SOPHOS

CYBERSICHERHEIT IST IM OBEREN MANAGEMENT ANGEKOMMEN – ABER NICHT ÜBERALL CHEFSACHE

Eine Studie über Wahrnehmung, Verantwortung und Chancen im DACH-Raum

Ein Sophos Whitepaper. November 2025

Inhalt

Einführung

Glaubt man den zahlreichen Podiumsdiskussionen, Interviews und Experteneinschätzungen, ist Cybersicherheit zur Chefsache erklärt. Doch wie sieht die Realität tatsächlich aus?

Zum dritten Mal hat das Marktforschungsinstitut Ipsos im Auftrag von Sophos die Frage gestellt: „Chef, wie hältst du's mit der Cybersicherheit?" Anders als übliche IT-Studien richtet sich diese Untersuchung exklusiv an das Top-Management in Deutschland, Österreich und der Schweiz: Geschäftsführer, Eigentümer, Direktoren und Senior Manager.

Statt technischer Details stehen hier Wahrnehmungen, Prioritäten und Entscheidungen in den Chefetagen im Fokus und wie unterschiedlich diese in Handel, Produktion und Dienstleistungen ausfallen.

Die folgenden Erkenntnisse zeigen: Cybersicherheit ist fest auf der Agenda, aber längst nicht überall auf der obersten Ebene verankert.

Kapitel 1 – Die wichtigsten Ergebnisse

- Über **60 % der Führungskräfte** in DACH hatten bereits direkten Kontakt mit Cybervorfällen.
- **36–42 %** geben an, Cybersicherheit an andere Ebenen zu delegieren.
- **47–60 %** erweitern Schutzmaßnahmen erst, wenn Schlagzeilen über staatliche Angriffe Druck erzeugen.
- Nur **16–22 %** betrachten KI heute als wichtiges Abwehrinstrument, während rund die Hälfte die Auswirkungen nicht einschätzen kann.
- **63–70 %** sind überzeugt, dass große Organisationen bessere Cyberschutzressourcen haben als kleinere.
- Über **80 %** der Führungskräfte lehnen Cybersicherheitsmaßnahmen so gut wie nie ab; wo es doch passiert, liegt es an zu hohen Kosten oder Komplexität.
- Nur **8–15 %** räumen ein, bewusst Risiken in Kauf genommen zu haben, die große Mehrheit verfolgt eine sicherheitsorientierte Haltung.

der Führungskräfte in DACH hatten bereits direkten Kontakt mit Cybervorfällen.

Cyberschutz ist auf der Agenda, aber ...

Digitale Sicherheit ist ein Thema im Top-Management. Dennoch wird Verantwortung häufig weitergereicht. Führungskräfte befassen sich oft erst dann persönlich damit, wenn ein Vorfall im eigenen Unternehmen auftritt oder wenn öffentliche Diskussionen Druck erzeugen.

KI, die große Unbekannte

Künstliche Intelligenz wird von den Führungsetagen registriert, bleibt jedoch ein Feld voller Unsicherheiten. Nur wenige glauben aktuell an ihren Nutzen für die Abwehr, ähnlich viele sehen sie eher als Bedrohung. Die größte Gruppe verharrt abwartend.

Das David-und-Goliath-Gefühl

Führungskräfte sehen Konzerne in nahezu allen Bereichen im Vorteil: Budget, Personal, Attraktivität für Fachkräfte. Kleinere Betriebe setzen auf externe Partner, haben aber oft das Gefühl, strukturell benachteiligt zu sein.

Viel Sicherheitsorientierung, wenig Risiko

Die Chefetagen im DACH-Raum sind vorsichtig: Maßnahmen werden nur selten abgelehnt, und bewusst eingegangene Risiken bleiben die Ausnahme. Wo es dennoch dazu kommt, sind fehlende Ressourcen oder hohe Komplexität die Ursachen.

