt
IDG Business Media GmbH, Lyonel-Feininger-Straße 26, 80807 München

Inhalt

Cyber Security

Mehr zu Cyber Security:
www.channelpartner.de/k/3485

Channel Excellence Awards 2017

Mehr zu den Channel Excellence Awards:
www.channelpartner.de/k/3490

Impressum

Medienhaus:
IDG Business Media GmbH
Lyonel-Feininger-Str. 26,
80807 München
Tel. 089 36086-0,
Fax 089 36086-118
E-Mail: info@idg.de

Chefredakteur:
Dr. Ronald Wiltscheck
(V.i.S.d.P. – Anschrift siehe Medienhaus)

Gesamtanzeigenleiter:
Sebastian Wörle (verantwortlich)
089 36086-113
swoerle@idgbusiness.de

Druck, einschließlich Beilagen:
Dierichs Druck+Media GmbH & Co. KG,
Frankfurter Str. 168, 34121 Kassel

ISSN 1864-1202
Erfüllungsort, Gerichtsstand: München

Inhaber und Beteiligungsverhältnisse:
Alleiniger Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der International Data Group Inc., Boston, USA. Aufsichtsratsmitglieder der IDG Communications Media AG sind Edward Bloom (Vorsitzender) und Toby Hurlstone.

Gründer: Patrick J. McGovern (1937 - 2014)

In unserem Medienhaus erscheinen außerdem folgende Medien-Marken

Cyber-Gefahren 2017: Was sie für den Channel bedeuten

Erpresserische Angriffe, DDoS-Attacken und Identitätsdiebstahl gehören zu den größten aktuellen Gefahren für Unternehmen. Branchenexperten erklären, was Channel-Partner tun müssen, um im Zeitalter von Ransomware und gezielten Attacken erfolgreich zu bleiben.

Text: **Andreas Th. Fischer**, Foto oben: **Negovura und Alexander Supertramp, Shutterstock**

Die Zeiten, in denen sich Unternehmen vor allem vor Script-Kiddies und Hobby-Hackern schützen mussten, sind lange vorbei. Heute sind die Cyber-Kriminellen immer häufiger selbst wie ein straff geführtes Unternehmen organisiert, in dem sich verschiedene Personen und Abteilungen um bestimmte Bereiche kümmern. Wie in einem echten Unternehmen sind ihre Ziele dabei vor allem finanzieller Natur. Alles, was Geld und Erfolg verspricht, wird auch durchgeführt und immer weiter verbessert.

Feind Nummer eins: Ransomware

Eine besondere „Erfolgsstory“ der vergangenen Jahre ist die Ransomware. Die ersten Erpressertrojaner richteten sich noch vor allem an Privatanwender, die vergleichsweise leicht hereinzulegen sind. Heute stehen dagegen Unternehmen im Fokus der Erpresser. Erst schleusen sie ihre Malware ein, verschlüsseln und löschen wertvolle geschäftliche Daten und verlangen anschließend ein „Lösegeld“. Die von ihnen verwendeten

„IT-Security-Know-how ist gefragt.“

Wieland Alge
Vice President und General Manager EMEA, Barracuda Networks

Foto: Barracuda Networks

„Partner werden immer häufiger die ganzheitliche Betreuung des Konzepts übernehmen.“

Mike Rakowski
Head of Business Unit Technology, Also Deutschland

Foto: Also

Techniken werden dabei immer ausgefeilter. Während sich frühe Ransomware teilweise noch relativ einfach überlisten ließ, so dass etwa Entschlüsselungs-Tools bereitgestellt werden konnten, ist dies heute kaum noch möglich. Die Opfer haben dann – sofern es kein funktionierendes Backup gibt – nur noch die Wahl, entweder zu zahlen und damit die Kriminalität weiter zu fördern oder ihre verlorenen Daten abzuschreiben.

Die Bedrohung durch Ransomware ist eines der wichtigsten Themen, das praktisch alle befragten Branchenexperten nennen. So weist etwa Holger Suhl, General Manager DACH bei Kaspersky Lab, darauf hin, dass sich Ransomware-Attacken auf Unternehmen im Jahr 2016 um das Dreifache erhöht haben. „Im Oktober des vergangenen Jahres fand weltweit alle 40 Sekunden ein Cyber-Erpressungsangriff auf ein Unternehmen statt“, nennt Suhl ein schockierendes Beispiel. Er warnt zudem davor, dass es 2017 zunehmend schwieriger werden wird, herauszufinden, wer hinter einer Cyber-Attacke steht. Die Gründe dafür seien nicht nur maßgeschneiderte Angriffe, sondern auch „Attacken unter falscher Flagge und Infizierungen, die nur von kurzer Dauer sind“.

