

Unternehmenschefs in DACH zu IT-Sicherheit: Die größte Herausforderung ist das Personal

Studie von Sophos in Führungsebenen:

- *Verfügbarkeit von Fachpersonal größte Herausforderung – in Österreich gilt dies auch für die externe Expertise*
- *Altes Vorurteil – Unternehmensführungen befürchten Beeinträchtigung der Unternehmensabläufe durch IT-Sicherheit*
- *Deutschland, Österreich und die Schweiz unterscheiden sich in einigen Aspekten z.T. deutlich*

Die Cybersicherheit in Unternehmen hat durch unterschiedliche Faktoren in der jüngeren Vergangenheit noch einmal an Bedeutung gewonnen. Hierzu zählen technologische Entwicklungen oder die wachsende Komplexität von IT-Infrastrukturen. Aber auch jene Faktoren, die durch agiles und mobiles Arbeiten, Homeoffice-Verfügbarkeiten, die Professionalisierung der Cyberkriminalität sowie eine verschärfte internationale Bedrohungslage geprägt sind, nehmen vermehrt Einfluss.

Eine moderne, allen Herausforderungen gerecht werdende IT-Sicherheit ist eine Mammut-Aufgabe für IT-Abteilungen. Wie stehen die Führungsebenen in deutschen, österreichischen und Schweizer Unternehmen dazu? Sophos hat in einer Studie explizit im Managementbereich von Unternehmen wissen wollen, wo die Leitungsebenen die größten Herausforderungen sehen und wie sich die Investitionen in die IT-Sicherheit in der jüngeren Vergangenheit entwickelt haben. Die Ergebnisse zeigen, dass (wie aktuell beinahe alle Berufsfelder und insbesondere die IT) natürlich auch der Spezialbereich der IT-Sicherheit unter einem starken Fachkräftemangel leidet. Aber auch in anderen Bereichen sehen die befragten Unternehmens-Entscheider:innen in der DACH-Region Herausforderungen.

Beim Personal klemmt es am meisten, in Österreich zudem auch bei externer Beratung
Befragt, welche Herausforderungen sie bei der Sicherstellung der Cybersicherheit in ihrem Unternehmen sehen, gaben die befragten Führungsebenen in allen drei Ländern die Verfügbarkeit von Personal am häufigsten an. In österreichischen Unternehmen werden die Schwierigkeiten, qualifiziertes Personal zu finden mit einer Häufigkeit von 69,8 Prozent am meisten genannt, in Deutschland mit 62,7 Prozent und in der Schweiz liegt der Wert mit 58,8 Prozent am niedrigsten.

Rund ein Drittel aller Unternehmen holen sich für die Professionalisierung ihrer Cybersicherheit ergänzend externe Beratungsleistungen in Form von z.B. [MDR-Services](#) hinzu. Insbesondere in Österreich scheinen hierbei ebenfalls Herausforderungen zu bestehen. Während nur 11,8 Prozent der Schweizer und 13,9 Prozent der deutschen Unternehmensleitungen angeben, in der Verfügbarkeit externer Beratungsleistungen Schwierigkeiten zu sehen, sind dies in Österreich immerhin ein Drittel (30,2 Prozent) der Befragten.

Chefs fürchten Behinderungen der Arbeitsabläufe durch IT-Sicherheit

Die IT-Sicherheitslösungen könnten Systeme und Abläufe verlangsamen – dieses Vorurteil hält sich in den Führungsetagen konstant. 45,1 Prozent der Schweizer und 40,3 Prozent der deutschen Befragten gaben an, dass aus ihrer Sicht die Beeinträchtigung der Arbeitsabläufe zu den Herausforderungen bei der Sicherstellung und Umsetzung der Cybersicherheit gehört. In Österreich benennen dies nur 28,3 Prozent.

Zweifel, ob die Cybersicherheit mit mobilem und agilem Arbeiten Schritt halten kann

Zwei Aspekte der modernen Arbeitswelt werden von den Chefs als Herausforderungen für die Umsetzung der IT-Sicherheit angesehen. In Österreich erwarten bei der Sicherstellung der Cybersicherheit 45,3 Prozent der Befragten Schwierigkeiten hinsichtlich der Koordination dieser Aufgabe mit den Modalitäten von Homeoffice-Lösungen. In Deutschland werfen hierauf 39,8 Prozent ein kritisches Auge, in der Schweiz sind es 35,5 Prozent der Befragten.