Fazit

Cybersicherheit ist ein Thema in den Führungsetagen im DACH-Raum. Dennoch wird Verantwortung häufig delegiert, und Maßnahmen folgen oft äußeren Anlässen statt einer kontinuierlichen Strategie. Die Studie zeigt deutliche Unterschiede zwischen Handel, Produktion und Dienstleistungssektor – vom Umgang mit Risiken bis zur Einschätzung neuer Technologien (Details im Branchenvergleich, Kapitel 4).

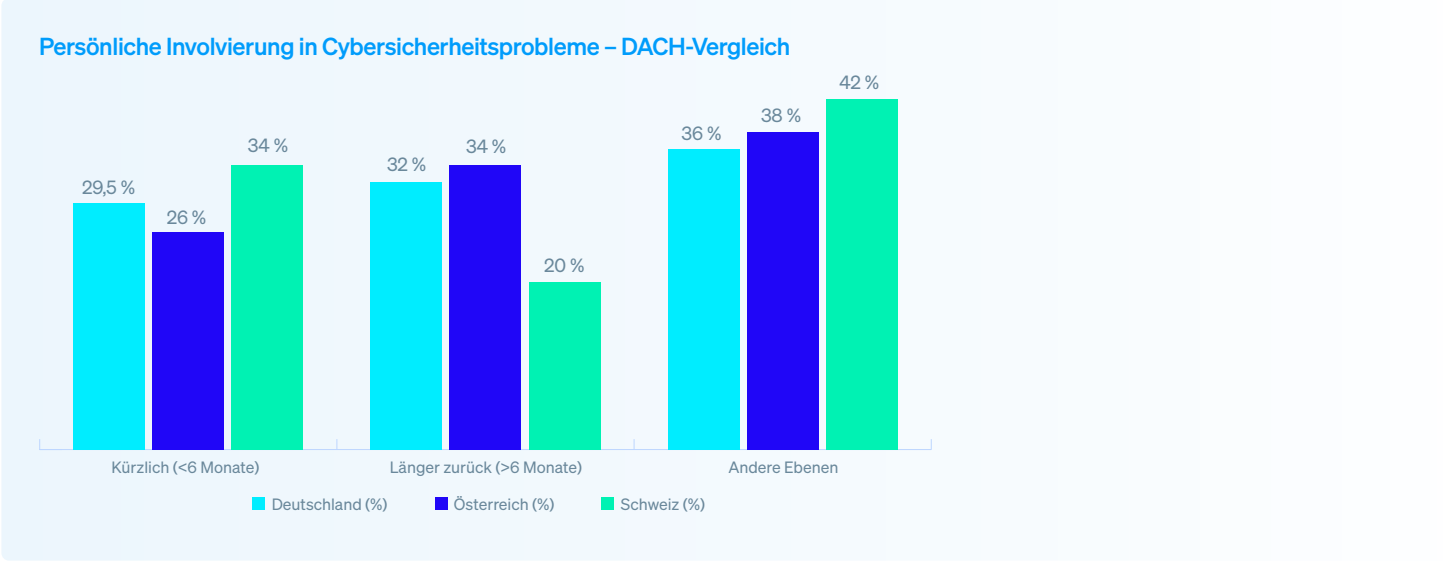
Drei zentrale Aufgaben ergeben sich für Führungskräfte: Verantwortung konsequent auf Top-Level verankern, strukturelle Ungleichgewichte zwischen großen und kleinen Unternehmen aktiv ausgleichen und einen klareren Kurs im Umgang mit KI entwickeln.

