SOPHOS

Sophos Management-Studie

Chef, wie hältst du es mit der Cybersicherheit?

Umfrage in Deutschland, Österreich und der Schweiz im C-Level-Unternehmensmanagement. IT-Fachkräfte wurden ausdrücklich nicht befragt.

Inhalt

TEIL I Studienergebnisse branchen- und länderübergreifend

1. Verantwortung für die IT-Sicherheit: IT-Sicherheit ist keine Chefsache
2. Folgen von Cyberattacken: Welche Szenarien befürchtet das Management? Die größte Sorge gilt den Kosten, Zahlungsunfähigkeit befürchten jedoch nur wenige
3. IT-Sicherheitsbewusstsein in Unternehmen: Das Unternehmensmanagement attestiert sich selbst ein besseres Sicherheitsbewusstsein als seiner Belegschaft
4. Stand der Investitionen in die IT-Sicherheit: Investitionen auf konstantem Niveau, genaue Daten oftmals nicht bekannt
5. IT-Sicherheitsmaßnahmen in Planung: Fast ein Drittel der Unternehmen will in zusätzliche IT-Sicherheitslösungen investieren
6. Herausforderungen für die Gewährleistung der IT-Sicherheit: Die größte Herausforderung ist das Personal
7. Einfluss der weltpolitischen Lage auf die Bedeutung der IT-Sicherheit in Unternehmen: Trotz des Kriegs in Europa: Chefetagen wähnen sich in IT-Sicherheit

TEIL II Branchen im Ländervergleich

1. Handelsunternehmen: Auswirkungen auf kaufmännische Abläufe und Zusatzkosten sind Sorge Nummer eins
2. Verarbeitendes Gewerbe: Mehr als 60 Prozent der DACH-Manager im verarbeitenden Gewerbe rechnen künftig mit einem Cyberangriff
3. Dienstleistungen: Optimale Cybersicherheit für Dienstleister? Nur mit externer Beratung und qualifiziertem Personal

Appendix

- Schulungen des Personals sind branchenübergreifend die wichtigste zusätzliche Sicherheitsmaßnahme

Cybersicherheit ist aufgrund der Professionalisierung der Cyberkriminalität und der verschärften Bedrohungslage für viele Unternehmen bereits seit Längerem von strategischer Bedeutung. So beschreibt etwa der Sophos Threat Report 2023 einen neuen Grad der Kommerzialisierung innerhalb der Cyberkriminalität, durch den zunehmend niedrigschwellige Einstiegsangebote für potenzielle Angreifer verfügbar sind: Fast alle Szenarien sind käuflich. Ein boomender Cybercrime-as-a-Service-Markt steht einer kriminellen Käuferschaft offen und stellt eine neue Qualität der Bedrohung für Unternehmen dar.

Über diese Situation hinaus hat das Thema Cybersicherheit in der jüngeren Vergangenheit durch weitere unterschiedliche Faktoren noch einmal an Dringlichkeit gewonnen. Hierzu zählen technologische Entwicklungen, die wachsende Komplexität von IT-Infrastrukturen oder auch sich ändernde gesetzliche Vorgaben für die Gewährleistung von Datensicherheit in Unternehmen, Organisationen oder Behörden. Aber auch jene Faktoren, die durch agiles und mobiles Arbeiten, Homeoffice-Verfügbarkeiten und eine verschärfte internationale Bedrohungslage geprägt sind, nehmen vermehrt Einfluss.

Spiegelt sich diese Gemengelage auch im Unternehmensalltag wider? Welche Security-Maßnahmen stehen ganz oben auf der Prioritätenliste der Unternehmensentscheider?

Wer ist innerhalb der Unternehmen schlussendlich in der Verantwortung für die IT-Sicherheit? Wo wird investiert? Welche Unterschiede gibt es zwischen den Ländern Deutschland, Österreich und der Schweiz und wie unterscheiden sich beim Thema Cybersicherheit unterschiedliche Branchen?

Diesen sowie einigen weiteren Fragen ging Sophos im Rahmen einer Management-Studie nach, die das Marktforschungsunternehmen Ipsos 2022 durchgeführt hat. Befragt wurden 201 C-Level-Manager aus Handel, Dienstleistung und verarbeitendem Gewerbe in Deutschland sowie jeweils 50 in Österreich und der Schweiz.

Die Ergebnisse sind in diesem Whitepaper zusammengefasst und zeigen, dass das Thema IT-Security mittlerweile tatsächlich in die allgemeine Unternehmensstrategie eingebunden ist und entsprechend Maßnahmen zum Schutz gegen Cyberangriffe getroffen beziehungsweise künftig umgesetzt werden. Es zeigt sich aber auch, dass trotz vieler Forderungen zum Beispiel aus Politik[1], Wirtschaft und Verbänden nach einer Ansiedelung der IT-Sicherheit in den höchsten Unternehmenshierarchien die meisten Unternehmen die Verantwortung letztlich doch an IT-Teams delegieren – entweder an die eigenen Inhouse-Abteilungen oder externe IT-Dienstleister. Die wenigsten Unternehmen verfügen über eine ausgewiesene IT-Sicherheitsinstanz.

Wichtigste Erkenntnisse aus der Studie in der Übersicht

- Cybersicherheit ist in den Unternehmen keine Chefsache
- Investitionen sind hoch, mehr als ein Drittel will in zusätzliche IT-Sicherheitsmaßnahmen investieren
- Bedeutung der Cybersicherheit wächst und doch wähnen sich Chefs in (IT-)Sicherheit
- Wirtschaftliche Schäden nach Cyberattacken sind größte Sorge von Managern
- Es bestehen Vorbehalte, sogar Vorurteile gegenüber neuen IT-Security-Technologien

[1]BSI: Cybersicherheit ist Chefsache. „...Die Stärkung der Cybersicherheit ist ein entschei-dender Faktor für den wirtschaftlichen Erfolg des Unternehmens und kann klare Wettbe-werbsvorteile schaffen. Hier ist die Unternehmensleitung gefragt, Sicherheitsrisiken zu erken-nen, Zuständigkeiten zu klären und passende Maßnahmen zu ergreifen."

Chefsache IT-Security?

NOCH IST SECURITY NICHT DURCHGÄNGIG IM C-LEVEL ANGEKOMMEN

Wie halten es die Führungskräfte in deutschen, österreichischen und Schweizer Unternehmen mit der Cybersicherheit?

Cybersicherheit ist noch keine Chefsache.
IT-Abteilungen sind in der Verantwortung.
Ein Drittel setzt auf externe IT-Dienstleistungen.

IT-Security ist Chefsache bei nur
16,4% deutscher
17% österreichischer
15,7% Schweizer
Unternehmen

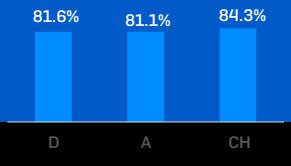
Allerdings: IT-Security ist seit mindestens zwei Jahren auf höherer Hierarchie angesiedelt bei
46,3 % deutscher
35,8 % österreichischer
54,9 % Schweizer
Unternehmen

Um die IT-Security kümmert sich dennoch hauptsächlich:

	IT-Abteilung	Dienstleister
D	39,8%	33,8%
AT	37,7%	32,1%
CH	43,1%	27,5%

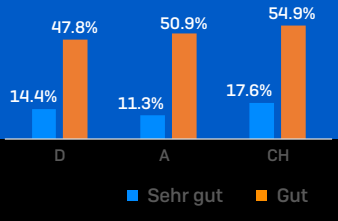
Chefs attestieren sich hohes Sicherheitsbewusstsein.

Die Mehrheit wiegt sich in Sicherheit



Chefs schätzen Cyberschutz als gut ein.

Nur wenige bewerten mit sehr gut



Über diese Studie: Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS
Cybersecurity evolved.

TEIL I Studienergebnisse branchen- und länderübergreifend

I.1 Verantwortung für die IT-Sicherheit

IT-Sicherheit ist keine Chefsache

Ganz allgemein kann im positiven Sinne festgehalten werden, dass das Thema Cybersicherheit auf der Agenda der Unternehmensführungen angekommen ist. In der Überprüfung im Rahmen der Studie, wie eng die Umsetzung des Themas tatsächlich mit den Entscheidern in den Führungsetagen verknüpft ist, zeigen sich jedoch deutliche Unterschiede zwischen der Bewertung des IT-Sicherheitsbewusstseins der Chefetagen und der tatsächlichen operativen Verantwortung: Die Verantwortung liegt bei den IT-Teams

Höher aufgehängt und doch: IT-Sicherheit ist keine Chefsache. Die IT ist in der Pflicht

Die große Mehrheit der befragten Manager (rund 81 Prozent) gibt an, ein hohes bis sehr hohes Bewusstsein für IT-Sicherheit zu haben. Auch wurde den Angaben aller Befragten zufolge in der Mehrheit der Unternehmen (über 60 Prozent) die IT-Sicherheit innerhalb der zurückliegenden drei Jahre auf einer höheren bzw. der höchsten Hierarchieebene angesiedelt.

Je größer die Unternehmen, desto weniger ist die Führungsebene in der Verantwortung

Hier offenbart sich ein interessanter Widerspruch, denn bei der Frage nach der tatsächlichen Verantwortung für die IT-Sicherheit zeigt sich dann doch ein anderes, durchaus zu erwartendes Bild: Je größer die Unternehmen sind, desto weniger steht die Führungsebene in der Verantwortung. Dies gilt vor allem für Unternehmen mit mehr als 200 Mitarbeitern, hier geben nur 1,9 Prozent der Befragten an, dass die IT-Sicherheit auf Geschäftsführungs- bzw. Vorstandsebene angesiedelt ist. Bei kleineren Unternehmen mit bis zu 199 Mitarbeitern sowie im Handel liegt dieser Wert deutlich höher; hier ist der Chef zu rund 22 Prozent noch höchstpersönlich mit eingebunden.

Vor allem in größeren Unternehmen sind die eigenen IT-Teams am Ruder

Die Hauptverantwortung für Cybersicherheit trägt in größeren Unternehmen in Deutschland zu 49 Prozent, in Österreich zu 47 Prozent und in der Schweiz sogar zu 58 Prozent die eigene IT-Abteilung. Bei kleineren Unternehmen sind zu jeweils einem guten Drittel (Deutschland 37, Schweiz 31 und Österreich 33 Prozent) ebenfalls die eigenen IT-Teams in der Pflicht. Zudem überträgt jeweils ein Drittel der größeren wie der kleineren Unternehmen in Deutschland und Österreich die Verantwortung für die IT-Sicherheit auf externe Dienstleister.

Ein leicht abweichendes Bild zeigt sich in der Schweiz: Hier wird bei größeren Unternehmen ebenfalls zu einem Drittel IT-Sicherheitswissen hinzugekauft. Bei kleineren Unternehmen setzen aber nur 21 Prozent auf externe Expertise.

Insgesamt gilt: In Deutschland ist zu 39,8 Prozent die eigene IT-Abteilung verantwortlich, 33,8 Prozent vertrauen dieses sensible Feld einem externen Dienstleister an. In Österreich verteilen sich die Zahlen auf 37,7 Prozent für die eigene IT und 32,1 Prozent auf zugekaufte IT-Security-Expertise. Die Schweiz behält die Verantwortung zu 43,1 Prozent im Haus (bei der eigenen IT-Abteilung) und vergibt sie zu 27,5 Prozent nach extern.

IT-Sicherheit wird als Aufgabe statt als Priorität eingestuft

„Die Ergebnisse in der DACH-Region sind zwar enttäuschend, entsprechen aber dem, was wir in Nordamerika, ASEAN und anderen Regionen beobachten. Leider wird die Sicherheit, wenn sie als Bestandteil der IT verwaltet wird, in der Regel auf den Status einer Aufgabe zurückgestuft, anstatt eine Priorität zu sein. Die Rolle des Sicherheitsteams besteht darin, Risiken zu identifizieren und dem Vorstand dabei zu helfen, diese Risiken nach Prioritäten zu ordnen, wohingegen die IT-Abteilung die Aufgabe hat, die erforderlichen Änderungen zu implementieren, je nachdem, wie diese Risiken angegangen werden sollen."

Chester Wisniewski, Principal Research Scientist bei Sophos

I.2 Folgen von Cyberattacken: Welche Szenarien befürchtet das Management

Die größte Sorge gilt den Kosten, Zahlungsunfähigkeit befürchten jedoch nur wenige

Die Folgen von Cyberangriffen können existenziell für Unternehmen sein. Produktionsausfälle, Lieferstopps, Zahlungsunfähigkeit oder auch schlicht die finanziellen Auswirkungen, die z. B. durch Lösegeldzahlungen nach Ransomware-Angriffen oder Wiederherstellung von Daten oder ganzen Infrastrukturen entstehen, können zumindest den reibungslosen Weiterbetrieb empfindlich stören oder sogar das Überleben von Unternehmen bedrohen. Ein wichtiges Anliegen der Studie war es daher, zu verstehen, welche Folgen von Cyberangriffen Entscheidungsträgern tatsächlich Sorge bereiten.

- Zusatzkosten sind die größte Sorge, Lieferkettenprobleme und Belegschaftsverlust kaum
- Die Sorge vor Zahlungsunfähigkeit ist in der Schweiz im Vergleich zu den Nachbarländern größer und in Österreich am geringsten ausgeprägt

Mit Blick auf die Folgen eines Cyberangriffs gilt in deutschen, österreichischen und Schweizer Chefetagen recht erwartungsgemäß die meistgenannte Sorge den dadurch entstehenden Kosten – etwa durch eine notwendige Wiederherstellung des Geschäftsbetriebs. Die möglichen Unterbrechungen der kaufmännischen Abläufe stehen in allen drei Ländern am zweithäufigsten im Fokus.

