BILD: COLIN FEARING - STOCK.ADOBE.COM

IT-Security gehört generalüberholt

Das Datenwachstum setzt sich ungebremst fort und bringt Sicherheitsrisiken mit sich. Um sie einzudämmen, ist ein Umdenken in Sachen Security erforderlich. Managed Security Services Provider (MSSPs) rücken dadurch in den Fokus.

Die weltweite Datenmenge wächst in einem nie dagewesenen Tempo. Das Internet der Dinge (IoT), Künstliche Intelligenz (KI) und die zunehmende Bedeutung von Edge Computing sind wesentliche Katalysatoren für den enormen Anstieg des weltweiten Datenvolumens. Verwalteten Unternehmen 2016 circa 1,45 Petabyte an Daten, waren es 2019 bereits 13,5 Petabyte, was einem Anstieg von 831 Prozent entspricht. Zu diesem Ergebnis kam die im März dieses Jahres erschienene Dell-Studie „Global Data Protection Index 2020 Snapshot". Eine große Bedrohung für diese Daten ist die steigende Anzahl von Störereignissen wie Cyberattacken oder Systemausfälle. Waren im Jahr 2018 noch 76 Prozent der befragten Unternehmen von solchen Ereignissen betroffen, galt das im Jahr 2019 bereits für 82 Prozent. Und auch die Kosten, die den Unternehmen durch diese Störereignisse entstehen, steigen rasant. So betrugen die geschätzten jährlichen Kosten für Ausfallzeiten 2019 im Durchschnitt rund 719.000 Euro. Im Jahr 2018 lagen sie noch bei rund 467.000 Euro.

Mit dem rasanten Datenwachstum gehen neue Herausforderungen einher: So glaubt der Dell-Studie zufolge die große Mehrheit, dass aktuelle Datensicherheitslösungen ihren zukünftigen Geschäftsanforderungen nicht mehr gerecht werden. Mobiles Arbeiten, die zunehmende Migration von Anwendungen in die Cloud sowie die Arbeit aus dem Homeoffice, die für viele Unternehmen während der Coronakrise Existenz bestimmend ist, lassen die Komplexität in puncto Datensicherheit weiter ansteigen. Denn wie bereits in Klagen gegen Plattformanbieter offensichtlich wurde: Bei dem Ad-hoc-Umstieg zur Remote-Arbeit wurden nicht alle Aspekte des Datenschutzes und der Datensicherheit berücksichtigt. „Die Nachfrage nach einem sicheren Remote-Zugriff und starker Authentisierung auf das Unternehmensnetzwerk und die dafür notwendigen technischen Voraussetzungen ist momentan – insbesondere in Corona-Zeiten – am höchsten. Aufgrund vielschichtiger und komplexer IT- und Compliance-Anforderungen verfügen insbesondere viele mittelständische Unternehmen noch über kein belastbares Home-

office-Konzept", betont Wolfgang Kurz, Gründer und CEO bei Indevis. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet aktuell eine Zunahme von Cyberangriffen mit Bezug zum Coronavirus auf Firmen und Bürger. Auch neue Technologien wie Künstliche Intelligenz (KI) und Machine Learning (ML), der 5G-Mobilfunk und Cloud-Edge-Infrastrukturen werden die Datensicherheit weiter verkomplizieren.

Der Fachkräftemangel, vermehrte Cyber-Angriffe, die damit verbundenen hohen Kosten sowie die daraus resultierenden steigenden Sicherheitsbedenken lassen Managed Security Services (MSS) an Bedeutung gewinnen. Das bestätigen auch die Zahlen: Beliefen sich die weltweiten Ausgaben für Security Services 2019 auf rund 62 Millionen US-Dollar, schätzt das Marktforschungsunternehmen Gartner die Ausgaben im Jahr 2022 auf 78 Millionen US-Dollar.

Auch laut dem diesjährigen „Managed Services Trends Report" von Solarwinds bieten Managed Security Services das größte Wachstumspotenzial. Zu den in Europa am meisten angebotenen und genutzten Security-Lösungen zählen Virenschutz (93 %), Datensicherung und -wiederherstellung (82 %), Firewalls (82 %) sowie Spamschutz (80 %). In Nordamerika waren die Befragten am zuversichtlichsten, was das Angebot und die Nutzung von Virenschutz (89 %), Firewalls (83 %), Datensicherung und -wiederherstellung (81 %) sowie Endpunktsicherheit (75 %) angeht.