Kapitel 2 – Cybersicherheit im DACH-Raum

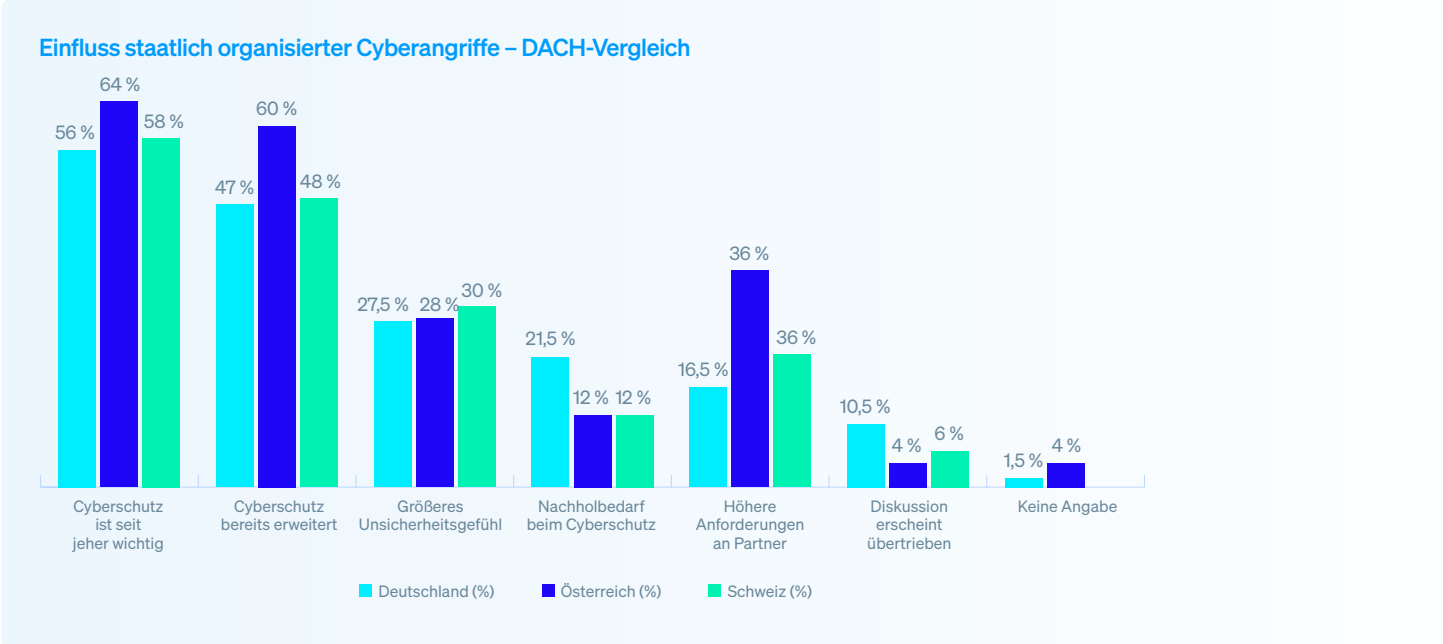
Cyberangriffe sind inzwischen Teil der täglichen Realität von Unternehmen aller Größen und Branchen. Mit der Zunahme digitaler Prozesse, vernetzter Lieferketten und wachsender Datenmengen ist Cybersicherheit zu einem zentralen Wettbewerbsfaktor geworden und damit zu einer Aufgabe für das Top-Management.