Zahlungsunfähigkeit nach Cyberangriff ist vor allem in der Schweiz ein Thema

Mit 21,6 Prozent steht in der Schweiz zusätzlich die Angst vor Zahlungsunfähigkeit im Raum, die Nachbarländer zeigen sich bei diesem Punkt erheblich gelassener: Nur 9,5 Prozent der befragten deutschen Chefs fürchten eine Zahlungsunfähigkeit, in Österreich sind dies sogar nur 5,7 Prozent.

Ein interessanter Aspekt hierbei: Probleme im Rahmen der Lieferketten vermuten insgesamt noch weniger Befragte als einen möglichen Imageverlust. Allein im verarbeitenden Gewerbe, und das ist keine große Überraschung, gehen immerhin insgesamt knapp 37 Prozent der Befragten davon aus, dass die Lieferketten möglicherweise betroffen sein könnten.

Die Sorge vor einem Imageschaden ist in Österreich größer als die vor einem drohenden Produktionsstopp

In Österreich liegt die Sorge vor einem Imageverlust mit 26,4 Prozent auf Platz drei und hat damit mehr Gewicht als etwa ein drohender Produktionsstopp (22,6 Prozent), der in Deutschland immerhin von 34,4 Prozent befürchtet wird und in der Schweiz sogar 51 Prozent der Befragten Sorge bereitet.

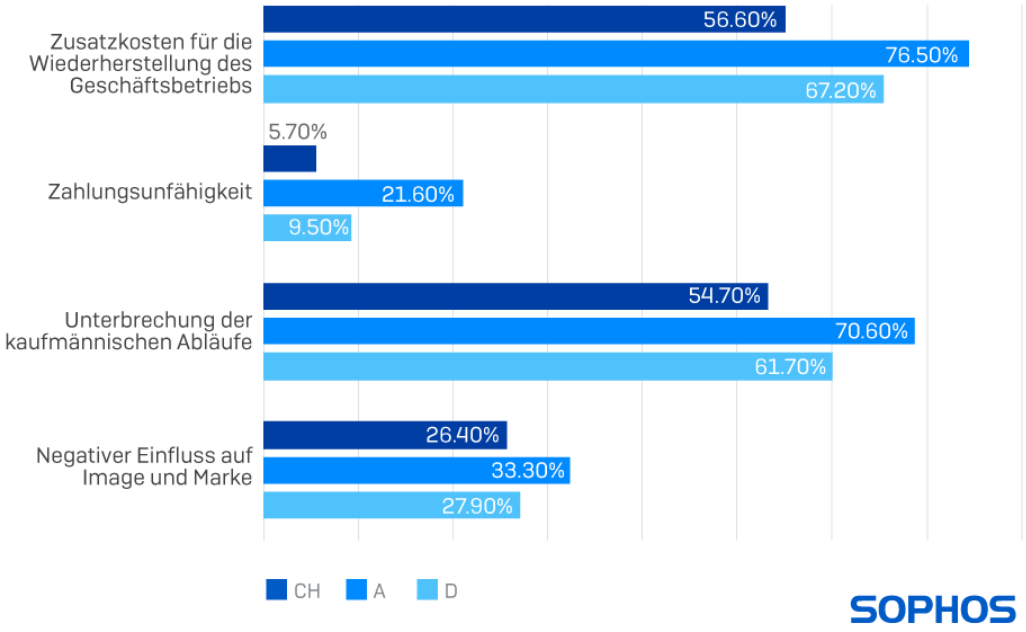
Kaum Sorge vor Verlust von Kunden oder Personal– mit Ausnahme der Schweizer Unternehmen

Dem Verlust von Kunden oder Beschäftigten als Folge von Cyberattacken messen die Führungskräfte hingegen kaum bis keine Bedeutung bei: Mit Kundenverlusten rechnen in Deutschland 19,4 Prozent und in Österreich 15,1 Prozent der Befragten. Noch weniger (Deutschland 1,4 Prozent, Österreich 1,9 Prozent) befürchten, Mitarbeitende zu verlieren.

Lediglich in der Schweiz fallen diese Aspekte mehr ins Gewicht. Hier macht die Sorge vor Kundenverlusten 27,5 Prozent aus, Angestellte zu verlieren fürchten immerhin 11,8 Prozent der Befragten.

Auch Zahlungsunfähigkeit und Bußgelder wegen Datenschutzverletzungen werden kaum als Risiken gesehen, lediglich in der Schweiz regt sich hier etwas mehr Sorge: Hier erwarten knapp 22 Prozent eine Zahlungsunfähigkeit sowie 11,8 Prozent Bußgeldzahlungen als mögliche Folgen von Cyberattacken.

Gefahren als Folgen von Cyberattacken aus Management-Sicht



I.3 IT-Sicherheitsbewusstsein in Unternehmen

Das Unternehmensmanagement attestiert sich selbst ein besseres Sicherheitsbewusstsein als seiner Belegschaft

- Die Schulung von Beschäftigten wird in DACH als eines der wichtigsten Mittel zur Verbesserung der Cybersicherheit angesehen
- Unternehmen attestieren ihrer Belegschaft gutes Sicherheitsbewusstsein, Schweiz und Deutschland kritischer als Österreich

Die IT-Sicherheit für Unternehmen ist kein fertiger Standardbausatz, den man einmalig erwirbt, installiert und ab und zu aktualisiert. Sie ist als Prozess zu verstehen, der immer wieder neu an die veränderten Bedingungen angepasst werden muss. Dabei helfen Technik und Technologien. Am Ende der IT-Nutzungskette jedoch sitzt der Mensch, der mithilfe von Computern und Geräten seine Tätigkeiten verrichtet. Der Faktor Mensch spielt immer wieder eine entscheidende Rolle, wenn es um Schwachstellen geht. Trauen Firmenleitungen in Deutschland, Österreich und der Schweiz ihren Angestellten zu, z. B. eine täuschend echt wirkende Phishing-E-Mail zu erkennen? Surfen sie im Homeoffice in ihren Pausen via Firmen-VPN und gefährden so die Betriebs-IT? Wie hoch ist das Sicherheitsbewusstsein in der Belegschaft?

Gut, aber mit Luft nach oben

Insgesamt und über alle drei Länder hinweg attestieren die Führungskräfte in Deutschland, Österreich und der Schweiz sich selbst und ihren Beschäftigten einen grundsätzlich positiven und verantwortungsvollen Umgang mit IT-Sicherheit – allerdings mit Luft nach oben. Positiv fällt das österreichische Beispiel auf, das wohlwollender mit sich und seinen Teams ins Gericht geht, während die Firmenleitungen zugleich das Bewusstsein weiter mit regelmäßigen Weiterbildungen aufrechterhalten.

Die Chefs in Deutschland und der Schweiz urteilen über sich und die Belegschaft recht ähnlich.

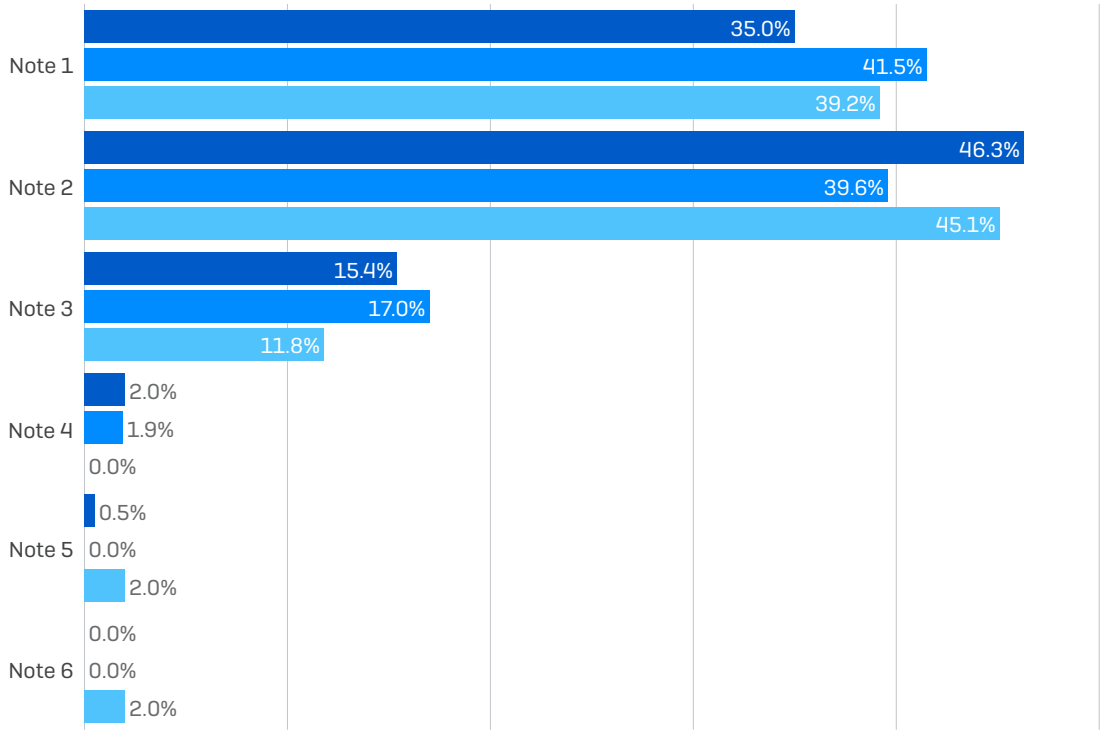
Deutsche Chefs bewerten sich mehrheitlich gut

Sich selbst attestieren deutsche Chefs über alle Branchen hinweg ein sehr hohes (35,3 Prozent) bis hohes (46,3 Prozent) Bewusstsein für die IT-Sicherheit. Bei der Selbsteinschätzung spielt die Unternehmensgröße durchaus eine Rolle: In größeren Betrieben (200 Angestellte und mehr) geben sich 30,2 Prozent der Manager die Bestnote, bei kleineren (50–199 Angestellte) sind es 37,2 Prozent

Schweizer Führungskräfte bewerten sich gut

Das Sicherheitsbewusstsein des Managements in der Schweiz wird mit 45,1 Prozent mit „gut" bewertet. Ein wenig mehr bei kleineren Betrieben (46,9 Prozent) etwas weniger bei großen Firmen (42,1 Prozent). Die Bestnote geben sich 39,2 Prozent der Schweizer Chefs für ihr eigenes Sicherheitsbewusstsein zu jeweils 42,1 Prozent mit „gut" oder „sehr gut".

Selbsteinschätzung über das Sicherheitsbewusstsein des Managements im Ländervergleich



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Manager österreichischer Großbetriebe bewerten sich und ihre Belegschaft am besten

Etwas anders sieht es dagegen in Österreich aus. Sich selbst attestieren die österreichischen Manager mit 41,5 Prozent ein sehr hohes beziehungsweise mit 39,6 Prozent ein hohes Sicherheitsbewusstsein – besser als die Selbsteinschätzungen der deutschen Führungsköpfe.

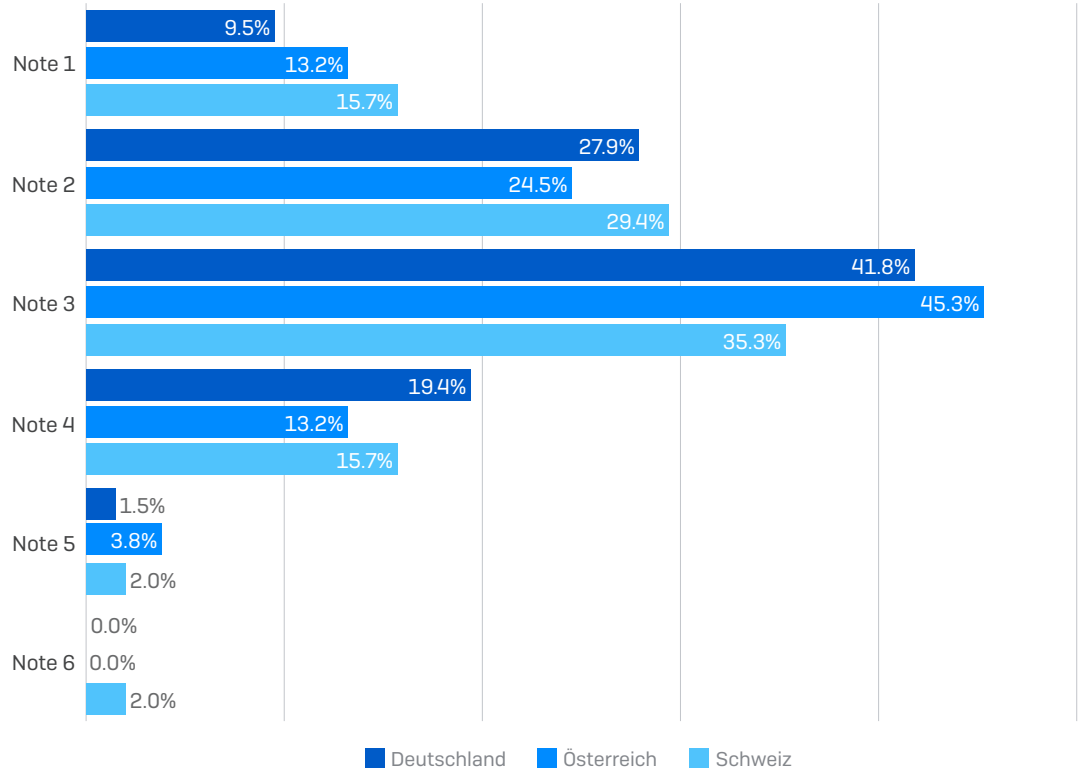
Während zudem wie in Deutschland die Mehrheit (45,3 Prozent) ihre Belegschaft ebenfalls befriedigend bewertet, liegt der Anteil der Bestnoten insgesamt höher als in Deutschland: In Österreich geben 13,2 Prozent der Befragten ihren Mitarbeitenden im Bereich Cyberbewusstsein eine sehr gute Note. Noch ein Unterschied: Haben in Deutschland die größeren Unternehmen eine kritischere Einschätzung, sieht es in der Alpenrepublik genau andersherum aus: 17,6 Prozent der Betriebe mit mehr als 200 Mitarbeitenden attestieren ihrer Belegschaft ein gutes bis sehr gutes Sicherheitsbewusstsein.