Bei einigen ausgefeilteren Sicherheitslösungen ist das Angebot jedoch noch ausbaufähig. Veredelte Services in Biometrik, Security Broker für den Cloud-Zugriff (CASBs) und digitales Rechtemanagement sind komplexe Leistungen, in denen der Studie zufolge noch großes Wachstumspotenzial steckt. Dienstleistungen, mit denen sich Befragte in Europa laut eigener Aussage am wenigsten auskennen, sind Penetrationstests (52 %), Audits und Compliance-Management (39 %) und Risikoabschätzungen (36 %). Nordamerikanische Befragte nennen hier Audits und Compliance-Management (53 %), Penetrationstests (47 %) und Sicherheitssystemarchitektur (39 %).

Im Lichte wachsender Cybergefahren und eines zunehmenden Problembewusstseins sind Sicherheitsdienste heute eine schiere Notwendigkeit, zumal kriminelle Hacker inzwischen auch MSPs ins Visier nehmen. „Je größer die Komplexität der IT beim Kunden ist, desto wichtiger ist das übergreifende Security-Knowhow durch einen Managed Security Services Provider", betont Norbert Book, Geschäftsführer und Management Consultant bei Consecur. Laut Book werden neben klassischen Security Services wie Virenschutz und Anti-Spam, auch „Services zur Erkennung von Angriffen (Intrusion Detection System) oder das Auffinden von Schwachstellen (Vulnerability Management) an Bedeutung gewinnen. SIEM (Security Information and Event Management) in Kombination mit Schwachstellenmanagement und SOAR (Security Orchestration Automation and Response) sind notwendige Managed Security Services." Auch Indevis-CEO Kurz sieht die steigende Bedeutung von Managed Security Services: „Nach wie vor zählt Ransomware zu den größten Bedrohungen. Solche Angriffe sind auch für weniger versierte Cyberkriminelle heute recht einfach durchzuführen. Eine gute Malware Protection muss daher immer Teil eines erfolgreichen Sicherheitskonzepts sein. Punktuelle Security aus der Steckdose gibt es jedoch nicht. Der Trend geht in Richtung eines integrierten Sicherheitskonzepts auf Basis von Managed Services. Nur wenn erstens Technik, zweitens Prozesse, Organisation und Schnittstellen sowie drittens Benutzer-Awareness gleichermaßen berücksichtigt werden, kann ein erfolgreicher Schutz gegen Cyberangriffe gelingen."

Doch liegt genau hier eine große Herausforderung für Managed Security Services Provider (MSSPs): „Kunden müssen sich trauen, einen MSSP zu beauftragen. Hierzu muss ein Vertrauensverhältnis zwischen Kunden und Service Provider vorhanden sein. Immerhin erhält ein externer Dienstleister tiefe Einblicke in die Infrastruktur des Unternehmens. Daher muss eine vor-

BILD: CONSECUR

Norbert Book,
CEO und Management Consultant bei Consecur

Zur Qualität von Managed Security Services tragen insbesondere die Automatisierung von Abläufen, das Entlasten von Analysten sowie das schnelle Einleiten von Maßnahmen und der Kostenfaktor bei.

BILD: DTS

Kai Mallmann,
CEO bei DTS Systeme

Im Bereich der Managed Services erwarten Kunden ein größtmögliches Maß an Flexibilität. Diese Erwartungshaltung steht jedoch vielmals im starken Gegensatz zu starren Lizenzmodellen der Hersteller.

BILD: AXIANS

Alain de Pauw, Leiter der Division Security bei Axians Deutschland

Nachholbedarf spiegelt sich in der Nachfrage nach SOC-Services und Awareness-Schulungen wider. Dass der Mensch den neuen Perimeter in der Security darstellt, wird in der Coronakrise vielen Firmen bewusst.

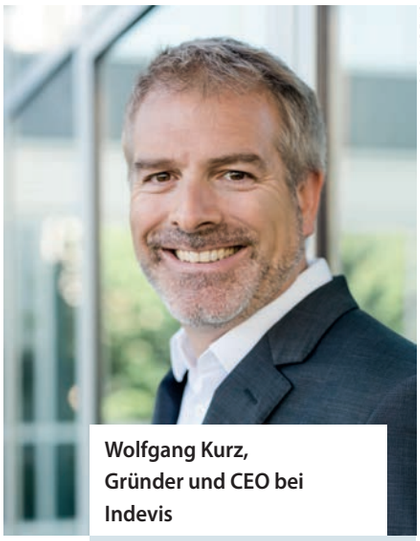

BILD: INDEVIS

Wolfgang Kurz, Gründer und CEO bei Indevis

Kunden müssen sich trauen einen MSSP zu beauftragen. Hierzu muss ein Vertrauensverhältnis zwischen Kunde und Dienstleister vorhanden sein. Daher muss zunächst eine vorherrschende Skepsis abgebaut werden.