2.1 Die Ausgangslage in Zahlen

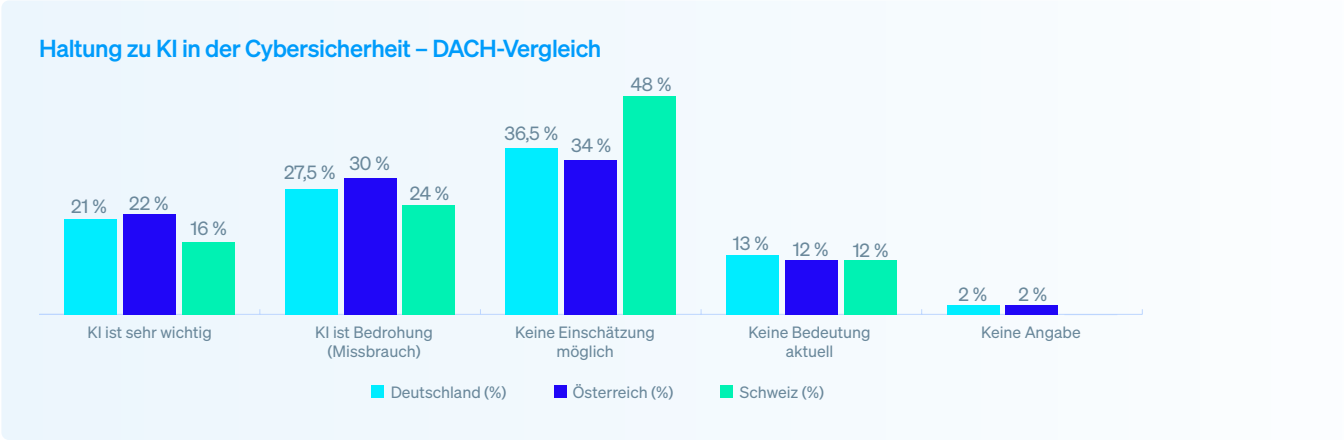
Betroffenheit: Über 60 Prozent der befragten Führungskräfte in Deutschland, Österreich und der Schweiz hatten bereits direkten Kontakt mit Cybervorfällen. Ein Drittel berichtet von Vorfällen innerhalb der letzten sechs Monate.



Delegation: Gleichzeitig geben 36 bis 42 Prozent an, Cybersicherheit an andere Unternehmensebenen zu delegieren – in der Schweiz ist dieser Anteil am höchsten.



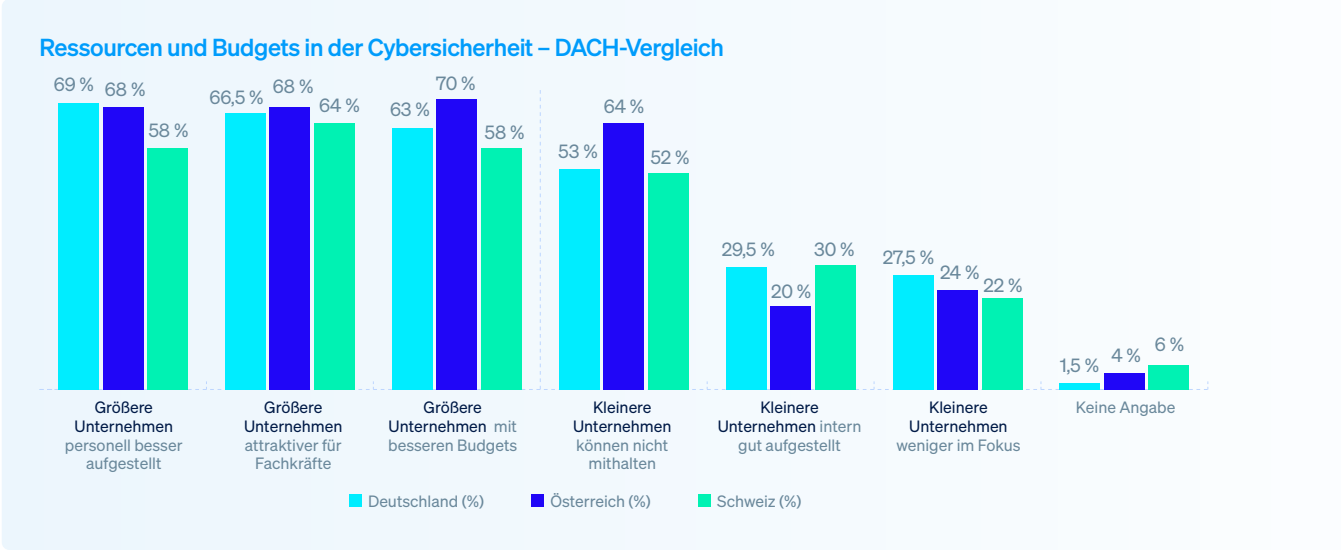
Rund die Hälfte der Führungskräfte hat Schutzmaßnahmen verstärkt, nachdem Medienberichte über staatliche Cyberangriffe Druck erzeugten. In Österreich hat mehr als ein Drittel auch die Anforderungen an Partner verschärft.