In der Schweiz schätzen 35,3 Prozent der Chefs (in großen Betrieben 26,3 Prozent, in kleineren 40,6 Prozent) das Sicherheitsbewusstsein ihrer Angestellten als befriedigend ein. Größere Betriebe geben ihrer Belegschaft eine gute Bewertung (36,8 Prozent).

Je größer das Unternehmen, desto geringer das Zutrauen der Manager in das Sicherheitsbewusstsein der Belegschaft

Bei der Beurteilung ihrer Teams sind die deutschen Manager etwas strenger: Die Mehrheit (41,8 Prozent) gibt ihnen lediglich ein „befriedigend". Die Bestnote an Mitarbeitende vergeben am meisten die Chefs aus Dienstleistungen (11 Prozent). Auch hier spielt die Unternehmensgröße bei der Beurteilung eine Rolle: Chefs von bis zu 199 Mitarbeitenden erscheint das Sicherheitsbewusstsein ihrer Belegschaft mit 10,8 Prozent sehr hoch. Manager bei Firmen mit über 200 Personen vergeben die Bestnote nur an 5,7 Prozent ihrer Belegschaft. Sie attestieren sogar zu 3,8 Prozent ein mangelhaftes Bewusstsein, während Manager kleinerer Unternehmen nur ihren Teams zu 0,7 Prozent ein derart geringes Sicherheitsbewusstsein zuschreiben.

Benotung des Sicherheitsbewusstseins der Mitarbeiter im Ländervergleich



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

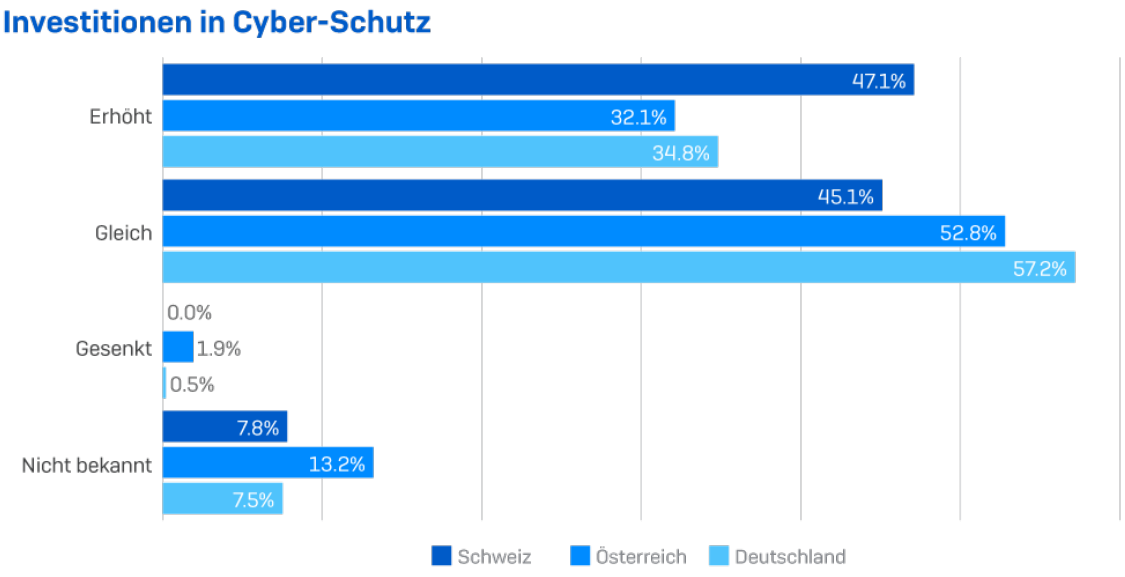
SOPHOS

I.4 Stand der Investitionen in die IT-Sicherheit

Investitionen auf konstantem Niveau, genaue Daten oftmals nicht bekannt

- Investitionen in die IT-Sicherheit bereits seit zwei Jahren auf hohem Niveau
- Schweiz mit den meisten Investitionserhöhungen in den letzten 24 Monaten
- 1,9 Prozent der österreichischen Unternehmen haben die Investitionen gesenkt

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 geben Schweizer Unternehmensführungen an, die Investitionen in den letzten 24 Monaten erhöht zu haben. In Deutschland (34,8 Prozent) und Österreich (32,1 Prozent) 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 in Deutschland können hierzu keine Angaben machen.

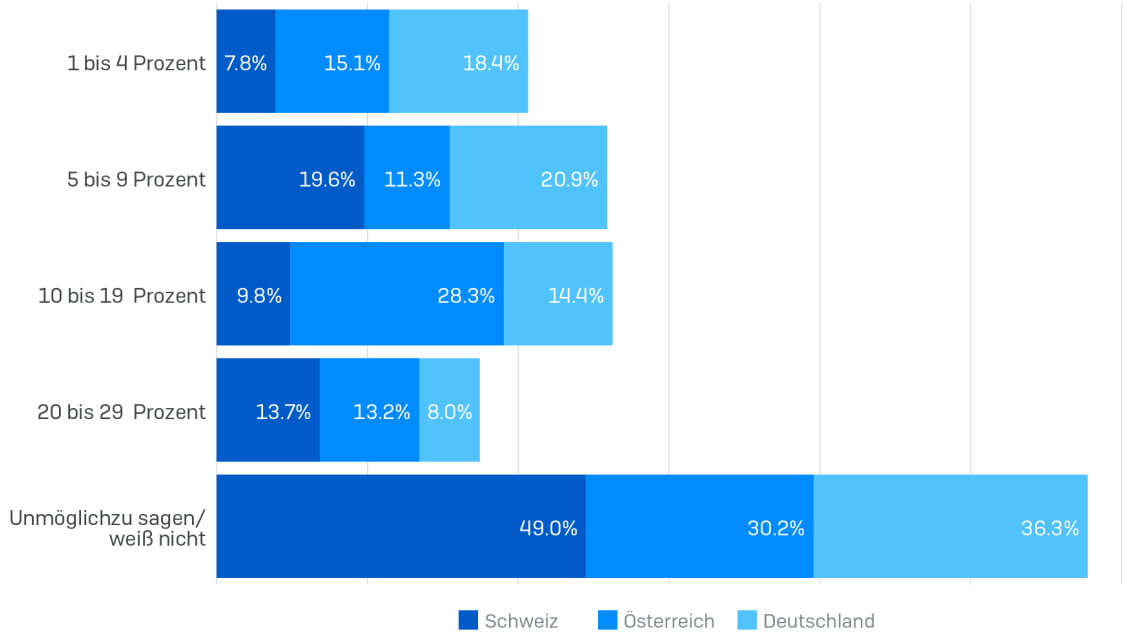


Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

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

Anteil IT-Security-Ausgaben



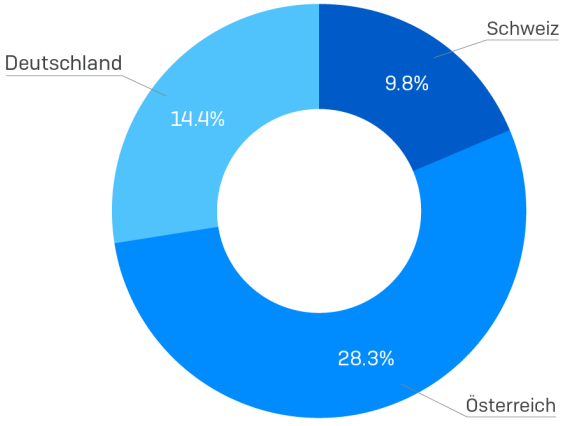
Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Schweiz und Österreich investieren anders als Deutschland

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 sogar 20 bis 29 Prozent ihres Budgets in diesen wichtigen Bereich.

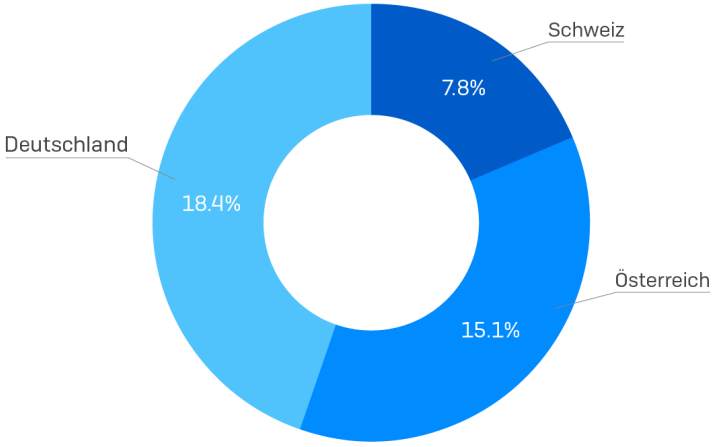
Anteil IT-Security-Ausgaben von 10 bis 19 Prozent



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Anteil IT-Security-Ausgaben von 1 bis 4 Prozent



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

I.5 IT-Sicherheitsmaßnahmen in Planung

Fast ein Drittel der Unternehmen will in zusätzliche IT-Sicherheitslösungen investieren

Unternehmensentsleitungen ist grundsätzlich bewusst, dass sich sowohl die Gefahrenlage, die von der immer professionelleren und zunehmend organisierten Cyberkriminalität ausgeht, als auch die Verteidigungsstrategien dagegen in einem höchst dynamischen Prozess befinden. Mit welchen Maßnahmen beabsichtigen die Manager ihre Unternehmen und Belegschaften weiter gegen Cyberattacken abzusichern?

- Unternehmen rüsten mit weiteren Security-Lösungen und Security-Strategien auf
- Personal für die IT-Sicherheit wurde bereits aufgestockt, weitere Einstellungen sind geplant
- Stärkere Einbindung der IT-Sicherheit in die Unternehmensstrategie
- Schulungen der Belegschaft als bedeutende Maßnahme

Mehr Security-Technologie und IT-Strategien

Zur Verbesserung der Cybersicherheit in Unternehmen sind neue technische Lösungen und die Adaption neuer IT-Sicherheitsstrategien die naheliegendsten Maßnahmen. Das sieht auch die Führungsebene in den Unternehmen in Deutschland, Österreich und der Schweiz so. Befragt, welche Maßnahmen das Unternehmensmanagement zur Sicherstellung der Cybersicherheit in ihrem Unternehmen ergreift, geben mit 27,9 Prozent fast ein Drittel der deutschen Manager an, dass sie künftig Investitionen in weitere IT-Sicherheitslösungen (z. B. Künstliche Intelligenz) planen (Österreich 28,3 Prozent; Schweiz 31,4 Prozent). 26,3 Prozent der deutschen Befragten (Österreich 18,8 Prozent; Schweiz 21 Prozent) bestätigen, dass sie bereits seit über einem Jahr ihre Investitionen in diesem Bereich hochgefahren haben.

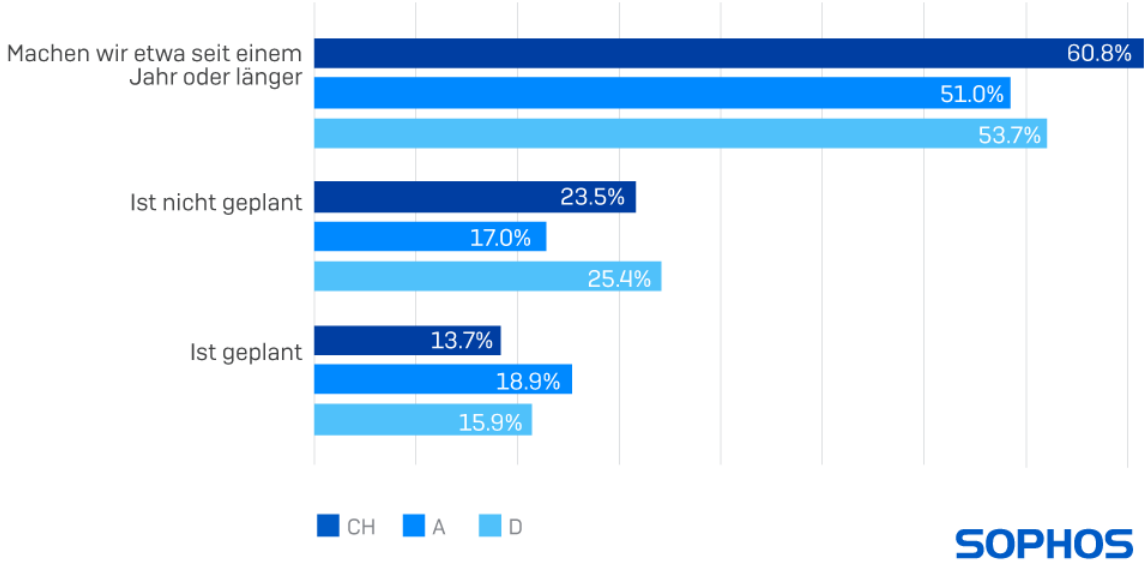
Schweizer Unternehmen mit einer Führungsrolle

Zudem planen die Führungskräfte, künftig weiterhin zusätzliche IT-Sicherheitsstrategien wie Zero Trust zu implementieren. Dies geben 23,9 Prozent der befragten Manager in Deutschland, 18,9 Prozent in Österreich und 19,5 Prozent in der Schweizer an. Laut den Umfrageergebnissen nehmen die Schweizer Manager eine Führungsrolle in Fragen der IT-Sicherheitsstrategien ein: 21,8 Prozent haben in ihren Unternehmen bereits während der letzten Jahre zusätzliche IT-Sicherheitsstrategien adaptiert (Deutschland 9,8 Prozent; Österreich 13,2 Prozent).

