Fehlendes Geld ist der größte Feind für Cybersicherheit

Neue Ergebnisse der DACH-weiten Management-Studie von Sophos zeigen, dass oftmals das Budget über die Umsetzung von Cybersicherheitsmaßnahmen entscheidet. Im Branchenvergleich gehen Produktionsbetriebe häufiger als andere Branchen budgetbedingte Cyberrisiken bewusst ein.

Unternehmen in Deutschland, Österreich und der Schweiz sind beim Thema Cybersicherheit auf den ersten Blick gut aufgestellt: In allen drei Ländern gibt eine klare Mehrheit von über 80 Prozent der Befragten an, dass sie noch keine Cybersicherheitsmaßnahme verworfen haben. Doch wenn es Hindernisse gibt, dann liegt es fast immer am Budget. Das zeigen aktuelle Zahlen aus der Management-Studie von Sophos in Deutschland, Österreich und der Schweiz.

Hohe Umsetzungsbereitschaft – aber nicht grenzenlos
In Deutschland sagen 81 Prozent, in Österreich 84 Prozent und in der Schweiz 80 Prozent der befragten C-Level-Entscheider:innen, dass in ihren Unternehmen noch keine Maßnahme zum Cyberschutz verworfen wurde. Das entspricht zunächst einer hohen Umsetzungsbereitschaft. Dennoch berichtet jedes zehnte Unternehmen, dass die Realisierung von Cybersicherheitsmaßnahmen am Ende am Geld gescheitert ist. In Deutschland bestätigen dies 10,5 Prozent, in Österreich 10 Prozent, in der Schweiz sogar 12 Prozent der Befragten.

Budgethürden vor allem in Produktionsunternehmen
Vor allem die Produktionsunternehmen scheinen mit diesem Problem zu kämpfen. Sie liegen in allen Ländern über dem Durchschnitt aller befragten Unternehmen: in Deutschland und Österreich bei jeweils rund 16 Prozent, in der Schweiz sind es 15,8 Prozent.
Aber auch der Handel zeigt Schwierigkeiten. In Österreich gibt ein Viertel der Handelsunternehmen an, aus Kostengründen auf Cybersicherheitsmaßnahmen verzichtet zu haben. In der Schweiz sind dies 14,3 Prozent. Dienstleistungsunternehmen berichten dagegen deutlich seltener von Budgetproblemen – in Deutschland tun das nur 8,7 Prozent, in der Schweiz 8,3 Prozent und in Österreich kein einziges.

Hohe Komplexität ist (fast) kein Hinderungsgrund
Eine zu herausfordernde Komplexität der Cybersicherheitslösungen spielt als Hinderungsgrund für eine Implementierung in allen drei Nachbarländern offenbar eine untergeordnete Rolle: In Deutschland benennen diesen Punkt 5,0 Prozent der Unternehmen und in der Schweiz 8,0 Prozent. In Österreich wird dieser Aspekt als Grund für nicht umgesetzte Maßnahmen überhaupt nicht genannt.

Produktionsunternehmen gehen auch häufiger bewusst Cybersicherheitsrisiken ein
Auf die Frage, ob Unternehmen schon einmal bewusst ein Risiko in der Cybersicherheit eingegangen sind, fällt das Bild differenzierter aus. In Deutschland bestätigen dies 11 Prozent, in Österreich 12 Prozent und in der Schweiz 8 Prozent der Befragten.
Auffällig sind dabei auch hier die Zahlen der Produktionsunternehmen: Mit 14,3 Prozent in Deutschland, 15,8 Prozent in Österreich und 10,5 Prozent in der Schweiz geben sie überdurchschnittlich häufig an, bewusst Cyberrisiken eingegangen zu sein. Ebenfalls über dem Durchschnitt bewegt sich bei diesem Aspekt auch der Handel in Österreich. Hier berichten 12,5 Prozent der Befragten, bereits bewusst ein Risiko eingegangen zu sein. In Deutschland (3,2 %) und der Schweiz (0 %) zeigen sich Händler deutlich weniger risikobereit, während die Dienstleistungsunternehmen länderübergreifend durchweg im Mittelfeld liegen (rund 8–11 Prozent).

Auch das Alter der Entscheidungsträger:innen scheint eine Rolle bei der bewussten Entscheidung für oder gegen Cyberrisiken zu spielen: In Deutschland und in der Schweiz

zeigen sich die unter 45-Jährigen risikobereiter. In Österreich führen überraschend die über 45-Jährigen.

Lösungsansätze: Sicherheit auch für kleine Budgets
„Cybersicherheit scheitert in vielen Unternehmen nicht am Willen, sondern am Budget", bestätigt Michael Veit, Sicherheitsexperte bei Sophos. „Gerade Produktionsbetriebe und Handelsunternehmen nennen häufig Kosten als Grund, Maßnahmen nicht umzusetzen. Für kleine und mittlere Unternehmen gibt es deshalb Lösungen, die bezahlbar sind und trotzdem den steigenden Bedrohungen standhalten. Managed Detection and Response (MDR) ist hier ein gutes Beispiel: Unternehmen lagern die 24/7-Überwachung und Abwehr von Angriffen an Spezialisten aus – und erreichen so ein Sicherheitsniveau, das sie alleine weder finanziell noch personell stemmen könnten."

Zur Studie
Ipsos befragte im Auftrag von Sophos im Frühjahr 2025 insgesamt 300 C-Level-Manager (keine IT-Verantwortlichen) aus verschiedenen Branchen: 200 in Deutschland sowie jeweils 50 in Österreich und der Schweiz. Thema der Umfrage war der Stellenwert von IT-Sicherheit und KI-Technologien in den Unternehmen. IT-Verantwortliche wurden explizit nicht befragt.

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/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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