Raphael Labaca Castro, Security Researcher bei Eset Deutschland, stimmt Suhl zu. „Ransomware ist ganz klar unser Favorit. Das kriminelle Geschäft um Verschlüsselungstrojaner wie Locky, TorrentLocker, Jigsaw, TeslaCrypt und Crysis hat sich 2016 als sehr lukrativ erwiesen.“ Aber der Kampf ist seiner Ansicht nach noch nicht verloren. Immerhin habe man für TeslaCrypt und Crysis Entschlüsselungs-Tools entwickeln können, „um die Nutzer aus der Geiselhaft zu erlösen“.

Ins selbe Horn stößt Helmut Nohr, Channel Sales Director bei Sophos Deutschland: „Ransomware wird ein Übel bleiben und tendenziell zunehmen.“ Man müsse allerdings berücksichtigen, dass „die allermeisten Unternehmen nicht von den Hypes gefährdet sind, sondern durch Alltags-Hacks wie zum Beispiel Passwortklau oder Phishing-Mails“. Nohr empfiehlt, dass „wir uns wieder mehr auf die grundsätzlichen IT-Sicherheitsregeln konzentrieren“. Dazu sei eine stringente IT-Security-Strategie die wichtigste Voraussetzung.

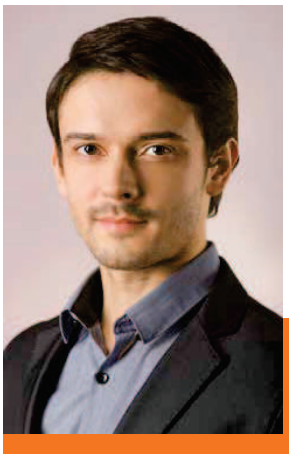
Die wichtigsten Verbreitungswege für Ransomware sind laut Sven Janssen, Regional Director Central Europe bei Sonicwall Deutschland, Spam-Mails, Drive-by-Infektionen und Schwachstellen in Web-Servern. Das Thema gewinne weitere Brisanz, weil viele Verbindungen ins Internet zunehmend verschlüsselt seien. „Die Abwehrmaßnahmen haben keinen Zugriff auf die verschlüsselte Verbindung und greifen deswegen erst, wenn die Schadsoftware schon im Unternehmen ist“, so Janssen. Dann sei es aber meist zu spät. „Ransomware greift ein Unternehmen von innen an“, warnt der Sicherheitsexperte.

Mit ganz neuen Dimensionen bei der Bedrohung durch Ransomware in diesem Jahr rechnet Michael Haas, Area Sales Director Central Europe bei Watchguard Technologies: „Künftig werden sich entsprechende Schadprogramme – ähnlich wie Netzwerkwürmer – über Endlos-Duplikate automatisch weiterverbreiten und ganze Netzwerke infiltrieren.“ Die perfekte Brutstätte für kriminelle Machenschaften seien öffentliche IaaS-Angebote: „Dem Thema Cloud Computing kommt eine besondere Bedeutung zu.“

„Bisher gab es keine Möglichkeit, den Verteidigern höhere Privilegien auf dem Endgerät einzuräumen als den Angreifern. Jetzt schon."

Carsten Böckelmann
Regional Sales Director DACH-NL, Bitdefender

Foto: Bitdefender



„Profis kümmern sich voll und ganz um die Sicherheit der angebotenen Dienstleistung und sind so in der Lage, jederzeit mit neuesten Technologien, Verfahren und Methoden zu reagieren."

Raphael Labaca Castro
Security Researcher, Eset Deutschland

Foto: Eset

Die digitale Erpressung durch gezielte Ransomware-Angriffe bezeichnet auch Christoph Stoica, Regional General Manager bei Micro Focus, als zunehmende Bedrohung für Unternehmen und sogar die ganze Gesellschaft. Weil die Erpresser keine Zahlungen in herkömmlichen Währungen, sondern Bitcoins verlangten, sei das Entdeckungsrisiko für die Täter sehr gering. Stoica machen aber auch die gigantischen Diebstähle von Datenbanken mit Kundeninformationen große Sorgen: „Unberechtigter Zugriff resultierend aus Identitätsdiebstählen ist – neben der Verbreitung von Schadcode – nach wie vor die häufigste Ursache für sicherheitsrelevante Vorfälle in Unternehmen", so der Manager.