Es besteht Handlungsbedarf für Fachpersonal

Neben dem Einsatz neuer Security-Technologien und der Adaption zusätzlicher Security-Strategien wollen Unternehmen auch ihren Personalbestand im Bereich IT-Sicherheit aufstocken, um besser vor Cyberbedrohungen geschützt zu sein. In Deutschland planen 15,9 Prozent (Österreich 18,9 Prozent; Schweiz 13,7 Prozent) der Führungskräfte eine künftige Erweiterung ihres IT-Security-Personals. 25,4 Prozent der deutschen Manager (Österreich 17,5 Prozent; Schweiz 23,5 Prozent) planen allerdings keine Aufstockung des Personals. Ein möglicher Grund dafür könnte sein, dass diese Unternehmen bereits in der Vergangenheit zusätzliches Security-Personal aufgebaut haben. 53,7 Prozent der deutschen Befragten (Österreich 51,5 Prozent; Schweiz 60,8 Prozent) geben an, bereits seit mindestens einem Jahr ihre Personaldecke in diesem Bereich zu erweitern.

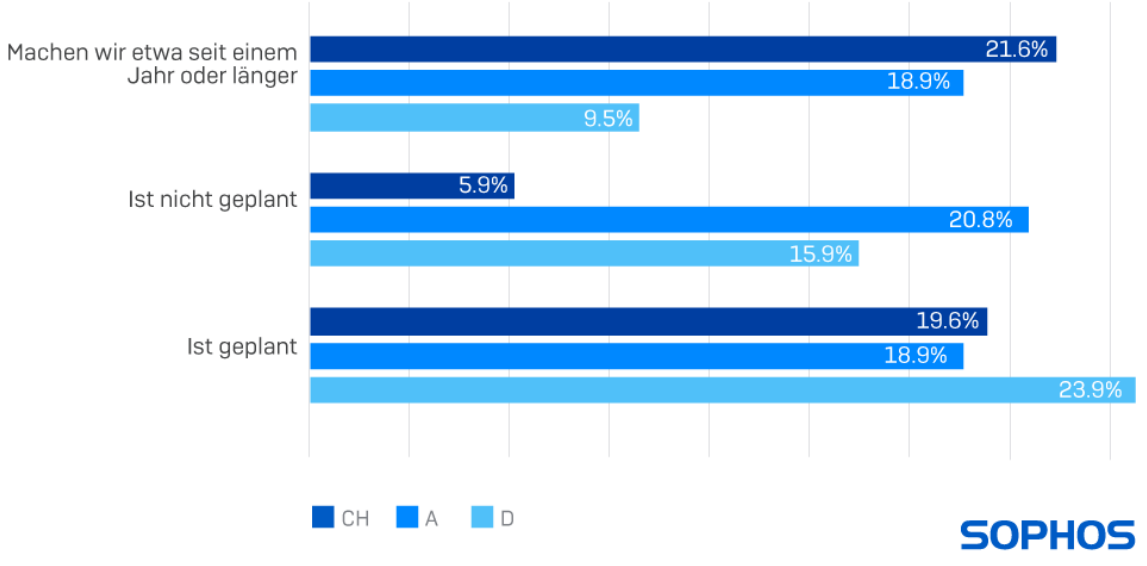
Aufstockung des Personals zur Verbesserung der IT-Sicherheit



Optimierung der IT-Sicherheitsprozesse

Die Optimierung bestehender IT-Prozesse ist ein Weg, um diese besser in die allgemeine Unternehmensstrategie einzubinden. Welche Dringlichkeit diese Maßnahme hat, verdeutlichten die Ergebnisse der Umfrage: Bereits 78,2 Prozent der Führungskräfte in Deutschland (Österreich 69,8 Prozent; Schweiz 80,4 Prozent) optimieren ihre Security-Prozesse seit einem Jahr oder länger und 13,9 Prozent planen diese Maßnahme zukünftig (Österreich 13,2 Prozent; Schweiz 11,8 Prozent). Lediglich drei Prozent der Manager in Deutschland (Österreich 3,8 Prozent; Schweiz 3,9 Prozent) sehen hierzu keine Veranlassung und planen diesen Schritt nicht.

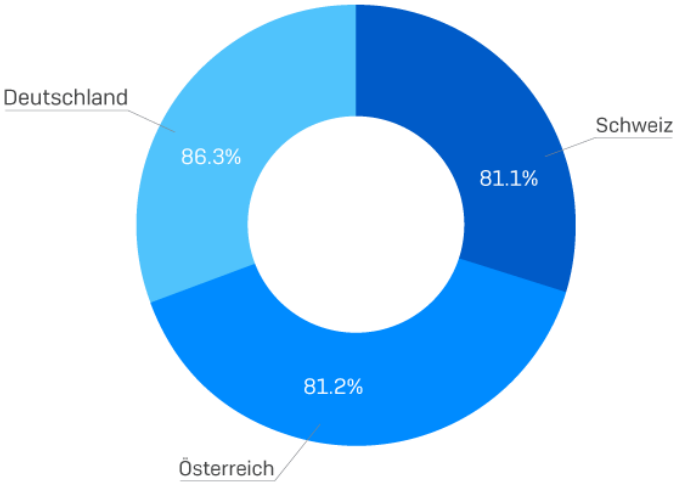
Adaption der IT-Sicherheitsstrategie, wie z.B. Zero-Trust Modell



Auch Anwender stehen im Fokus der Security, Schulungen sind wichtige zusätzliche Maßnahmen

Der Mehrheit der Betriebe ist bewusst, dass der Mensch ein kritischer Faktor bei der Cybersicherheit ist. Schulungen von Mitarbeitenden gehören seit Jahren zur wichtigsten Sicherheitsmaßnahme, die Schweiz verzeichnet hier sogar den höchsten Wert. In Sachen IT-Security-Schulung für die Belegschaft sind die Unternehmen nach Meinung der Führungskräfte in DACH gut aufgestellt: Mit 81,1 Prozent gibt die Mehrheit der Befragten in Deutschland (Österreich 81,2 Prozent; Schweiz 86,2 Prozent) an, ihre Teams seit etwa einem Jahr oder länger zu schulen.

Schulung der Mitarbeiter zur Verbesserung der Cybersicherheit seit etwa einem Jahr oder länger im Ländervergleich



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

I.6 Herausforderungen für die Gewährleistung der IT-Sicherheit

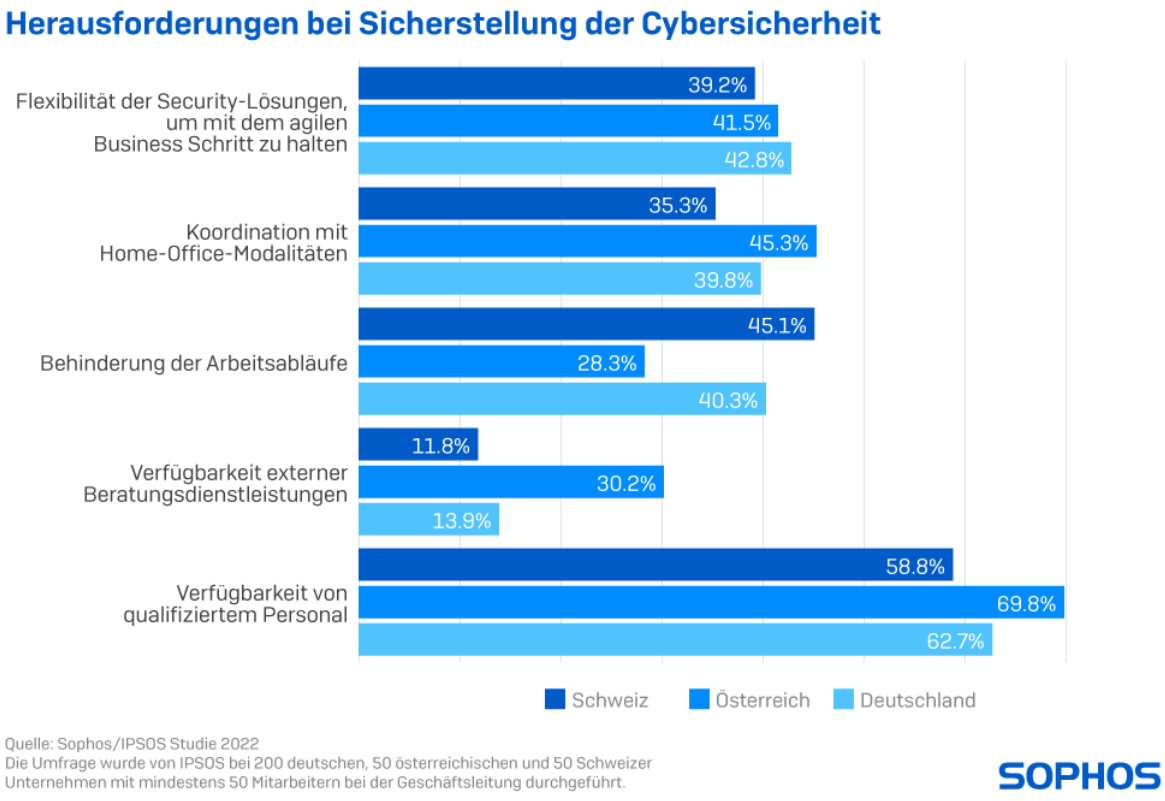
Die größte Herausforderung ist das Personal

Eine moderne, allen Herausforderungen gerecht werdende IT-Sicherheit ist eine Mammutaufgabe für IT-Abteilungen. Sophos wollte in seiner Studie wissen, wo die Leitungsebenen die größten Herausforderungen für die Gewährleistung der IT-Sicherheit in ihren Unternehmen sehen.

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

Beim Personal klemmt es am meisten, in Österreich zudem auch bei externer Beratung

Zur Frage, welche Herausforderungen sie bei der Sicherstellung der Cybersicherheit in ihrem Unternehmen sehen, geben die Führungskräfte 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.

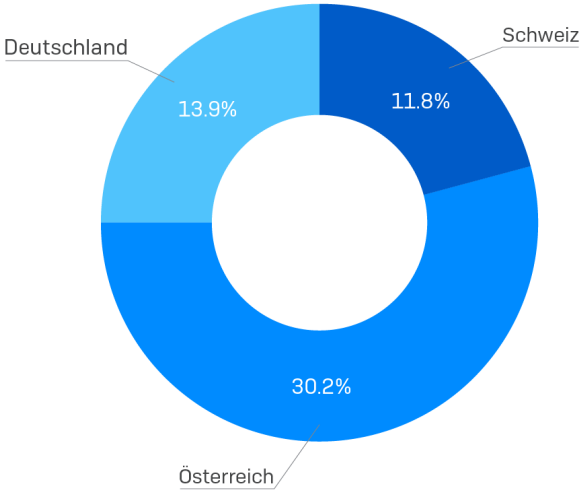


Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Rund ein Drittel aller Unternehmen holen sich für die Professionalisierung ihrer Cybersicherheit ergänzend externe Beratungsleistungen in Form von z. B. MDR-Services. 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, ist dies in Österreich immerhin bei einem Drittel (30,2 Prozent) der Befragten der Fall.

Herausforderungen bei der Verfügbarkeit externer Beratungsdienstleistungen



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Das Management hat Zweifel, ob die Cybersicherheit mit zunehmend mobilem und agilem Arbeiten Schritt halten kann

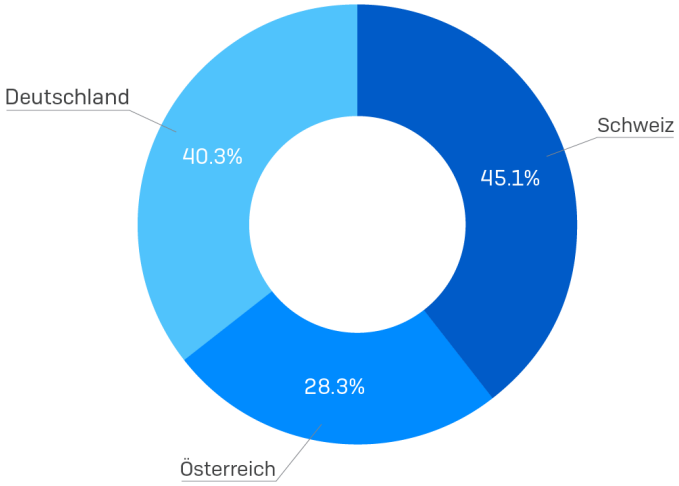
Zwei Aspekte der modernen Arbeitswelt werden von den Chefs als Herausforderungen für die Umsetzung der IT-Sicherheit angesehen. In Österreich erwarten bei der Sicherstellung der Cybersicherheit 45,3 Prozent der Befragten Schwierigkeiten hinsichtlich der Koordination dieser Aufgabe mit den Modalitäten 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**. Aber sind 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 Prozent der Schweizer Befragten äußern hier Zweifel.

Chefs vermuten Behinderungen der Arbeitsabläufe durch IT-Sicherheitslösungen

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 geben an, dass aus ihrer Sicht die Beeinträchtigung der Arbeitsabläufe zu den Herausforderungen bei der Sicherstellung und Umsetzung der Cybersicherheit gehört. In Österreich sagen dies nur 28,3 Prozent.