Künstliche Intelligenz: Nur 16 bis 22 Prozent betrachten KI heute als relevantes Abwehrinstrument. Etwa die Hälfte kann die Auswirkungen nicht einschätzen. Auch mit Blick auf die kommenden fünf bis zehn Jahre überwiegt Zurückhaltung.

„Künstliche Intelligenz verändert die Spielregeln der Cybersicherheit: Sie erhöht Risiken, eröffnet aber ebenso neue Chancen. Führungskräfte, die den Einsatz von KI aktiv gestalten und Kompetenzen gezielt aufbauen, stärken die digitale Resilienz ihrer Organisation und fördern zugleich Innovation und Wettbewerbsfähigkeit. So wird KI vom Risiko zum Potenzial."

Michael Veit, Sicherheitsexperte bei Sophos



Große vs. kleine Unternehmen: 63 bis 70 Prozent sehen große Organisationen klar im Vorteil – bei Budget, Personal und Attraktivität für Fachkräfte.

Risikobereitschaft: Über 80 Prozent lehnen es ab, bewusst Sicherheitsrisiken einzugehen. Wo Maßnahmen dennoch ausgeschlagen wurden, lagen die Gründe bei Kosten (rund 10 Prozent) oder Komplexität.

2.2 Unterschiede zwischen den Branchen

Wie Führungskräfte mit diesen Herausforderungen umgehen, unterscheidet sich deutlich zwischen Handel, Produktion und Dienstleistungen. Ein Blick in die Branchen zeigt, wo spezifische Stärken und Schwachstellen liegen, und eröffnet Perspektiven für gezielte Maßnahmen.

Kapitel 3 – Die Branchen

Die Gesamtzahlen zeigen: Führungskräfte beschäftigen sich mit Cybersicherheit, jedoch häufig anlassgetrieben. Wie intensiv und auf welche Weise, unterscheidet sich zwischen den Branchen deutlich. Während im Handel knappe Margen das Denken prägen, stehen in der Produktion vernetzte Prozesse und Lieferketten im Fokus. Die Dienstleistungsbranche ist geprägt von hoher Datenverantwortung und zugleich von ausgeprägter Delegation.

> „Cybersicherheit gelingt dort am besten, wo Führung und IT gemeinsam Verantwortung übernehmen. Damit vereinen sich strategische Entscheidungen mit technischem Know-how und stärken zugleich das Vertrauen in die Organisation. Sicherheit sollte zentraler Bestandteil moderner Unternehmensführung sein."
>
> *Michael Veit, Sicherheitsexperte bei Sophos*

3.1 Der Handel – Risikoaversion und Budgetdruck

Persönliche Betroffenheit ohne strategische Konsequenz

Handels-Führungskräfte sind überdurchschnittlich häufig persönlich mit Cybervorfällen konfrontiert: in Österreich fast zwei Drittel, in der Schweiz mehr als die Hälfte, in Deutschland knapp 40 Prozent. Doch trotz dieser Nähe handeln viele erst, wenn äußere Impulse wie Schlagzeilen zusätzlichen Druck erzeugen.