Gezielte Datendiebstähle werden auch nach Ansicht von Jörn Kraus, Senior System Engineer bei Westcon Security, in besorgniserregender Weise zunehmen. „Diesen Attacken, bei denen der Angreifer ein ganz bestimmtes Unternehmen ins Visier nimmt, um ganz bestimmte Daten zu stehlen, ist unglaublich schwer beizukommen." Für 2017 rechnet Kraus zudem mit einer rasanten Zunahme an DDoS-Attacken auf Unternehmen. Durch zielgerichtete, hochvolumige Attacken, bei denen einzelne Dienste wie DNS lahmgelegt werden, seien häufig auch andere Unternehmen indirekt betroffen. Gezielte Attacken sieht auch Thorsten Kurpjuhn, Market Development Manager Europe bei Zyxel, im Kommen. Dies bedeute, dass nicht mehr wahllos IT-Systeme angegriffen werden, um „einfach nur Schaden zu verursachen". Kurpjuhn: „Firmen werden direkt angegangen."

Ransomware als Dienstleistung

Auf einen weiteren Trend weist Sascha Plathen hin. Der Director Channel Sales bei Intel Security warnt vor Ransomware-as-a-Service. Seiner Meinung nach erweitert sich die Angriffsfläche, wenn auch ungeschulte Angreifer einen leicht zu bedienenden Dienst mieten und dann versuchen können, eigene Opfer zu finden. Plathen ist überzeugt, dass Ransomware-as-a-Service und individualisierte Ransomware die Sicherheitsbranche vor allem in der ersten Hälfte des Jahres beschäftigen werden. Der Vertriebsexperte weist darauf hin, dass die IT-Sicherheit in Unternehmen oft nicht ausreichend ausgerüstet ist: „Es werden veraltete Standards verwendet, und Ransomware kann einfach in die Systeme eindringen und großen Schaden anrichten." ►

„Schon jetzt ist Ransomware die erfolgreichste Malware aller Zeiten."

Torsten Harengel
Operations Director Security, Cisco Deutschland

Foto: Cisco

Auf die Beweggründe der Cyber-Kriminellen geht Mike Rakowski, Head of Business Unit Technology bei Also Deutschland, ein: „Die Motivation der Angriffe ist heute fast ausschließlich auf wirtschaftliche Interessen zurückzuführen." Darüber hinaus gehe es aber auch darum, Daten zu erlangen und Unternehmen zu blockieren. „Cyber Crime ist ein Markt mit rapider Entwicklung", so Rakowski. Ihm stimmt Torsten Harengel, Operations Director Security bei Cisco Deutschland, zu, der Ransomware als „profitables Geschäftsmodell" bezeichnet: „Schon jetzt ist es die erfolgreichste Malware aller Zeiten."

Für dieses Jahr rechnet Harengel damit, dass die Cyber-Kriminellen versuchen werden, „insbesondere die Verbreitung der Schadsoftware zu optimieren". Wie Intel-Director Plathen kritisiert Harengel „Software, die nicht auf dem neuesten Stand gehalten wird". Zurückzuführen sei dies oft auf einen Mangel an Personal im Bereich Cyber Security und dem damit fehlenden Know-how in Unternehmen.

„Alleine kann kein Sicherheitsanbieter für vollständigen Schutz sorgen."

Sascha Plathen
Director Channel Sales, Intel Security

Foto: Intel

Sorgen bereiten auch Amir Alsbih, Chief Operating Officer bei KeyIdentity, die vielen Systeme in Unternehmen, die nicht auf dem aktuellen Stand sind. „Das Zeitfenster von der Veröffentlichung von Sicherheits-Patches bis zum Einspielen auf den Systemen kann einem Generalschlüssel gleichkommen." Viele Grundprozesse wie Patch-, Change- und Release-Management seien „suboptimal". Außerdem existiere in vielen Unternehmen kein Perimeter mehr, den man mit Mauern schützen könne. Das gefährde die Sicherheit enorm.

Zunehmende Bedrohung durch IoT

Eine weitere Gefahr beschreibt Carsten Böckelmann, Regional Sales Director DACH-NL bei Bitdefender: „Viele aktuelle Bedrohungen haben ihre Ursachen in der sich wandelnden IT. Virtualisierung, Vernetzung und das Internet der Dinge bestimmen die Entwicklung." Böckelmann sieht „fallende Grenzen zwischen persönlicher und beruflicher Nutzung, öffentlichem und unternehmenseigenem Netzwerk, Premises- und Cloud-Strukturen." Seine eindringliche Warnung lautet: „So finden Angreifer täglich neue Lücken, in die sie vorstoßen können."

Für 2017 rechnet Böckelmann mit einem „weiterhin exponentiellen Anstieg von Angriffen, egal ob das nun Advanced Persistent Threats, digitale Erpressungen oder DDoS-Angriffe auf Infrastrukturen sind". Die Sicherheitsmechanismen von Unternehmen würden dadurch stündlich auf die Probe gestellt.