Aus dem modernen Arbeitsalltag nicht mehr wegzudenken sind agile Methoden. Sind denn die verfügbaren Security-Lösungen flexibel genug, um mit dem agilen Business Schritt zu halten? Immerhin 42,8 Prozent der deutschen, 41,5 Prozent der österreichischen und 39,2 der Schweizer Befragten äußern hier Zweifel.

Oftmals noch alte Vorurteile gegenüber IT-Sicherheit

„Die Zahlen bezüglich der Arbeitsabläufe und Flexibilität für agile Workflows machen deutlich, dass in den Chefetagen oftmals immer noch ein veraltetes und traditionelles Bild von IT-Security vorherrscht, das auf starren Strukturen beruht“, so Michael Veit, Cybersicherheits-Experte bei Sophos. „Moderne Cybersecurity-Lösungen bieten allerdings genau das Gegenteil und zeichnen sich durch ihre modulare und flexible Handhabung sowohl in der Architektur als auch bei der Nutzung im Alltag aus. Technologien wie Zero Trust, Managed Security Services oder auch adaptive Cybersecurity-Ökosysteme ermöglichen heutzutage ein flexibles Arbeiten, bei dem der Anwender die IT-Sicherheits-Prozesse im Hintergrund gar nicht mehr mitbekommt.“

Investitionen auf konstantem Niveau – genaue Daten nicht bekannt, Schweiz hier vorn

Befragt, ob die Investitionen sich in den letzten zwei Jahren verändert haben, gibt eine Mehrheit der Befragten in Deutschland (57,2 Prozent) und Österreich (52,8 Prozent) sowie 45,1 Prozent in der Schweiz an, dass die Investitionen auf einem unvermindert hohen Niveau geblieben sind. Zu 47,1 Prozent und damit am meisten gaben Schweizer Unternehmensführungen an, die Investitionen in den letzten 24 Monaten erhöht zu haben. In Deutschland (34,8 Prozent) und Österreich (32,1) investierten ein gutes Drittel mehr in die IT-Sicherheit. 13,2 Prozent in Österreich, 7,8 Prozent in der Schweiz und 7,5 Prozent der befragten Manager:innen in Deutschland konnten hierzu keine Angaben machen.

Den genauen Anteil der Ausgaben für die IT-Sicherheit zu beziffern fiel den Führungsebenen, sicher nicht zuletzt aufgrund der Komplexität innerer sämtlicher Kostenfaktoren für die IT, eher schwer. Dies trifft insbesondere auf die Schweiz zu. Hier gab beinahe die Hälfte (49 Prozent) der Befragten an, dass dies unmöglich zu beziffern sei. Befragte aus deutschen Unternehmen konnten zu 36,3 Prozent den Anteil der IT-Sicherheit an den Ausgaben für die IT nicht benennen, in Österreich waren dies 30,2 Prozent.



Ansonsten verteilen sich die Investitionen in die Cybersicherheit in DACH wie folgt: In Deutschland geben 20,9 Prozent der Unternehmen 5 bis 9 Prozent ihrer Ausgaben in die IT-Sicherheit, 14,4 Prozent investieren 10 bis 19 Prozent. In Österreich geben 28,3 Prozent immerhin 10 bis 19 Prozent für die IT-Sicherheit aus und bei 13,2 Prozent der befragten Unternehmen liegt der Anteil sogar bei 20 bis 29 Prozent. In der Schweiz zeigt sich folgendes Bild: Hier fließen bei 19,6 Prozent der Unternehmen 5 bis 9 Prozent der Ausgaben in die Cybersicherheit und 13,7 Prozent investieren gar 20 bis 29 Prozent ihres Budgets in diesen wichtigen Bereich.

Über die Umfrage:

Ipsos hat im Auftrag von Sophos 201 C-Level-Managerinnen und -Manager aus Handel, Dienstleistung und verarbeitendem Gewerbe in Deutschland sowie jeweils 50 in Österreich und der Schweiz zum Thema IT-Sicherheit in ihren Unternehmen 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/>

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