Cybersicherheit behindert Arbeitsabläufe



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

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. 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.“ Michael Veit, Security Evangelist, Sophos

I.7 Einfluss der weltpolitischen Lage auf die Bedeutung der IT-Sicherheit in Unternehmen

Trotz des Kriegs in Europa: Chefetagen wähnen sich in IT-Sicherheit

Selbstverständlich war es Sophos auch ein Anliegen zu erfahren, ob und inwieweit sich angesichts der weltpolitischen Lage und des aktuellen Kriegs in Europa, der bereits lange vor der eigentlichen militärischen Auseinandersetzung auf Cyberebene tobte, die Wahrnehmung und die Bedeutung von IT-Sicherheit innerhalb der letzten zwei Jahre verändert haben.

- Chefs bestätigen hohes Bewusstsein für Cybergefahren in ihren Unternehmen
- Bestehende IT-Sicherheitsinfrastrukturen werden als gut bewertet
- Die Sorge vor Cyberattacken ist in den Ländern unterschiedlich ausgeprägt

Die Bedeutung des Themas Cybersicherheit ist gewachsen

23 Prozent der Befragten aus deutschen Unternehmen mit mehr als 200 Angestellten sowie knapp 36 Prozent aus kleineren Unternehmen bestätigen, dass Cybersicherheit noch wichtiger geworden sei. In der Schweiz betonen dies mit 47,4 Prozent der Firmen mit mehr als 200 Mitarbeitern sowie 46,9 Prozent der kleineren Unternehmen insgesamt noch mehr Firmen. Die österreichische Sicht auf die Dinge ist hier ähnlich wie beim alpenländischen Nachbarn: Für 37,7 Prozent ist die Cybersicherheit insgesamt noch wichtiger geworden, größere Unternehmen machen sich hier mit knapp 53 Prozent mehr Sorgen als kleinere Betriebe (31 Prozent).

Bewertung des Bewusstseins für Cybergefahren: Deutschland gibt sich Spitzenwerte

Mehrheitlich jedoch wähnen sich Unternehmen in Sachen Bewusstsein für Cybergefahren bereits ohnehin auf einem hohen Wert: 53 Prozent der kleineren und sogar knapp 70 Prozent der größeren Unternehmen in Deutschland geben an, dass sich hinsichtlich des Bewusstseins für das Thema Cybersicherheit in den letzten zwei Jahren nichts verändert habe und man hierfür bereits ohnehin gut aufgestellt gewesen sei. In der Schweiz bestätigen dies 47,3 Prozent der kleineren und 40,6 Prozent der größeren Unternehmen, in Österreich antworten 61 Prozent der kleineren und 41 Prozent der größeren Unternehmen entsprechend.

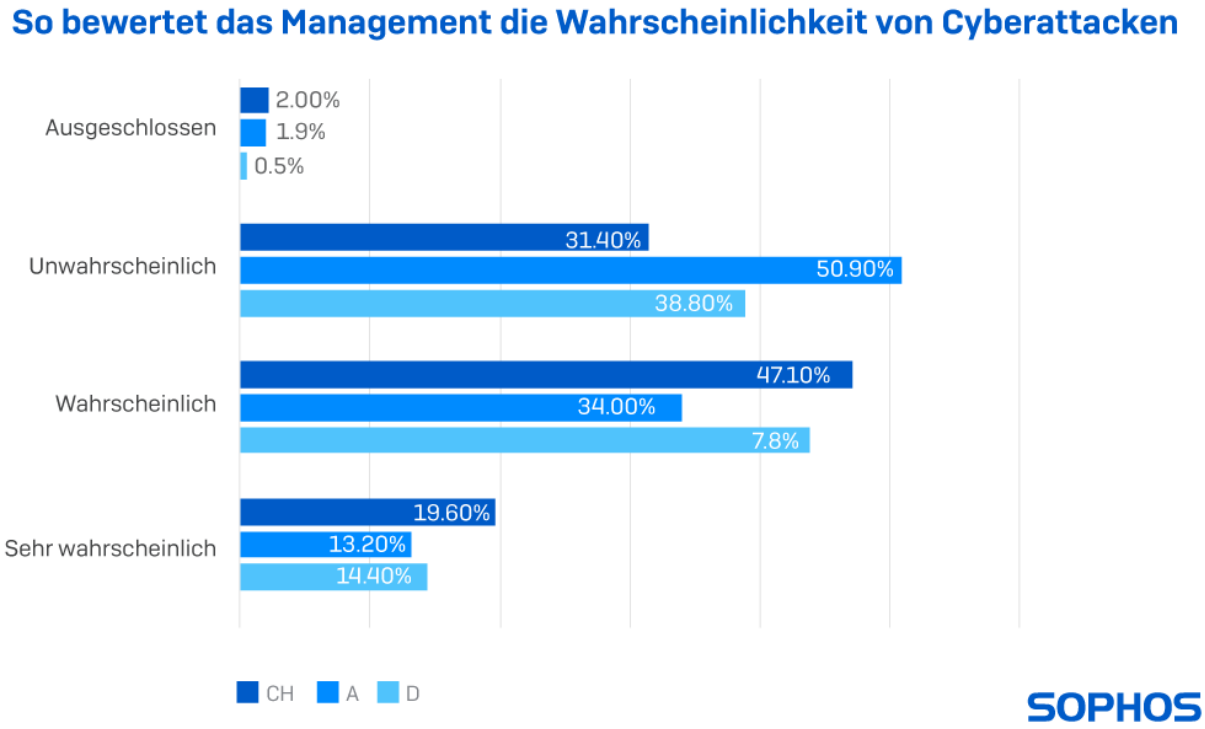
IT-Sicherheitsinfrastrukturen: Man fühlt sich gut aufgestellt

Auch in Bezug auf die bestehenden IT-Sicherheitsinfrastrukturen im Unternehmen herrscht Zufriedenheit: 62,2 Prozent der deutschen Manager geben an, ihr Unternehmen sei gut bis sehr gut gegen Cyberattacken gewappnet, bei den Leitungen unter 45 Jahren liegt dieser Wert sogar noch um 2,5 Prozentpunkte höher.

Auch in Österreich zeigt man sich zu 62,2 Prozent optimistisch in Bezug auf die Wirksamkeit der bestehenden IT-Sicherheitsstrukturen. Besonders gut aufgestellt wähnen sich die Unternehmen in der Schweiz, hier geben 72,5 Prozent der Befragten an, die Unternehmens-IT-Sicherheit sei auf Cyberangriffe gut vorbereitet.

Deutsche Unternehmensleitungen gehen am ehesten von künftigen Cyberangriffen aus, in Österreich dagegen ist gut die Hälfte optimistisch, verschont zu bleiben

Einen cyberkriminellen Angriff auf ihr Unternehmen halten gut 58 Prozent der deutschen Manager für wahrscheinlich bis sehr wahrscheinlich, in den Nachbarländern Österreich und Schweiz antworten jeweils gut 47 Prozent der Befragten entsprechend. Fast ein Drittel der Schweizer, knapp 39 Prozent der deutschen und sogar 51 Prozent der österreichischen Unternehmensführungen halten es dagegen für eher unwahrscheinlich, dass ihr Unternehmen künftig angegriffen werden könnte.



Chester Wisniewski: International ein ähnliches Bild

„Der Krieg in der Ukraine hat die Einstellungen nicht wirklich verändert, abgesehen von den kritischen US-Infrastrukturen. Die US-amerikanische CISA-Agentur hat ihre Bemühungen zur Verbesserung des Sicherheitsbewusstseins und in einigen Fällen der Meldepflichten für Anbieter kritischer Infrastrukturen verstärkt, aber außerhalb der USA oder in anderen Unternehmen des privaten Sektors sind keine großen Bedenken oder Maßnahmen zu erkennen."

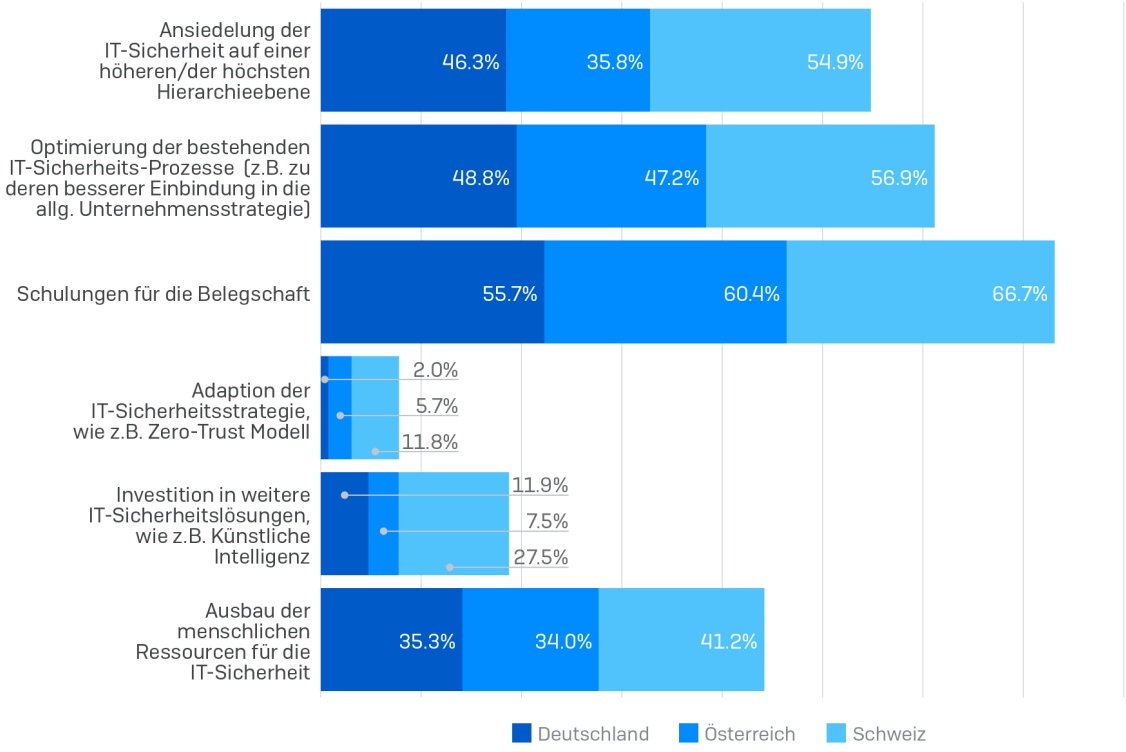
Fazit

Insgesamt nähern sich auch die Chefetagen zunehmend dem Thema Cybersicherheit. Dennoch obliegt die tatsächliche Verantwortung dafür den IT-Teams. Insbesondere bei großen Unternehmen war ein solches Ergebnis angesichts der komplexen und vielfältigen Anforderungen an Unternehmensentscheider durchaus zu erwarten und erscheint nachvollziehbar.

Unternehmen, so zeigt sich, investieren bereits viel und konstant in die IT-Sicherheit und haben das Thema – zumindest was die Einbettung in die Unternehmensstrategie betrifft – bereits in der Vergangenheit auf die Agenden höherer Hierarchieebenen gesetzt.

Gleichzeitig lässt sich feststellen, dass Unternehmensmanager mit konkreten, angesichts der Bedrohungslage entscheidenden, modernen Maßnahmen zur IT-Sicherheit noch fremdeln und hinsichtlich Investitionen in Technologien wie KI-gestützte Security-Lösungen oder auch Veränderungen in der IT-Sicherheitsstrategie hin zu Zero-Trust-Philosophien noch zögerlich erscheinen.

Verbesserung der Cybersicherheit im Unternehmen seit mindestens zwei, drei Jahren im Ländervergleich



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

TEIL II Branchenvergleich

Im folgenden zweiten Teil der Management-Studie werden die hierfür befragten Branchen im Einzelnen betrachtet: Handelsunternehmen, verarbeitendes Gewerbe und Dienstleistungsunternehmen.

II.1 Handelsunternehmen

Auswirkungen auf kaufmännische Abläufe und Zusatzkosten sind Sorge Nummer eins

Was fürchten die Führungsetagen im Handel am meisten, wenn es um die Sicherstellung der Cybersicherheit geht? Wie gut sind die Unternehmen dafür bereits aufgestellt, wo wird hierfür noch investiert und wer ist tatsächlich dafür zuständig, dass es klappt mit der IT-Sicherheit?

- Größte Sorge sind die Folgekosten und Störungen der kaufmännischen Abläufe
- Image relevanter als Lieferkette?