„IoT wird 2017 verstärkt in den Fokus der Hacker geraten", ist auch Sven Janssen, Regional Director Central Europe von Sonicwall, überzeugt. Fehlende Sicherheitsstandards machten ihnen erfolgreiche Attacken relativ einfach. Besonders bei kritischen Infrastrukturen wie Energie, Wasser, Transport und Verkehr könne ein Angriff unvorhersehbare und vor allem weitreichende Folgen für Unternehmen und Verbraucher mit sich bringen. „In diesem Zusammenhang sind auch Szenarien denkbar, in denen ein Botnetz, das aus einer beliebigen Zahl von Smartphones weltweit besteht, Attacken auf Unternehmen oder andere Einrichtungen ausführt", warnt Janssen. Die Wahrscheinlichkeit sei deshalb so hoch, weil viele Smartphones nicht durch Sicherheits-Software geschützt seien.

Es liegt auf der Hand, das auch die Software in vielen IoT-Geräten aktualisiert werden sollte. Darin ►

„Security-Dienstleister haben das Know-how, ihre Kunden hier zu unterstützen.“

Sven Janssen
Regional Director Central Europe, Sonicwall
Foto: Sonicwall

sieht Christoph Stoica von Micro Focus jedoch auch ein Problem: „Für das Einspielen solcher Updates muss das System auf das Internet zugreifen. Ein Angreifer könnte sich als Update-Server ausgeben und auf diesem Weg einen Trojaner installieren.“ Auch Wieland Alge, Vice President und General Manager EMEA bei Barracuda Networks, ist der Meinung, dass Hersteller und Anwender kaum in der Lage sind, IoT-Geräte sicher zu produzieren und einzusetzen: „Die Vernetzung durch das Internet der Dinge und Industrie 4.0 bietet Cyber-Kriminellen von Tag zu Tag größere Angriffsflächen.“

Weil die Kosten für digitale Angriffe gesunken sind, geraten vermehrt Mittelständler und Kleinstunternehmen in den Fokus der Cyber-Kriminellen. „Die Robustheit von mittelständischen IT-Infrastrukturen wird 2017 harten Praxistests ausgesetzt“, warnt der Barracuda-Manager.

Nichtsdestotrotz muss die Absicherung des Internet of Things und der rasant wachsenden Industrie 4.0 oberste Priorität bleiben, betont Jörn Kraus von Westcon Security. „Der groß angelegte Angriff auf Telekom-Router vor einigen Wochen war nur ein erster Vorgeschmack auf die Attacken, mit denen wir 2017 rechnen müssen.“

„Zeigen Sie, dass Sie in der Lage sind, eine angepasste Dienstleistung zu liefern und nicht ausschließlich ein Schema F zu bedienen.“

Amir Alsbih
Chief Operating Officer, KeyIdentity
Foto:KeyIdentity

Auch Raphael Labaca Castro von Eset Deutschland sieht Gefahren im IoT: „Der Trend zeichnet sich ab, alles zu hacken, was in irgendeiner Weise vernetzt und smart ist.“ Im vergangenen Jahr sei es Hackern bereits gelungen, größere Infrastrukturen lahmzulegen. Das beste Beispiel dafür sei der Trojaner BlackEnergy, der 1,4 Millionen Menschen in der Ukraine vom Strom abgetrennt habe. Auch in Bayern sei ein Atomkraftwerk mit der Malware Win32/Ramnit und Win32/Conficker infiziert worden. Die betroffenen Systeme seien zwar nicht online gewesen, die Infektionen hätten sich aber leicht über USB-Sticks verbreiten können.

Alexander Noffz, Channel Manager EMEA Central bei Ping Identity, sieht dagegen das Ende einer auf Passwörter und Logins fokussierten IT-Sicherheit nahen. „Die Identität eines jeden Geräts, einer Person oder Applikation sollte der Dreh- und Angelpunkt für die konsolidierte Identifikation sein.“ Nur so könne verhindert werden, dass unberechtigte Personen einen Zugriff auf Daten, Geräte oder Anwendungen erhalten.

Wie sich der Zugang zu den Kunden verbessern lässt

Der wichtigste Nutzen von IT-Security ist in den Augen von Barracuda-Networks-Manager Alge die Hochverfügbarkeit geschäftskritischer Prozesse. Zum Schutz gegen die heutige Bedrohungslandschaft benötigen Unternehmen seiner Ansicht nach drei Komponenten, die sie von ihren Dienstleistern und Partnern erhalten können: „Erstens eine Next Generation Firewall in der gesamten eigenen Infrastruktur, die nicht länger auf On-Premises beschränkt ist, sondern auch IaaS-Clouds umfasst. Zweitens E-Mail-Security in einer zeitgemäßen Form, die auch SaaS-Anwendungen wie Office 365 schützt. Und drittens Backup inklusive der Sicherung aller Cloud-Ressourcen.“ Eine zuverlässige Backup-Infrastruktur sei als „letzte Verteidigungslinie“ unerlässlich. Auf ►