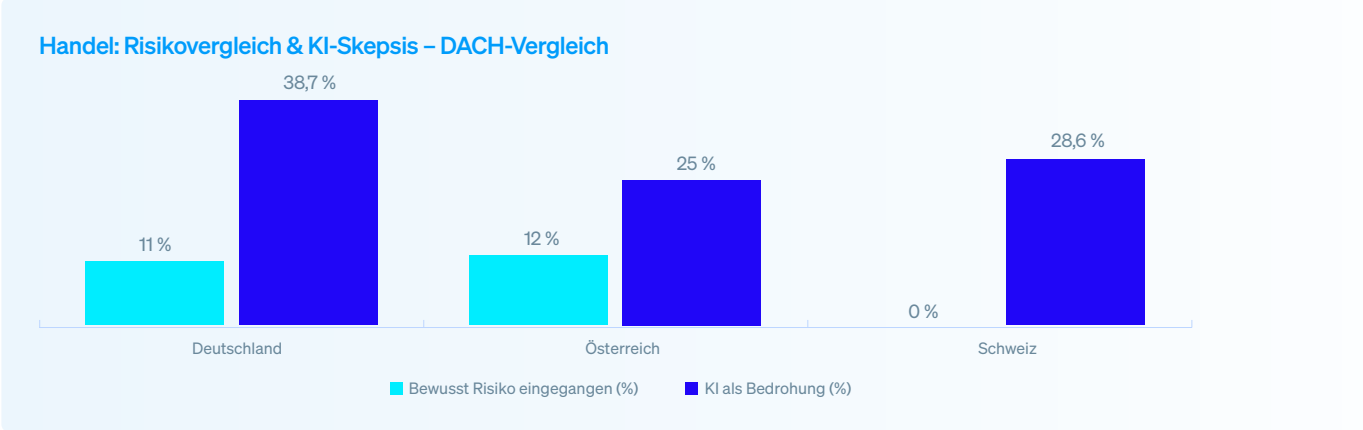
Budgethürden besonders in Österreich und der Schweiz

Kostendruck ist im Handel spürbar: In Österreich gab ein Viertel der Unternehmen an, aus Kostengründen auf die Umsetzung von Cybersicherheitsmaßnahmen verzichtet zu haben, in der Schweiz 14 Prozent. Deutschland liegt mit nur 3 Prozent deutlich darunter. Damit zeigt sich der Handel als Branche, in der knappe Margen auch die Sicherheitsstrategie limitieren.

Österreich verschärft Lieferkettenanforderungen, die Schweiz lehnt jedes Risiko ab

In Österreich haben über 60 Prozent ihre Schutzmaßnahmen erweitert, mehr als ein Drittel verschärfte die Anforderungen an Lieferanten – deutlich mehr als in Deutschland (17 Prozent) oder der Schweiz (22 Prozent).

Beim bewussten Eingehen von Risiken zeigen sich markante Unterschiede: In Deutschland räumen 11 Prozent ein, Risiken in Kauf genommen zu haben, in Österreich 12 Prozent. In der Schweiz: null. Gleichzeitig delegiert die Schweiz häufiger – etwa ein Drittel der Führungskräfte überträgt Cybersicherheit an nachgeordnete Stellen im Unternehmen.



KI: mehr Bedrohung als Chance

Im Handel überwiegt bei Künstlicher Intelligenz die Skepsis. Nur eine kleine Minderheit sieht sie als Abwehrinstrument. Viele empfinden KI als Bedrohung, hier besonders deutsche Führungskräfte, die dies zu knapp 39 Prozent bestätigen. In Österreich dominiert Unsicherheit (62,5 Prozent).

Fazit Handel: Vorsicht prägt die Branche. Österreich reagiert konsequent, Deutschland schwankt, die Schweiz zeigt höchste Risikoaversion bei gleichzeitig stärkster Delegation. KI wird kritisch bis ablehnend gesehen.

Drei Schritte für mehr Cybersicherheit im Handel

Zahlungsverkehr und Point-of-Sale-Systeme absichern:
Diese Einfallstore sind im Handel besonders kritisch.