Die Kosten, die durch Cyberattacken entstehen können, sind die größte deutsche Sorge

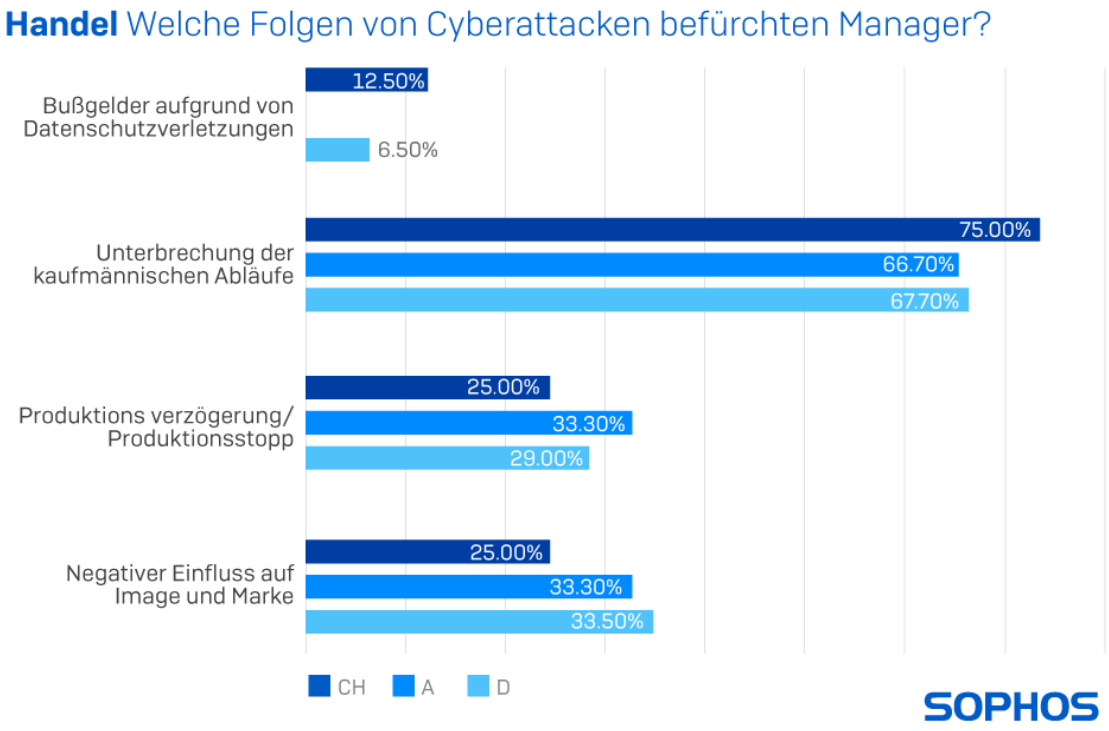
Mehr als alles andere fürchten Handelsunternehmen in Deutschland die Kosten, die durch die Wiederherstellung von Daten und Betriebsabläufen entstehen können. 77,4 Prozent der befragten Manager äußerten sich im deutschen Handel entsprechend. Und damit mehr als der Durchschnitt der Führungskräfte aus den anderen befragten Branchen (67,2 Prozent) und deutlich mehr als Handelschefs in Österreich (66,7 Prozent) und in der Schweiz (50 Prozent).

Worst-Case-Szenario aus Schweizer Sicht: Störung der kaufmännischen Abläufe

Auch die Unterbrechung kaufmännischer Abläufe ist eine Auswirkung, die Handelsunternehmen als Folge von Cyberattacken befürchten. In Deutschland nennen diesen Aspekt 67,7 Prozent der Befragten, in Österreich haben dies 66,7 Prozent auf dem Radar (und damit ist dies hier ebenso gefürchtet wie mögliche Zusatzkosten, siehe oben). Ganz vorne liegt bei diesem Punkt aber die Schweiz: Hier sorgen sich 75 Prozent der Leitungskräfte, dass eine Cyberattacke bedeutende negative Auswirkungen auf die kaufmännischen Abläufe haben könnte.

Image geht vor Lieferkette – besonders in Österreich, aber nicht in der Schweiz

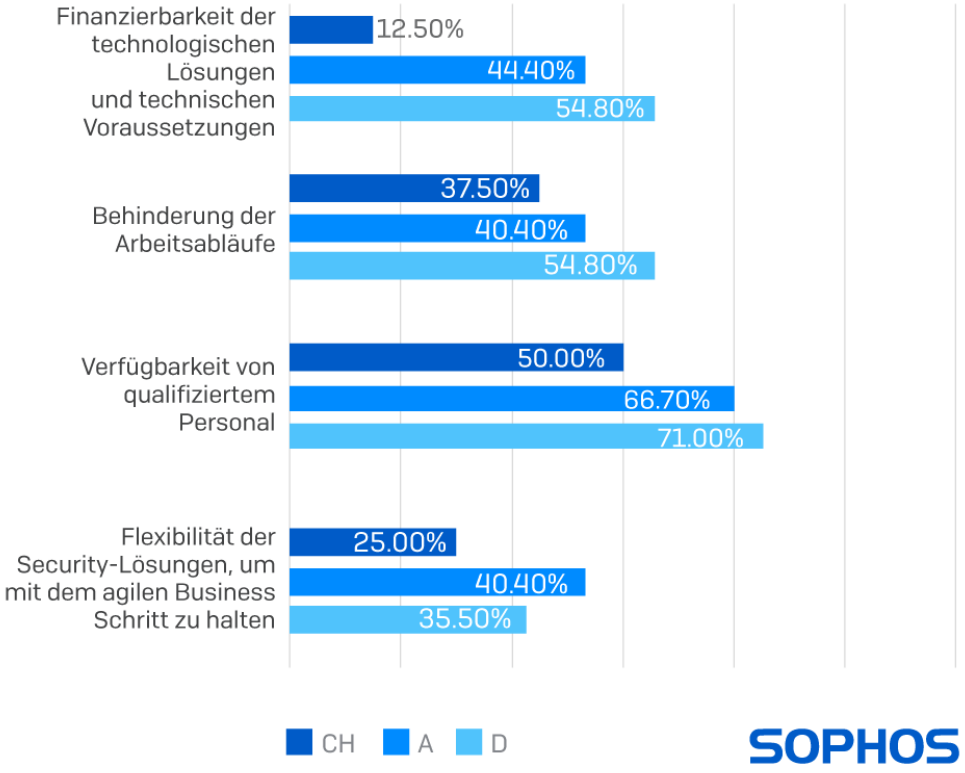
Bemerkenswert ist, dass alle befragten Unternehmensleitungen branchenübergreifend den möglichen Imageverlust mit durchschnittlich 27,9 Prozent besorgniserregender finden als etwa Schäden an der Lieferkette (22,9 Prozent). Immerhin: Im Vergleich zum verarbeitenden Gewerbe und Dienstleistung ist der Handel, was die Lieferketten angeht, zumindest in Deutschland und der Schweiz die am meisten sensibilisierte Branche. Raubt deutschen Managern zu 35,5 Prozent der mögliche Imageverlust den Schlaf, sind dies drohende Lieferkettenengpässe immerhin noch zu 32,3 Prozent. In Österreich ist einem guten Drittel der Unternehmensleitungen (33,3 Prozent) das Image dagegen deutlich mehr wert als die Lieferketten (22,2 Prozent). Lediglich in der Schweiz erachtet man die Lieferketten (37,5 Prozent) abweichend vom Rest aller Befragten sogar als schützenswerter als das Image (25 Prozent).



Personal als größte Herausforderung, vor allem in Deutschland, weniger in der Schweiz

Als die größte Herausforderung für die Umsetzung einer tragfähigen Cybersicherheit wird branchenübergreifend der Personalmangel genannt. In Deutschland mit einem branchenübergreifenden Höchstwert von 71 Prozent und in Österreich mit 66,7 Prozent. Auch hier ist die Schweiz die Ausnahme. So liegt hier der Wert mit 50 Prozent immer noch hoch, aber damit gleichzeitig niedriger als der Durchschnitt der anderen eidgenössischen Branchen (58,8 Prozent) wie auch der übrigen Branchen in Deutschland (62,7 Prozent) und Österreich (69,8 Prozent).

Handel
Herausforderungen für die Cybersicherheit aus Sicht des Managements



Handel in D und CH sieht sich gut gewappnet, Österreich mit befriedigendem Wert

Insgesamt sieht sich die Handelsbranche in DACH gut gegen Cybergefahren gerüstet. Der deutsche Handel attestiert sich, mit 61,3 Prozent im Branchenvergleich (47,8 Prozent) gut gegen Cybergefahren aufgestellt zu sein. Besonders gut gerüstet sieht sich die Schweiz: Schweizer Handelsunternehmen halten sich mit dem höchsten Branchenwert von 75 Prozent (Mittel 54,9 Prozent) für gut gegenüber Cybergefahren aufgestellt.

Die österreichischen Nachbarn sind etwas strenger im Urteil und geben sich zu 55,6 Prozent nur einen befriedigenden Wert – im Gegensatz zu verarbeitendem Gewerbe und Dienstleistungen, die sich im Alpenland gut aufgestellt sehen.

Neue Investitionen sind am ehesten in Deutschland geplant, der Schweizer Handel investiert am meisten

Auch bei der Frage zu weiterer Investitionsbereitschaft zeigen sich Unterschiede zwischen den Ländern: am wenigsten Bereitschaft, noch weitere Investitionen in die Cybersicherheit zu tätigen, zeigt der österreichische Handel mit 66,7 Prozent (andere Branchen 58,8 Prozent) – und das, obwohl man sich hinsichtlich der bereits bestehenden Maßnahmen nur ein „befriedigend" gegeben hat.

In der Schweiz will jeder Zweite keine weiteren Sicherheitsaktivitäten mehr finanzieren

Deutschland zeigt sich investitionsbereiter: Nur knapp jeder dritte (29 Prozent) leitende Mitarbeiter im Handel lehnt eine Budgeterhöhung ab – andere deutsche Branchen sagen hier öfter nein.

Insgesamt investiert der eidgenössische Handel im Vergleich zu Deutschland und Österreich die höchsten Summen in Security-Maßnahmen.

Wo stehen Chefs am IT-Sicherheits-Ruder? In Deutschland mehr, in Österreich weniger

In Deutschland geben im Branchenvergleich mit 22,6 Prozent mehr Leitungskräfte im Handel an, für die Cybersicherheit selbst zuständig zu sein, als in den anderen Branchen (16,4 Prozent) und den Nachbarländern. Jeweils ungefähr ein gutes Drittel der deutschen Unternehmen vertraut in dieser Frage der internen IT-Abteilung (35,5 Prozent) bzw. einem externen Dienstleister (32,3 Prozent). In der Schweiz sind mit 12,5 Prozent deutlich weniger Chefs selbst in der Verantwortung. In eidgenössischen Unternehmen sind zu jeweils 37,5 Prozent die interne IT oder externe Anbieter in der Pflicht. Die wenigsten Unternehmenslenker sind in Österreich selbst am Ruder (11,1 Prozent), auch externe Dienstleister (22,2 Prozent) sind weniger involviert als in den Nachbarländern. Österreichs Handel setzt in Sachen Cybersicherheit vor allem auf die Expertise der eigenen IT-Leute (55,6 Prozent).

Schweizer Handelsunternehmen rechnen am wenigsten mit Cyberangriffen

Befragt, für wie wahrscheinlich sie einen Cyberangriff auf ihr Unternehmen halten, gibt eine knappe Mehrheit der deutschen Handelsunternehmen an, einen Angriff für sehr wahrscheinlich (9,7 Prozent) oder wahrscheinlich (45,2 Prozent) zu halten. Als unwahrscheinlich bezeichnen 41,9 Prozent der Unternehmen einen Cyberangriff.

Ein anderes Bild zeigt sich in Österreich. Hier geht eine knappe Mehrheit (55,6 Prozent) davon aus, dass mit einer Attacke auf die IT-Systeme eher nicht zu rechnen ist. Einen Angriff als wahrscheinlich sehen 33,3 Prozent der Befragten an und als sehr wahrscheinlich benennen ihn 11,1 Prozent der österreichischen Handelsunternehmen.

Noch sicherer wiegen sich Unternehmen in der Schweiz. Hier gehen 12,5 Prozent davon aus, dass ein Angriff sehr wahrscheinlich ist, 25 Prozent sehen hierin ein wahrscheinliches Szenario. 50 Prozent der eidgenössischen Händler sehen in einem Cyberangriff einen eher unwahrscheinlichen Fall. Und einzig in der Schweiz sagen 12,5 Prozent der Befragten sogar, dass sie einen Angriff für ausgeschlossen halten.

II.2 Verarbeitendes Gewerbe

Mehr als 60 Prozent der DACH-Manager im verarbeitenden Gewerbe rechnen künftig mit einem Cyberangriff

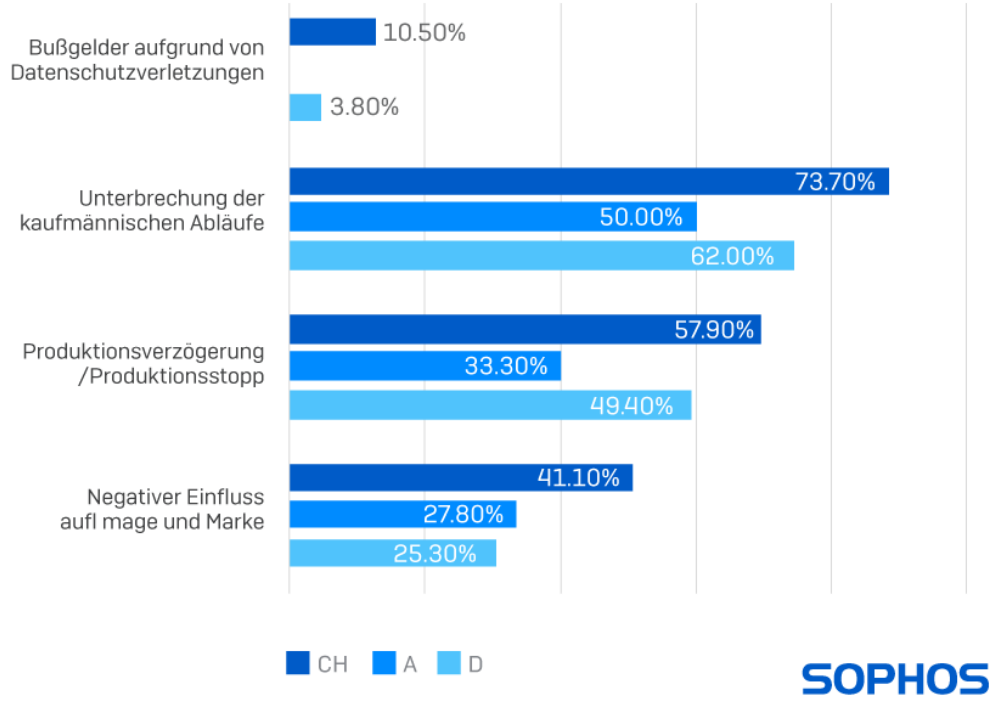
- Eine deutliche Mehrheit rechnet künftig mit einem Cyberangriff
- Unternehmen sehen sich gegen Cyberattacken gut gerüstet
- Verantwortlichkeiten für die IT in Firmen im DACH-Vergleich unterschiedlich verteilt

Im Sektor „Verarbeitendes Gewerbe" rechnet die Mehrheit des Unternehmensmanagements künftig mit einem Cyberangriff: Einen Cyberangriff auf ihr Unternehmen halten 63 Prozent der deutschen, 61 Prozent der österreichischen und 68 der Schweizer Führungskräfte für wahrscheinlich oder sehr wahrscheinlich.