die Frage, wer sich um IT-Security kümmern sollte, antwortet Mike Rakowski, dass das Thema „in vielen Unternehmen bereits zur Chefsache erklärt wurde“. Security-Dienstleistern und interessierten Resellern rät er, sicherzustellen, dass sie ausreichend Know-how bereitstellen können und beim Endkunden präsent sind. „Ein ganzheitlicher Ansatz wird immer wichtiger, also der Schutz der User von innen und außen“, plädiert der Also-Deutschland-Manager.

„Kein Sicherheitsanbieter kann allein mit Software allen Anforderungen von Unternehmen entsprechen.“

Holger Suhl
General Manager DACH, Kaspersky Lab
Foto: Kaspersky

Lücken schließen und neue verhindern

Carsten Böckelmann von Bitdefender empfiehlt Dienstleistern, ihren Kunden anzubieten, die gesamte IT-Infrastruktur daraufhin zu untersuchen, ob es ungesicherte Zugänge ins Netzwerk gibt. Böckelmann: „Dann gilt es, diese Lücken dauerhaft zu schließen und mit Prozessen, zum Beispiel Einkaufs- oder Support-Prozessen, dafür zu sorgen, dass keine neuen Schwachstellen entstehen.“ Der Manager empfiehlt, auch gelegentlich nichtklassische Wege zu probieren, um mit Kunden ins Gespräch zu kommen. „Einfache Fragen wie ‚Haben Sie eine Überwachungskamera?‘ und ‚Haben Sie die schon einmal gepatcht?‘ können Türen öffnen“, lautet Böckelmanns Ratschlag.

Sicherheitsspezialist Torsten Harengel von Cisco Deutschland sieht den besten Weg für Dienstleister darin, das eigene Security-Portfolio auszubauen: „Ein starkes Herstellernetz kann helfen, auf neueste Security-Entwicklungen schnell zu reagieren.“ Das Ziel müsse aber in jedem Fall eine „integrierte Security-Architektur ohne Silo-Lösungen sein, die mit Hilfe von Schnittstellen Verbindungen aller Security Lösungen ermöglicht und dem Kunden am Ende einen ganzheitlichen Überblick und entsprechende automatisierte Handlungs-Optionen bietet“.

Auch Sascha Plathen empfiehlt ein konzertiertes Vorgehen: „Die IT-Sicherheitsbranche beginnt zu verstehen, dass man diesen Bedrohungen nur zusammen entgegentreten kann.“ Nicht jeder könne ein Spezialist in jedem Bereich sein. „Alleine kann kein Sicherheitsanbieter für vollständigen Schutz sorgen“, so der Intel-Security-Manager. Je mehr Sicherheitsdienstleister zusammenarbeiteten, desto besseren Schutz könnten sie den Kunden bieten.

Software allein genügt nicht mehr

Dienstleister und Reseller sollten vor allem Antworten auf elementare Fragen geben können, die viele Kunden derzeit beschäftigen, ist Kaspersky-Lab-Mann Holger Suhl überzeugt. Er nennt ein paar Beispiele: „Wie vermeidet man Mitarbeiterfehler? Wie lassen sich Daten, die das Unternehmen bereits verlassen haben, weiterhin schützen? Und wie sollte man auf fundamentale Mängel in der IT-Infrastruktur reagieren?“ Kein Sicherheitsan-

„Entscheidend für eine bessere und effektivere Abwehr von Bedrohungen und Datenmissbrauch ist die Verkürzung von Reaktionszeiten auf Sicherheitsvorfälle.“

Christoph Stoica
Regional General Manager, Micro Focus
Foto: Micro Focus

bieter könne allein mit Software allen Anforderungen entsprechen, denen Unternehmen heute gerecht werden müssten.

Kompetenz auszustrahlen ist der Tipp von KeyIdentity-COO Amir Alsbih. Security-Dienstleister sollten demonstrieren, dass „sie die richtigen Leute haben, um entsprechende Probleme zu lösen“. Auf Kundenspezifik komme es an: Wichtig sei zu zeigen, dass man „in der Lage ist, eine angepasste Dienstleistung zu liefern und nicht ausschließlich ein Schema F zu bedienen“. Nur mit Technologie alleine könne man keine Probleme lösen. Vielmehr rät Alsbih, zu „analysieren, was die Hauptursache für die Probleme bei einem Unternehmen ist“. Dabei gehe es vor allem darum, methodisch an die Themen heranzugehen und „das Vorgehen durch eine Kombination von Risiko- und Bedrohungsanalysen zu verankern“.

