Unternehmen rüsten auf: 86 Prozent werden ihr IT-Sicherheitsbudget bis 2024 erhöhen

Vielen Unternehmen sind die betrieblichen Gefahren durch IT-Vorfälle bewusst. Sie planen Investitionen in Technik und Know-how und nähern sich auch neuen Sicherheitsansätzen wie Zero Trust. Was die technischen Entscheider:innen aus Handel, Industrie oder Dienstleitung von Sicherheitslösungen erwarten, zeigt eine Umfrage von techconsult, bei der Sophos mitgewirkt hat.

Mehr als die Hälfte aller Befragten (52 Prozent) hatten in den letzten 12 Monaten unter einem (26 Prozent) oder mehreren Sicherheitsangriffen auf ihr Unternehmen zu leiden. **Phishing** (42 Prozent) und **Ransomware** (36 Prozent) belegen dabei die ersten Plätze. Bronze (31 Prozent) erhält der Angriffstyp **„Insider Bedrohung“,** Untertyp „fahrlässig“ (es gibt auch „kriminell“, aber dieser macht nur 15 Prozent aus). Darunter fallen salopp gesagt Schusseligkeit und Unwissen von Mitarbeiter:innen, externen Dienstleister:innen, Partnerunternehmer:innen oder Ex-Kolleginnen und -Kollegen.
Diese drei Probleme sehen die Befragten für die nächsten Jahre auch als Sicherheitsbedrohungen für ihre Branchen: Phishing (51 Prozent), fahrlässige Insider Bedrohung (34 Prozent) und Ransomware (28 Prozent).

Ein gutes Drittel (32 Prozent) beklagte Störungen und Ausfälle im Geschäftsablauf. 26 Prozent erlitten finanzielle Einbußen ebenso wie den Verlust sensibler Daten.
Immerhin setzen viele Unternehmen das Thema auf Vorstandsebene an (43 Prozent) und haben eine abgestimmte Sicherheits- und Netzwerkstrategie (42 Prozent). So verfügen 49 Prozent über Antiviren-Lösungen und Malware-Erkennung, 41 Prozent über eine Paketfilter-/Proxy-Firewall und 38 Prozent haben Datensicherungs-, Backup- und Wiederherstellungs-Lösungen in der Schublade.

Wie wollen sich die Unternehmen gegen zukünftige Gefahren wappnen?
48 Prozent setzen auf den Einsatz neuer Sicherheits-Technologien. Aktuell verfügen nur 16 Prozent über einen ZTNA (Zero Trust Network Access). Aber 61 Prozent planen die Einführung einer Zero Trust-Architektur, entweder innerhalb von 12 Monaten (26 Prozent), 24 Monaten (20 Prozent) oder langfristig (15 Prozent). Für nur 6 Prozent ist dieser Sicherheitsansatz kein Thema.
Die Komplexität der Implementierung (36 Prozent), Know-how-Mangel im Unternehmen (33 Prozent), zu hohe Investitionskosten (26 Prozent), aber auch intransparente (jeweils 22 Prozent) und zu wenig erprobte Angebote der Anbieter stehen oder standen der Einführung von Zero Trust bisher jedoch entgegen.

87 Prozent wollen mehr ausgeben für technische Tools und Schulungen
Die sichere Anbindung und Vernetzung ihrer Filialen ist für 58 Prozent der Befragten eine Motivation, Zero Trust im Unternehmen stärker zu fördern. Auch mehr Datensicherheit und der Erhalt der Home-Office-Infrastruktur (beides 56 Prozent) würden Zero Trust ankurbeln. Schutz vor Insider-Bedrohungen (55 Prozent) könnte die zukünftigen Befürchtungen (siehe oben) abschwächen.
Zwei Drittel (60 Prozent) rechnen bei einer Zero-Trust-Architektur mit geringeren Sicherheitsvorfällen. Auch höhere Zugriffssicherheit auf Applikationen in der Cloud und verbesserte Netzwerksicherheit (beides 57 Prozent) versprechen sich die Unternehmen. Onboarding von Beschäftigten im Rahmen von New Work hat für mehr als jeden Zweiten einen

sehr hohen Stellenwert (56 Prozent). Auch geringere Kosten und Komplexität sowie weniger Ausfallzeiten (beides 51 Prozent) sprechen für Zero Trust.

Angesichts dieses attestierten Nutzens planen Unternehmen konkrete technische Maßnahmen in den nächsten Jahren. Darunter fallen die Verschlüsselung von Daten und Transportwegen (34 Prozent), Nutzerprofile und entsprechende Richtlinien (33 Prozent), Data Loss Prevention (30 Prozent) oder auch VPN (23 Prozent).

Neben den technischen Lösungen beschäftigen sich die Unternehmen auch mit organisatorischen Maßnahmen innerhalb ihrer Zero Trust-Architektur. Dazu gehören Notfall- und Reaktionspläne (35 Prozent), Bedarfsanalysen und Zertifizierungen (je 32 Prozent). Netzwerk Segmentierung (mit 17 Prozent vorletzter Platz) sowie Etablierung einer Risikoanalyse mit -management (15 Prozent) wird offenbar nur wenig Bedeutung beigemessen.

Um das alles zu realisieren, planen 86 Prozent in den nächsten zwei Jahren eine Erhöhung ihres Sicherheitsbudgets. Die Mehrheit der Befragten (36 Prozent) peilt ein Plus von 11-20 Prozent an.

Über die Umfrage
Im Rahmen eines Multi Client Projekts, an dem unter anderem Sophos beteiligt war, wurden im Dezember 2021 204 Unternehmen befragt, aus Handel, IT, Logistik, Dienstleitung und Industrie. Neben Vorständen gaben besonders CIO, CSO und IT-Informationssicherheitsbeauftragte Auskunft.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de