Wie in anderen Branchen auch **fürchten sie als wirtschaftliche Auswirkungen** besonders Störungen in kaufmännischen Abläufen. Dies sagen 62 Prozent der deutschen, 50 Prozent der österreichischen und 74 Prozent der Schweizer Manager. Auch befürchten sie Produktionsverzögerungen oder einen Produktionsstopp. Dies geben 49 Prozent der befragten Führungskräfte in Deutschland, 33 Prozent in Österreich und 58 Prozent der Schweizer Manager an.

Einen negativen Einfluss auf Image und Marke durch einen Cyberangriff erwarten mit 42 Prozent die Chefs in der Schweiz, während dies lediglich 25 Prozent der deutschen und 28 Prozent der österreichischen Chefs denken. Auch die Sorge um Bußgelder aufgrund von Datenschutzverletzungen als wirtschaftlicher Auswirkung eines Cyberangriffs treibt Schweizer Führungskräfte mit knapp über 10 Prozent um; stärker als ihre Pendants in Deutschland (4 Prozent) und Österreich (0 Prozent).

Verarbeitendes Gewerbe
Welche Folgen von Cyberattacken befürchten Manager?



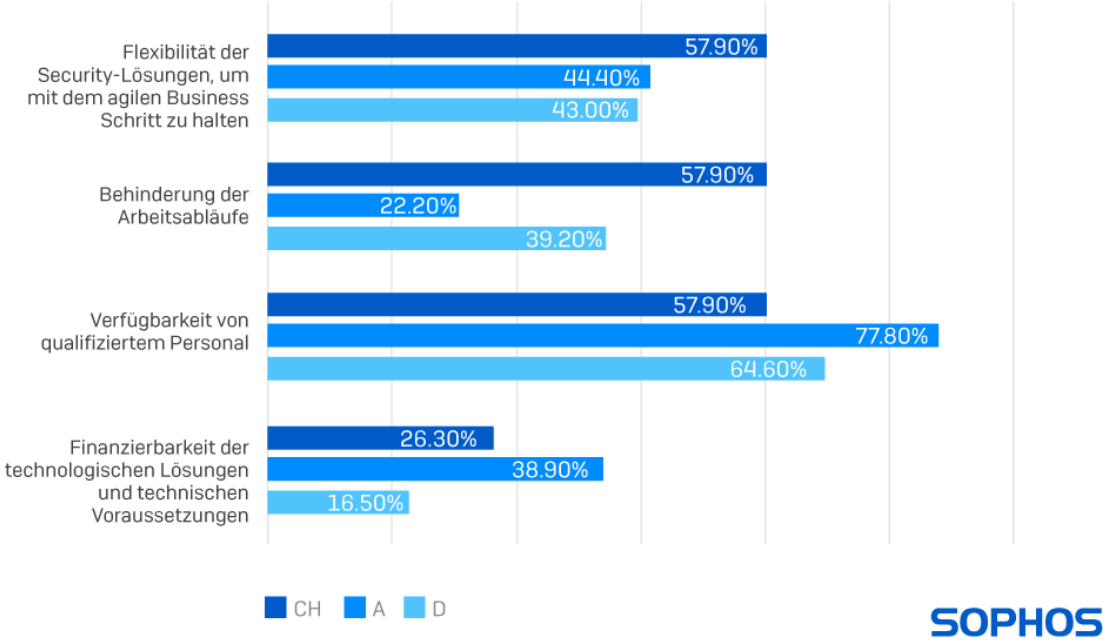
Cybersicherheit ist an Bedeutung gewachsen, besonders in der Schweiz

Insgesamt hat sich die Wahrnehmung und Bedeutung von Cybersicherheit bei vielen leitenden Mitarbeitenden in den DACH-Unternehmen des verarbeitenden Gewerbes in den letzten zwei bis drei Jahren verändert. So geben mit 33 Prozent rund ein Drittel der Führungskräfte in Deutschland und 39 Prozent der österreichischen Manager an, dass Cybersicherheit für sie noch wichtiger geworden ist. In der Schweiz meinen dies sogar mehr als die Hälfte (53 Prozent).

Weitere Investitionen vor allem in Deutschland und der Schweiz

Demzufolge sind auch die gesamten Investitionen in Cyberschutz und IT-Sicherheit in den Unternehmen gestiegen. 2022 wurden nach Angaben der Führungskräfte im verarbeitenden Gewerbe in DACH diese Investitionen erhöht. Dabei war die Schweiz mit fast 53 Prozent Spitzenreiter, gefolgt von den österreichischen Unternehmen mit 39 Prozent und deutschen Unternehmen mit 33 Prozent. Künftig sollen laut den Managements im verarbeitenden Gewerbe die Cybersecurity-Maßnahmen verstärkt werden, wobei Führungskräfte in der DACH-Region insbesondere in weitere IT-Security-Lösungen, wie z. B. in KI, investieren möchten. Im Ländervergleich bestehen allerdings Unterschiede: So planen in Deutschland 35,4 Prozent der Chefs und in der Schweiz knapp 37 Prozent, mehr Geld dafür in die Hand zu nehmen; in Österreich sind dies lediglich 27,5 Prozent.

Verarbeitendes Gewerbe
Herausforderungen für die Cybersicherheit aus Sicht des Managements



Aufstockung von Fachpersonal: Ziel und Herausforderung zugleich

Dass das Thema Cybersecurity verstärkt in den Mittelpunkt der DACH-Führungskräfte im verarbeitenden Gewerbe gerückt ist, zeigt auch der Ausbau der IT-Sicherheitsfachkräfte in diesen Unternehmen. So haben in den vergangenen zwei bis drei Jahren 56 Prozent der Führungskräfte in Deutschland (Österreich 66 Prozent; Schweiz 68 Prozent) Fachkräfte für IT-Sicherheit aufgestockt. 22 Prozent der deutschen Führungskräfte planen auch zukünftig, weitere Fachkräfte einzustellen (Österreich: 17 Prozent; Schweiz: 15 Prozent). Diese Maßnahme zur Sicherstellung und Umsetzung der Cybersecurity beinhaltet allerdings auch eine große Herausforderung, denn wie in allen Bereichen besteht auch hier ein großer Fachkräftemangel. Dass es an qualifiziertem Fachpersonal mangelt, meinen 65 Prozent der deutschen, 78 Prozent der österreichischen und 58 Prozent der Schweizer Manager.

Eigene Cybersicherheitsinstanz: Schweiz mit höchstem Wert

Hinsichtlich der für die Cybersicherheit im verarbeitenden Gewerbe verantwortlichen Akteure bestehen in den DACH-Ländern große Unterschiede. Während in 39 Prozent der österreichischen Unternehmen die IT-Abteilung für die Cybersicherheit verantwortlich ist, sind dies in Deutschland 48 Prozent und in der Schweiz 47 Prozent. Über eine dezidierte Cybersicherheitsinstanz im Unternehmen verfügen 9 Prozent der deutschen, 11 Prozent der österreichischen und 26 Prozent der Schweizer Unternehmen. Ein Drittel der österreichischen Führungskräfte (33 Prozent) und 29 Prozent der deutschen Führungskräfte vertrauen externen Dienstleistungsunternehmen; in der Schweiz sind dies lediglich 15 Prozent.

Chefsache ist die IT-Sicherheit in nur wenigen Unternehmen aus dem verarbeitenden Gewerbe: Das Thema ist lediglich bei 14 Prozent der deutschen, 11 Prozent der österreichischen und 11 Prozent der Schweizer Unternehmen direkt auf Geschäftsführer- bzw. Vorstandsebene angesiedelt.

Höchster Branchenwert: Schweizer Unternehmen sehen sich besonders gut gerüstet

Insgesamt sieht sich das verarbeitende Gewerbe in DACH gut gegen Cybergefahren gerüstet: 62 Prozent der Manager in Deutschland und 61 Prozent in Österreich meinen, gut bis sehr gut gegen Cybergefahren aufgestellt zu sein. Besonders gut gerüstet sieht sich die Schweiz: Führungskräfte der Schweizer Unternehmen aus dem verarbeitenden Gewerbe halten sich mit dem höchsten Branchenwert von 79 Prozent für gut bis sehr gut gegenüber Cybergefahren aufgestellt.

II.3 Dienstleistungsunternehmen

Optimale Cybersicherheit für Dienstleister? Nur mit externer Beratung und qualifiziertem Personal

- Dienstleistungsunternehmen in DACH fühlen sich gut gegen kommende Cybergefahren gerüstet, aber: Sie sehen ihren Schutz auch in Gefahr
- Mangel an Fachpersonal, fehlende externe Beratungsangebote und gestörte Arbeitsabläufe bereiten ihnen Sorgen

Im Segment Dienstleistungen ist man länderübergreifend frohen Mutes, die anstehenden Cyberbedrohungen dank mehrjähriger Aufrüstung in Technik und Teamschulungen gut überstehen zu können.

Wer kümmert sich um die IT-Sicherheit?

Die Mehrheit der Dienstleistungsunternehmen in DACH lagert ihre IT-Sicherheit aus: Etwas mehr als der Durchschnitt im Branchenvergleich, also etwas mehr als ein Drittel, vertraut einem externen IT-Dienstleistungsunternehmen. Etwas weniger als ein Drittel und somit auch etwas weniger als der Durchschnitt beauftragt die eigene IT-Abteilung mit der IT-Sicherheit. Dass hier keine eigene große Logistik aufgebaut, sondern auf eingekaufte IT-Angebote zurückgegriffen wird, erklärt sich aufgrund der großen Anzahl oft nur singulär betriebener Dienstleistungsangebote, die sich vom Nagelstudio über den freiberuflichen Architekten bis zur Altenpflege erstrecken.

Kennen sich Mitarbeiter und Chefs mit IT-Sicherheit aus?

Insgesamt bewertet das österreichische (50 Prozent), Schweizer (41,7 Prozent) und deutsche (41,8 Prozent) Management das Sicherheitsbewusstsein der Dienstleistungsmitarbeitenden als „befriedigend".

Österreichische Dienstleister-Chefs stellen sich mit 50 Prozent ein „sehr gut" aus (Mittel 41,5 Prozent). Auch die Angestellten kommen gut weg: Deutlich über dem Durchschnitt von 13,2 Prozent attestieren sie ihnen mit 19,2 Prozent ein „sehr gut".

Deutschland hält ebenfalls viel vom Sicherheitsbewusstsein seiner Dienstleistungsteams und vergibt überdurchschnittlich (9,5 Prozent) oft die Bestnote (11 Prozent). Die Chefs schneiden in Deutschland und der Schweiz mit einer insgesamt guten Bewertung besser als die Mitarbeitenden ab.

Gewappnet: Unternehmen glauben, bestehende IT-Sicherheit hält Bedrohungen stand

Wie bewerten Manager im Dienstleistungswesen die bestehenden Cybersicherheitsinfrastrukturen im Unternehmen? Grundsätzlich zeigen sich die Befragten hier zuversichtlich, die Mehrheit geht davon aus, dass die bestehenden Systeme einen guten Schutz bieten.

In Deutschland fühlen sich 15,4 Prozent sehr gut, 42,9 Prozent gut und 30,8 Prozent immerhin noch befriedigend gewappnet. Ein ähnliches Bild zeigt sich in der Schweiz. Hier geht man zu 12,3 Prozent davon aus, sehr gut, zu 54,2 Prozent gut und zu 29,2 Prozent befriedigend aufgestellt zu sein. Österreichs Handelsunternehmen sind aus Sicht der befragten C-Level-Führungskräfte sehr gut gegen Cyberangriffe aufgestellt. 65,4 Prozent sagen, sie sind gut aufgestellt, 7,7 Prozent bezeichnen die bestehende Cybersicherheit sogar als sehr gut.

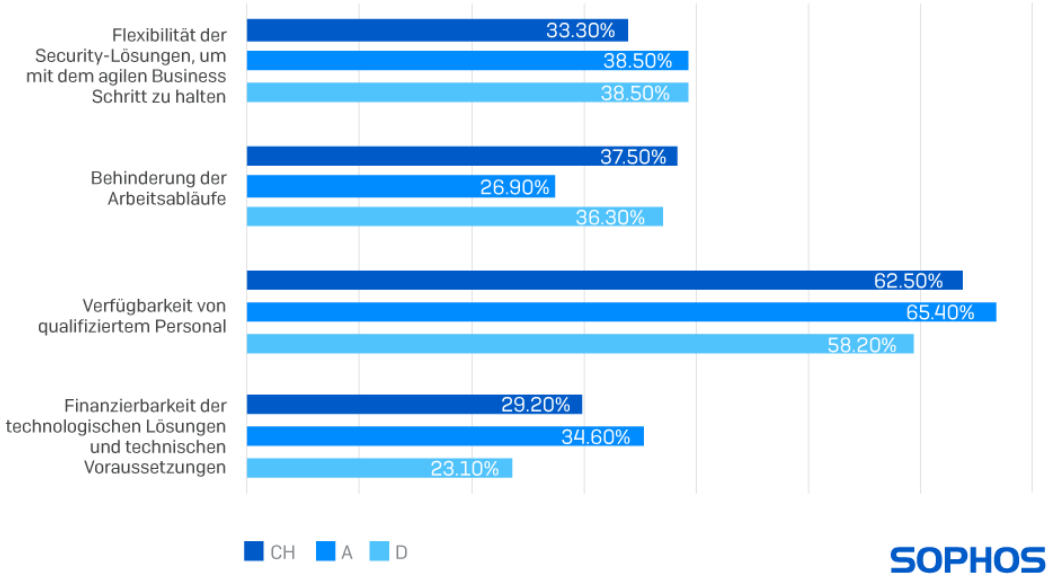
Was hemmt die eigene Cybersicherheit?