„Von alleine kommen Kunden nur selten“, sagt Sophos-Deutschland-Director Helmut Nohr mit einem Augenzwinkern. Dem Channel empfiehlt Nohr folgende Maßnahmen: „Zielgruppenanalyse, Analyse der eigenen Stärken, Ressourcen-Check, Einbinden von Marketing,

„Beratung, Beratung und nochmals Beratung.“

Jörn Kraus
Senior System Engineer bei Westcon Security

Foto: Westcon Security

einen Action-Plan sowie eine Kontrolle der eingeleiteten Maßnahmen.“ Nohr: „Der Markt ist umkämpft; eigene Aktivität ist unabdingbar.“ Nach Meinung von Zyxel-Marktentwickler Thorsten Kurpjuhn ist zunächst meist etwas Aufklärung notwendig. Teilweise sei das Bewusstsein für die Gefahren noch nicht vollständig entfaltet. Kurpjuhn: „Eine IT-Security-Lösung sollte ganzheitlich auf das Netzwerk ausgerichtet sein, so dass ein Firmeninhaber auch die Zusammenhänge einordnen kann.“

„Entwickeln Sie bei Ihren Kunden ein Bewusstsein für den Wert ihrer Daten und digitalen Identitäten."

Alexander Noffz
Channel Manager EMEA Central, Ping Identity

Foto: Ping Identity

Einen 100-prozentigen Schutz gibt es nicht

Sich nicht alleine auf die Technologie zu verlassen, ist auch der Rat von Micro-Focus-Regionalchef Christoph Stoica. „Egal wie technologisch ausgereift zukünftige Sicherheitslösungen auch sein mögen, einen hundertprozentigen Schutz vor Cyber-Angriffen werden sie nie leisten können." Stattdessen komme es darauf an, die Effektivität bei den angewendeten Abwehrmaßnahmen zu verbessern, sie schneller anzupassen und zu versuchen, die Angriffsmuster besser zu erkennen. Hier brauchen die Anwender persönliche Untersützung: „Security-Dienstleister müssen reagieren und verstärkt Beratungsleistungen und Angebote für eine ganzheitliche, prozessorientierte Betrachtung der Informationssicherheit entwickeln."

„Health-Checks sind ein probates Mittel, um weitere Maßnahmen einleiten zu können."

Helmut Nohr
Channel Sales Director, Sophos Deutschland

Foto: Sophos

Alexander Noffz von Ping Identity rät Dienstleistern, bei den Kunden ein „Bewusstsein für den Wert ihrer Daten und digitalen Identitäten" zu entwickeln. Ansätze wie die authentizitätsbasierte Authentifizierung würden sicherstellen, dass nur berechtigte Personen den Zugriff auf „ihre" Anwendungen erhalten. Bei den Kunden implementierte Lösungen sollten nach Empfehlung von Noffz „so einfach und komfortabel wie möglich, gleichzeitig aber effizient und automatisiert funktionieren".

Gute Zeiten für Security-Dienstleister sieht Michael Haas von Watchguard Technologies heraufziehen. „Sicherheit wird in Unternehmen zunehmend strategisch betrachtet, zumal fast jeden Tag neue Schlagzeilen von Datenpannen die Runde machen." Insbesondere vor dem Hintergrund der neuen EU-Datenschutz-Grundverordnung und anderen Aspekten wie der digitalen Transformation lasse sich das Thema optimal positionieren. Trotz der Vielschichtigkeit der Herausforderungen gelte es hier, die Anwender nicht zu überfordern: „In diesem Zusammenhang darf die Komplexität aber nicht überhandnehmen." Obwohl das Ziel eine umfassende Gefahrenabwehr sein müsse, sollte sich die Sicherheitsarchitektur intuitiv beherrschen und auf einen Blick erfassen lassen.

Für den Fall der Fälle, dass es doch einmal zu einem erfolgreichen Angriff gekommen ist, sollten Dienstleis-

ter eine „zeitnahe und umfassende Incident-Response-Strategie entwickeln“, rät Westcon-Security-Ingenieur Jörn Kraus. Hierzu gehöre es unter anderem, die Architektur möglichst redundant aufzusetzen, Prozesse und Anforderungen klar zu dokumentieren und ein dediziertes Incident-Response-Team für Notfälle zu berufen. „Am besten mit einem Mix interner und externer Experten“, so Kraus. „Aufklären und Awareness schaffen ist das A und O – gerne auch mit unkonventionellen Mitteln, so etwa mit der Simulation von Angriffsszenarien.“

Lukrative Security-Services

Eine besondere Art von Gesundheitstests für Unternehmen anzubieten, bei der der Partner die Ist-Situation des Kunden analysiert, lautet der eindringliche Rat von Helmut Nohr. „Diese Health-Checks sind ein probates Mittel, um weitere Maßnahmen einleiten zu können“, erläutert der Sophos-Deutschland-Manager seinen Vorschlag. Darüber hinaus empfiehlt er, Mitarbeiterschulungen für die Kunden ins Programm aufzunehmen. Zu sorgloser Umgang mit sensitiven Daten und das Nichteinhalten der Unternehmensrichtlinien seien die wichtigsten Gründe für Erfolge der Cyber-Kriminellen.