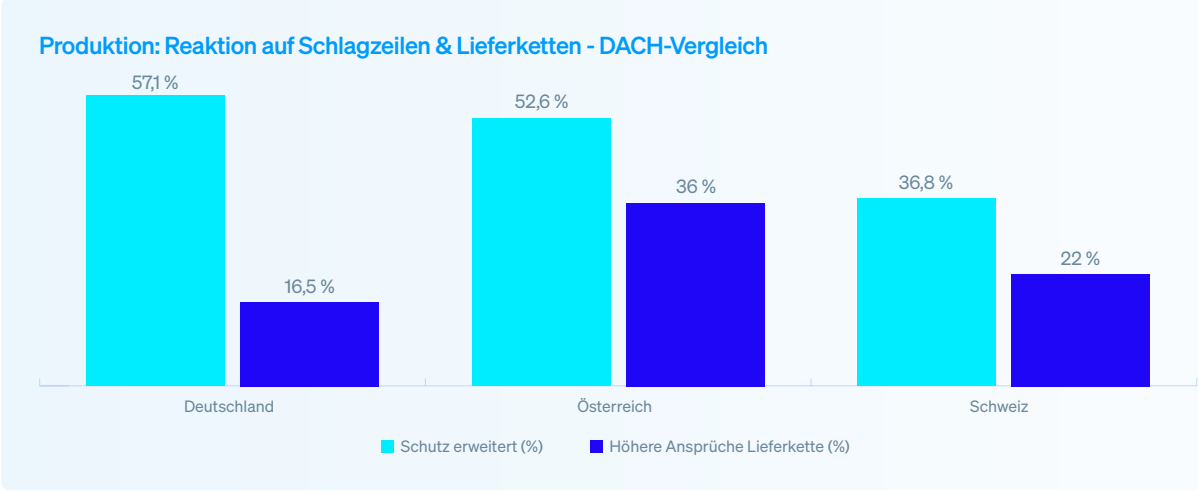
Lieferkettenstandards definieren und durchsetzen:
Partner regelmäßig überprüfen, technische Kontrollen etablieren.

Kundendaten systematisch schützen:
Identitäten absichern, E-Mail-Sicherheit stärken, bei Bedarf Detection & Response einbinden.

3.2 Produktion – Nähe zu Vorfällen und Budgetdruck

Chefs im direkten Kontakt mit Vorfällen
Produktionsbetriebe sind verwundbar: Angriffe auf Steuerungssysteme, Maschinenstillstand, unterbrochene Lieferketten. Entsprechend sind Führungskräfte überdurchschnittlich häufig persönlich involviert. In Deutschland gaben mehr als ein Drittel, in Österreich über die Hälfte der Führungskräfte an, direkten Kontakt zu Cybersicherheitsvorfällen gehabt zu haben.

Schlagzeilen über staatliche Angriffe wirken im Produktionssektor besonders stark: 57 Prozent der deutschen Betriebe justieren Schutzmaßnahmen nach, in Österreich gut die Hälfte, in der Schweiz ein gutes Drittel.



Österreich stärkt Lieferketten, Schweiz delegiert, Deutschland reagiert auf Erfahrungen
Mehr als die Hälfte der österreichischen Führungskräfte hat nicht nur intern nachgebessert, sondern auch Lieferkettenanforderungen verschärft. In Deutschland werden Maßnahmen vor allem dann angepasst, wenn das C-Level selbst mit Vorfällen konfrontiert war (rund ein Drittel). In der Schweiz berichten nur 26 Prozent von direktem Kontakt, hier delegieren 42 Prozent der Befragten die Aufgaben der Cybersicherheit an andere Ebenen im Unternehmen.

Schlagzeilen über staatliche Angriffe wirken in diesem Sektor besonders stark und haben in Deutschland den stärksten Einfluss: 57,1 Prozent der Betriebe haben hier ihre Schutzmaßnahmen nachjustiert, in Österreich sind es knapp mehr als die Hälfte und in der Schweiz ein gutes Drittel.