Herausforderungen bei der eigenen Cybersicherheit gibt es dennoch: Während deutschen Dienstleistern mit 15,4 Prozent über dem Durchschnitt von 13,9 Prozent die Verfügbarkeit von externen Beratungsdienstleistungen fehlt, stresst die Österreicher eher der notwendige Zeitrahmen, den sie zu immerhin 26,9 Prozent benennen und damit deutlich höher als der Gesamtdurchschnitt (17 Prozent). Die Schweiz bemängelt mit 62,5 Prozent und damit auch im Vergleich mit den beiden anderen Branchen am häufigsten das fehlende qualifizierte Personal. Die Finanzierbarkeit geeigneter Abwehrmaßnahmen steht für alle im Raum, hier zeigten sich deutsche Firmenleitungen etwas gelassener als österreichische.

Auch in der Dienstleistungsbranche hält sich zudem der Glaube, dass IT-Sicherheitslösungen die Arbeitsabläufe verlangsamen oder anderweitig behindern könnten. Schweizer und deutsche Chefs antworten zu rund 38 Prozent entsprechend, in Österreich zeigt man sich hier milder im Urteil, weniger als ein Drittel der Befragten geht hier von Beeinträchtigungen durch Security-Lösungen aus.

Auch bei der Flexibilität der Security-Lösungen angesichts agiler Arbeitsweisen und Homeoffice etc. halten sich bei Dienstleistungs-Chefs Zweifel. Knapp 40 Prozent der deutschen und österreichischen Befragten äußern sich dahin gehend. Schweizer Entscheider haben hier mit gut 30 Prozent etwas weniger Zweifel als die Kollegen der Nachbarländer.

Dienstleistung
Herausforderungen für die Cybersicherheit aus Sicht des Managements



Cyberangriffe vermuten eher Deutschland und die Schweiz, Österreich fühlt sich sicher

Mehrheitlich gehen deutsche Dienstleistungsunternehmen davon aus, dass Cyberangriffe auf ihr Unternehmen im Rahmen der Möglichkeit sind. Zu 15,4 Prozent – und damit mit einem branchenübergreifend sehr hohen Wert – gehen Dienstleistungsentscheider davon aus, dass Angriffe sehr wahrscheinlich sind, 39,6 Prozent halten sie für wahrscheinlich. Als unwahrscheinlich sehen 41,8 Prozent Angriffe an und 1,1 Prozent sagen sogar: ausgeschlossen.

Auch Schweizer Dienstleistungsunternehmen gehen mehrheitlich von einer Angriffsbedrohung aus, 25 Prozent halten einen solchen Fall für sehr wahrscheinlich, 50 Prozent für wahrscheinlich. Als unwahrscheinlich beziffern 25 Prozent ein entsprechendes Szenario.

Anders in Österreich: Hier gibt man sich gelassen und sieht einen Cyberangriff zu 57,7 Prozent als unwahrscheinlich an, 3,8 Prozent halten ihn gar für ausgeschlossen. Weniger als in den Nachbarländern sehen in einem Angriff auf die IT-Systeme des Unternehmens einen wahrscheinlichen (30,8 Prozent) oder sehr wahrscheinlichen Fall (7,7 Prozent).

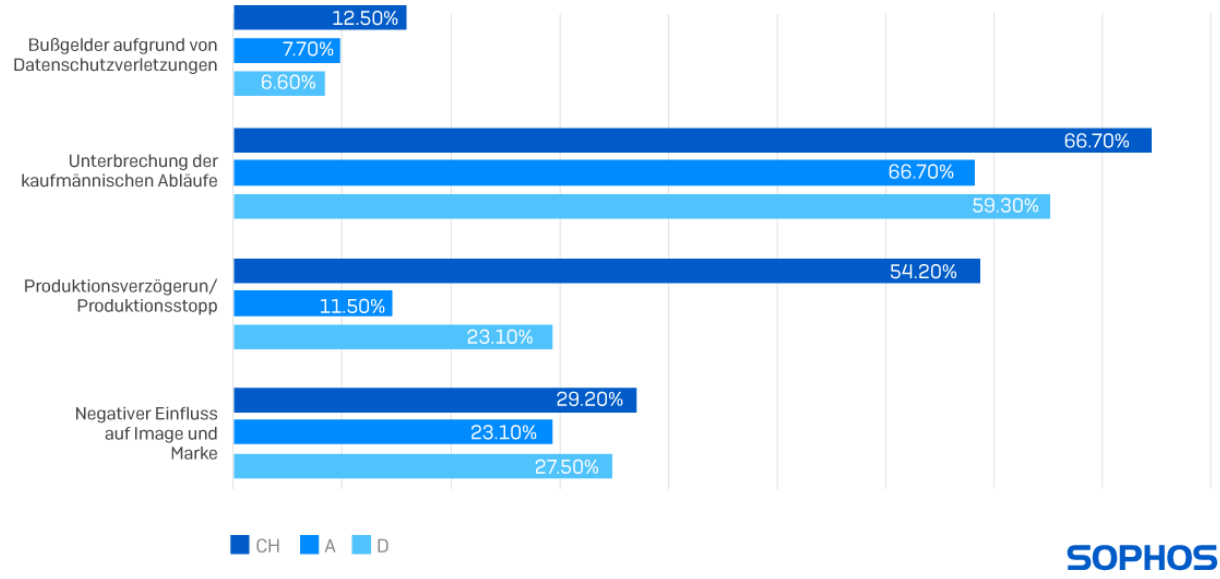
Folgen von Cyberattacken beschäftigen Schweizer Unternehmen mehr, österreichische weniger

Ähnlich wie in den anderen Branchen und in allen Ländern geht es auch den Dienstleistungsunternehmen vor allem um die wirtschaftlichen Schäden, die durch Cyberangriffe entstehen können. An Platz eins stehen dabei die möglichen Unterbrechungen in den kaufmännischen Abläufen, die durch Ausfälle nach Angriffen entstehen können, gefolgt von Kosten durch Wiederherstellungsmaßnahmen

sowie Produktionsverzögerungen oder -stopps. Auch ein negativer Einfluss auf Image und Marke beschäftigt immer noch knapp ein Drittel der Befragten. Kaum ins Gewicht fällt dagegen die Sorge vor Bußgeldbescheiden aufgrund von Datenschutzverletzungen – mit Ausnahme der Schweizer Unternehmen.

Auffällig ist insgesamt, dass Schweizer Unternehmen bei allen genannten möglichen Folgen aus Cyberattacken die meisten Befürchtungen äußern. Insbesondere drohende Produktionsverzögerungen oder -ausfälle bewerten die eidgenössischen Befragten mit rund 67 Prozent mehr als doppelt bzw. dreimal maßgeblicher als die deutschen (rund 23 Prozent) und österreichischen (rund 12 Prozent) Kollegen.

Dienstleistung
Welche Folgen von Cyberattacken befürchten Manager?



Schweizer Unternehmen haben zuletzt am meisten Investitionen in die IT-Sicherheit gesteigert, österreichische Händler haben zu einem kleinen Prozentsatz sogar Kosten gekürzt

Handelsunternehmen in Deutschland haben zu 38,5 Prozent mehr Geld in die IT-Sicherheit gesteckt, bei 58,1 Prozent der Unternehmen ist die Investitionshöhe gleich geblieben.

Die Kosten erhöht haben vor allen Dingen Schweizer Unternehmen des Handelsbereichs, hier geben 45,8 Prozent der Befragten an, mehr investiert zu haben. Bei 50 Prozent sind die Investitionssummen unverändert geblieben.

Österreichische Handelsunternehmen haben der Befragung nach ihre Investitionen in die Sicherheit ihrer Daten und IT-Systeme in den letzten 24 Monaten zu 30,8 Prozent erhöht, während 46,2 Prozent angeben, dass ihre Investitionen stabil geblieben sind. Und 3,8 Prozent der Händler im Alpenland haben sich sogar eine Kosteneinsparung verordnet.

Ein geringer Prozentsatz aller befragten Entscheidungsträger konnte zu diesem Punkt keine Angaben machen.

Appendix

Schulungen des Personals sind branchenübergreifend die wichtigste zusätzliche Sicherheitsmaßnahme

- Verarbeitendes Gewerbe schult am intensivsten
- Nachholbedarf besteht bei Handelsunternehmen

Im Branchenvergleich zeigt sich, dass Unternehmensleitungen der drei befragten Branchen neben Investitionssteigerungen vor allem in der Schulung ihrer Angestellten einen entscheidenden Faktor für die Sicherstellung der Cybersicherheit in ihren Unternehmen sehen.

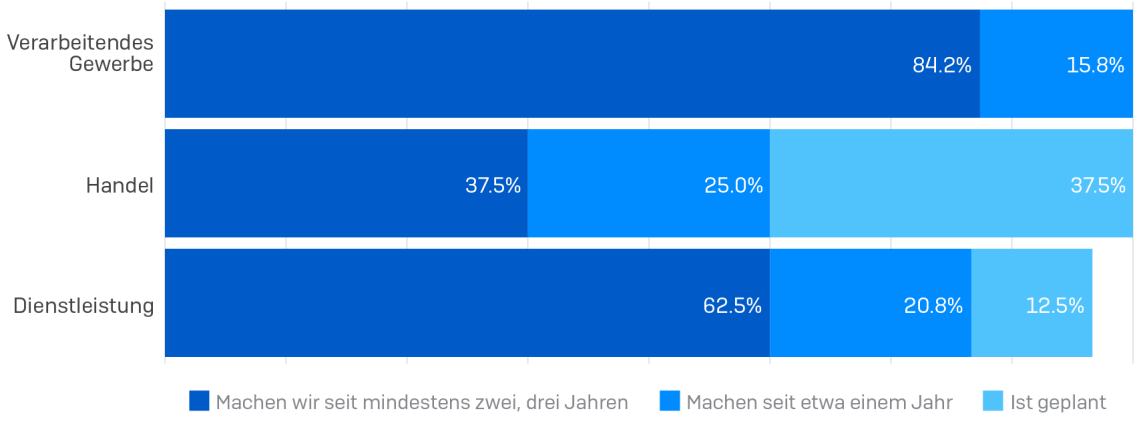
Das verarbeitende Gewerbe in Deutschland ist dabei mit 64,6 Prozent bei der Schulung seit mehreren Jahren besonders engagiert, der Handel bildet seine Mitarbeitenden dagegen mehrheitlich erst seit etwa einem Jahr dahin gehend aus (41,9 Prozent).

Im Nachbarland Österreich investieren die Chefs mit 64,4 Prozent ebenfalls seit mindestens zwei, drei Jahren als wichtigste ihrer Schutzmaßnahmen in die Sicherheitsfähigkeiten ihrer Beschäftigten. Im Handel ist dieser Wert mit 44,4 Prozent am geringsten. Seit erst einem Jahr hält rund jedes fünfte Unternehmen Mitarbeiterschulungen ab (20,8 Prozent). Auch hier zeigt sich wieder ein starker Unterschied zwischen verarbeitendem Gewerbe (27,8 Prozent) und Handel (11,1 Prozent), wobei der Handel mit 33,3 Prozent angibt, diese zu planen.

Die Eidgenossen sehen ebenfalls die Schulung der Belegschaft mit 66,7 Prozent als wichtigste Maßnahme zur Verbesserung der Cybersicherheit und betreiben dies seit mindestens zwei, drei Jahren. Das Schweizer verarbeitende Gewerbe liegt hier mit 84,2 Prozent deutlich über dem Durchschnitt, der Handel mit 37,5 Prozent stark darunter, die Dienstleister mit 62,5 Prozent nahe am Durchschnitt. Die Betriebsgröße ist in der Schweiz kein entscheidender Parameter und weicht nur marginal vom Durchschnitt ab.

Länderübergreifend zeigt sich folgendes Bild: Das verarbeitende Gewerbe schult sein Angestellten bereits am längsten auf gutem Niveau, Dienstleistungsunternehmen arbeiten zu einem hohen Prozentsatz ebenfalls daran, ihre Belegschaft auf Cybergefahren vorzubereiten, 12,5 Prozent der Unternehmen sind hierfür noch in Planung. Den meisten Aufholbedarf haben Handelsunternehmen, bei denen 37,5 Prozent der Befragten angeben, hinsichtlich Mitarbeiterschulungen in der Planung zu sein.

Schulung der Mitarbeiter als Verbesserungen der Cybersicherheit über alle Länder nach Branche



Quelle: Sophos/IPSOS Studie 2022
Die Umfrage wurde von IPSOS bei 200 deutschen, 50 österreichischen und 50 Schweizer Unternehmen mit mindestens 50 Mitarbeitern bei der Geschäftsleitung durchgeführt.

SOPHOS

Sophos Deutschland
Tel: +49 800 2782761
Email: sales@sophos.de

2023-02-24 WP (MP)