Mit der zunehmenden Virtualisierung beschäftigt sich dagegen Carsten Böckelmann von Bitdefender. In diesem Jahr würden erstmals Sicherheitsprodukte herauskommen, die auf Hypervisor-Ebene laufen und so virtuelle Maschinen besser sichern können. „Bisher gab es keine Möglichkeit, den Verteidigern höhere Privilegien auf dem Endgerät einzuräumen als den Angreifern. Jetzt schon.“ Wenn Malware sich nicht mehr verstecken und tarnen könne, verschaffe dies den Sicherheitsverantwortlichen eine dringend benötigte Verschnaufpause.

Die größte Chance für Dienstleister sieht Böckelmann darin, dass viele Kunden kaum noch Zeit finden, sich mit den vielen Angriffsvektoren und den zahlreichen, ineinandergreifenden Sicherheitsangeboten ausreichend zu beschäftigen. „Langfristig ist es für sie effizienter, das Sicherheits-Management vollständig an Dienstleister auszulagern.“

Dieser Ansicht stimmt auch Mike Rakowski von Also Deutschland, zu. Für viele Unternehmen sei es schwer, eigenes Know-how für den Bereich IT-Security aufzubauen. Rakowski: „Partner werden deswegen immer häufiger die ganzheitliche Betreuung des Konzepts übernehmen." Darüber hinaus könnten Security-Awareness-Maßnahmen sowie Trainings und Kampagnen entscheidend zum Schutz der User und Unternehmen beitragen.

Dienstleistungen im Cyber-Sicherheitsbereich, Schulungsprogramme für Mitarbeiter und Trainings auf höherem Niveau für Sicherheitsexperten empfiehlt auch Holger Suhl von Kaspersky Lab. Darüber hinaus können seiner Ansicht nach Informationen zur Bedrohungslandschaft die hausinterne Cyber-Sicherheit verbessern. Weitere interessante Bereiche seien eine Unterstützung der Kunden bei der Durchführung von Penetrationstests, der Einhaltung behördlicher Auflagen sowie gängiger Branchen- und Unternehmensstandards wie zum Beispiel PCI DSS (Payment Card Industry Data Security Standard).

Ausbau der Beratungsleistungen

„Beratung, Beratung und nochmals Beratung", fasst Jörn Kraus von Westcon Security seine Empfehlungen knapp und prägnant zusammen. „Die Technologien, die Infrastrukturen und die Bedrohungen sind heute so komplex, dass es selbst für große Unternehmen mit eigenen IT-Abteilungen extrem schwer ist, ihr Security-Standing und ihre Schwachstellen korrekt zu bewerten und die IT an den richtigen Stellen zu verstärken." Der Beratungsbedarf sei daher enorm. Die Wünsche der Anwender reichten von Analysen der Schatten-IT über das Assessment der Network Security bis hin zu Consulting-Angeboten rund um die europäische Datenschutzgesetzgebung. Kraus: „In all diesen Bereichen können Security-Integratoren ihr Business heute mit überschaubarem Vertriebsaufwand deutlich ausbauen und ganz nebenbei den Boden für weiterführende Security-Projekte bereiten."

„Beratungsdienste in verschiedenen Ausführungen" hält auch Ping-Identity-Manager Alexander Noffz für ein zukunftsträchtiges Geschäftsfeld. „Das beginnt beim Design der einzelnen Lösung sowie ihrer Implementierung und setzt sich über fortlaufende Anpassungen einzelner Software-Applikationen fort." Je nachdem, ob die betreffenden Lösungen beim Anbieter oder beim Kunden betrieben werden, könnten Partner ihre Mitarbeiter auch an Unternehmen ausleihen, um dann vor Ort den laufenden Betrieb sowie etwaige Änderungen zu verwalten.

Wie individuelle Lösungen das Portfolio erweitern können

Eigene Lösungen zu entwickeln, die nicht von der Stange sind, rät Raphael Labaca Castro von Eset Deutschland allen Security-Dienstleistern. Wer als Kunde nicht die nötigen Ressourcen oder das Personal für eine umfassende Sicherheitsarchitektur besitzt, der greife gerne auf Managed Services zurück. „Die Profis kümmern sich dann voll und ganz um die Sicherheit der angebotenen Dienstleistung und sind so in der Lage, jederzeit mit neuesten Technologien, Verfahren und Methoden zu reagieren", sagt Castro.