herrschende Skepsis zunächst abgebaut werden, damit Kunden Vertrauen in den MSSP und seine Expertise fassen können", führt Indevis-Gründer Kurz weiter aus. Auch Alain de Pauw, Leiter der Division Security bei Axians Deutschland, sieht das Awareness-Problem: „Kunden, die sich für den Einsatz von Managed Security Services entscheiden, erwarten, dass sie sich um nichts mehr kümmern müssen. Hier klären wir auf, denn die Verantwortung für die Cyber Security bleibt bei ihnen, und der Erfolg von MSS setzt eine enge Zusammenarbeit der internen IT mit uns als Provider voraus. Dass der Mensch den neuen Perimeter in der Cybersecurity darstellt, wird in der Corona-Pandemie vielen Firmen bewusst." Auch Kai Mallmann, CEO bei DTS, sieht die Erwartungshaltung des Kunden als aktuell größtes Problem: „Im Bereich der Managed Services erwarten Kunden ein größtmögliches Maß an Flexibilität. Diese Erwartungshaltung steht jedoch vielmals im starken Gegensatz zu starren Lizenzmodellen der Hersteller. Hier ist der MSSP gefragt, den Anforderungen des Markts dennoch nachzukommen und die veredelten Produkte und daraus resultierenden Lösungsangebote in den geforderten Pay-per-Use Modellen zur Verfügung zu stellen."

Erschwerend hinzu kommt der Mangel an Security-Fachkräften: „Für Unternehmen ist es aktuell eine große Herausforderung, eigene Security-Experten rund um die Uhr zu beschäftigen sowie im Falle eines Sicherheitsvorfalls ausreichend Fachkräfte kurzfristig hinzuziehen zu können", erläutert DTS-CEO Mallmann. Doch nicht nur Firmen, auch MSSPs haben laut de Pauw mit dem Fachkräftemangel zu kämpfen: „Auch für uns ist der Fachkräftemangel eine der größten Herausforderungen. Wir investieren in Ausbildungs- sowie Arbeitsbedingungen und bringen uns so im Kampf um Talente in eine gute Position. Zudem ist es sinnvoll, Services zu automatisieren, um als Dienstleister effizienter zu werden."

Je weiter die Nutzung von mobilen und Cloud-basierten Lösungen um sich greift, desto wichtiger werden Netzwerke jeglicher Couleur für das Funktionieren der Wirtschaft. Aber auch klassische Architekturen der Netzwerksicherheit, bei denen Unternehmensdaten, Anwendungen und Informationen zentral in einem Rechenzentrum abgelegt werden, werden immer schwerfälliger und ineffizienter. So vollzieht sich aktuell ein Paradigmenwechsel in der Netzwerkinfrastruktur. „Mit einer Zunahme von Remote-Nutzern und Software as a Service-Anwendungen (SaaS), der Verlagerung von Daten in die Cloud und einem höheren Datenverkehr zwischen Public-Cloud-Diensten und Rechenzentren ist der Bedarf eines neuen Ansatzes für die Netzwerksicherheit gestiegen – das können wir als Managed Security Service Provider nur bestätigen", betont Indevis-CEO Kurz.

Als nächste Stufe der Netzwerkrevolution wird das Gartner-Sicherheitskonzept SASE (Secure Access Service Edge) bezeichnet. SASE ist die Zusammenführung von Netzwerk- und Sicherheitsarchitekturen und -lösungen wie Cloud Access Security Broker, Zero Trust Network Access und Firewall as a Service zu einer einheitlichen Cloud-Plattform. Dadurch könnte SASE Produktkategorien wie SD-WAN, WAN-Optimierung, Firewalls der nächsten Generation, sichere Web-Gateways, CASB und Zero Trust Network Access transformieren. Das Konzept basiert auf identitätsgetriebener Zuordnung, egal ob dies eine Person, eine Applikation, ein Service oder ein Gerät ist. SASE ist zudem ein reines Cloud-Produkt, das deshalb auch weltweit verfügbar und Edge-fähig ist.

Besonderen Zugriffsschutz bei der Nutzung von Cloud-Diensten liefert das Zero-Trust-Modell. Hierbei wird der Datenaustausch sowohl innerhalb als auch außerhalb des Unternehmensnetzwerk zentral und DSGVO-konform gestaltet. Nach dem Motto „Traue niemandem" bietet dieser Ansatz besonderen Schutz vor einer unbemerkten Infiltrierung von Schadsoftware beziehungsweise dem unbemerkten Abfischen von Unternehmensdaten.

Mehr unter:
bit.ly/MSS-ITB

Autor:
Sarah Böttcher