Individuell ausgefeilte Managed Services bieten auch nach Meinung von Intel-Manager Sascha Plathen einiges Potenzial: „Partner können mit maßgeschneiderten Ergänzungen ihr Geschäftsmodell ausbauen und ihren Kunden als vertrauenswürdiger Sicherheitsberater zur Seite stehen." Konsequente Vorbeugung etwa bei Bedrohungen durch Ransomware lautet hin-

„Künftig werden sich entsprechende Schadprogramme über Endlos-Duplikate automatisch weiterverbreiten und ganze Netzwerke infiltrieren."

Michael Haas
Area Sales Director Central Europe, Watchguard Technologies

Foto: Watchguard Technologies

„Eine IT-Security-Lösung sollte ganzheitlich auf das Netzwerk ausgerichtet sein."

Thorsten Kurpjuhn
Market Development Manager Gateway – Europe, Zyxel

Foto: Zyxel

gegen der Rat von Sonicwall-Regionaldirektor Sven Janssen: „Maßnahmen erst im Moment des Angriffs einzuleiten, greift zu kurz." Stattdessen sollte bereits bevor es zu Attacken gekommen sei „intensive Aufklärungsarbeit betrieben werden, um ein angemessenes Bewusstsein für die Problematik zu schaffen". Unter anderem empfiehlt Janssen gezielte, zielgruppengerechte Awareness-Schulungen, um das Sicherheitsbewusstsein der Mitarbeiter zu schärfen. „Security-Dienstleister haben das Know-how, ihre Kunden hier zu unterstützen."

Auf einen anderen Punkt will Christoph Stoica von Micro Focus die Aufmerksamkeit lenken: „Entscheidend für eine bessere und effektivere Abwehr von Bedrohungen und Datenmissbrauch ist die Verkürzung von Reaktionszeiten auf Sicherheitsvorfälle." Moderne SIEM-Lösungen (Security Information and Event Management) ermöglichten eine umfassende Auswertung aller Sicherheitsinformationen und könnten durch Korrelation auch automatisiert Gegenmaßnahmen einleiten. Partnern empfiehlt auch Stoica, Managed Services anzubieten: „Oft verfügen Kunden nicht über das erforderliche Personal und/oder die notwendige Kompetenz, um die aus den aufbereiteten Informationen gewonnenen Erkenntnisse in konkrete Gegenmaßnahmen umzusetzen."

Auch Michael Haas von Watchguard Technologies hält verständlich aufbereitete Security-Informationen für essenziell und betont die Bedeutung von Threat Intelligence (TI). Es gehe dabei vor allem darum, Security-Events im Netzwerk und am Endpunkt mit detaillierten Analysen der Bedrohungslage in Verbindung zu setzen. „Dadurch lassen sich potenzielle Angriffe früher erkennen und priorisieren." Entsprechend geschnürte Pakete würden allen Beteiligten „einen klaren Mehrwert bieten". Die klassische Firewall als Single-Purpose-Lösung sei jedenfalls längst nicht mehr zeitgemäß: „Im Zuge der immer ausgefeilteren Angriffsmethoden müssen sich auch die Sicherheitstechnologien weiterentwickeln."

Wieland Alge von Barracuda Networks empfiehlt ebenfalls, über Produkte und ihre Konfiguration hinauszudenken: „IT-Security-Know-how ist gefragt." Ein funktionierendes Restore- und Backup-Management sowie ein umfassendes Monitoring böten einen hohen zusätzlichen Nutzen für die Kunden, denen sich die Sicherheitsexperten dadurch dauerhaft verbinden könnten: „Auf diese Weise können Dienstleister einen langfristigen Cashflow erreichen."

Fazit

Unsere Security-Umfrage unter erfahrenen Experten aus der Branche hat gezeigt, dass ihnen in diesem Jahr vor allem Ransomware und DDoS-Angriffe Sorgen bereiten. Aber auch die Absicherung des Internets der Dinge muss 2017 Priorität haben. Der Angriff auf mehr als eine Million Telekom-Router im vergangenen Jahr legt nahe, dass hier noch einige Aufgaben zu erledigen sind.

Für Partner bieten sich 2017 zahlreiche Chancen, wenn sie bereit sind, ihre Managed Services, ihre Schulungsangebote und ihre Beratungsleistungen auszubauen. Der reine Fokus auf Produkte und Technologien hat jedenfalls keine Zukunft mehr. In diesem Punkt sind sich praktisch alle Branchenexperten einig. ■