Verzicht auf Maßnahmen aus Geldmangel: Produktion im Branchenvergleich vorn
Rund 16 Prozent der Führungskräfte in Deutschland und Österreich gaben an, aus Kostengründen auf Maßnahmen verzichtet zu haben, in der Schweiz sind es ebenfalls knapp 16 Prozent. Damit liegt die Produktion in allen drei Ländern über dem Gesamtdurchschnitt. Komplexität spielt dagegen kaum eine Rolle: Nur 5 bis 8 Prozent nannten sie als Hindernis, in Österreich niemand.

Höhere Risikobereitschaft als andere Branchen
Auf die Frage, ob schon einmal bewusst ein Cybersicherheitsrisiko eingegangen wurde, fallen Produktionsunternehmen auf: In Deutschland gut 14 Prozent, in Österreich knapp 16 Prozent, in der Schweiz rund 10 Prozent – durchweg über dem Gesamtdurchschnitt.

KI: diffuse Einschätzungen
In Deutschland sehen nur 18 Prozent KI als wichtiges Abwehrinstrument. In Österreich überwiegt Zurückhaltung – knapp 70 Prozent halten eine künftige Schlüsselrolle für möglich, legen sich aber nicht fest. In der Schweiz zeigt sich ein fragmentiertes Bild: Gut 40 Prozent bleiben unentschlossen.

Fazit: Direkte Betroffenheit, höherer Budgetdruck und etwas mehr Risikobereitschaft als andere Branchen. Österreich agiert aktiv, Deutschland reagiert auf Erfahrungen, die Schweiz delegiert häufiger.

Drei Schritte für mehr Cybersicherheit in der Produktion

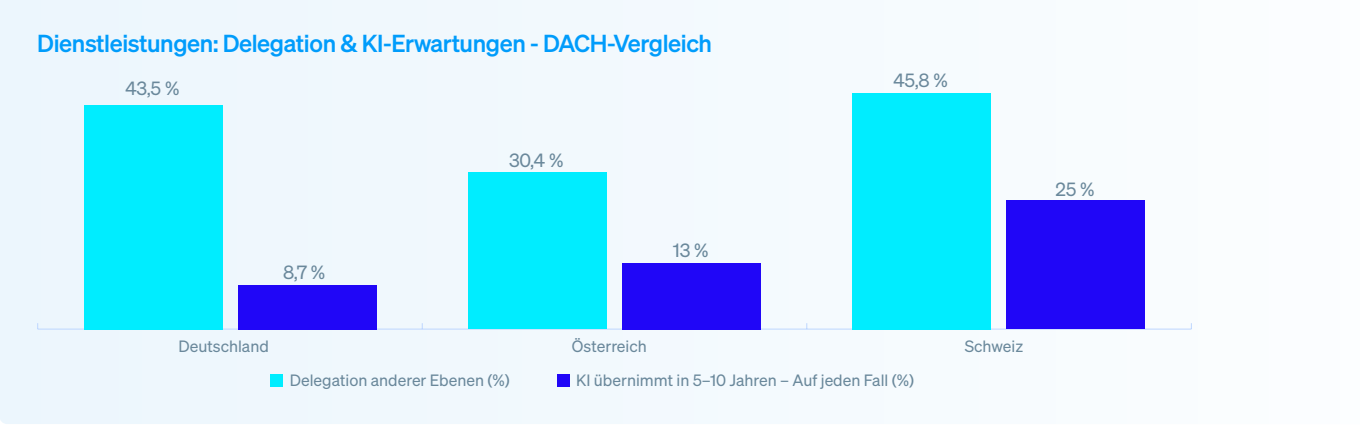
IT und OT konsequent segmentieren:
Angriffe auf Steuerungssysteme verhindern, Zugriffe nach Zero-Trust-Prinzipien steuern.

Kontinuierliche Überwachung mit klaren Playbooks:
Detection & Response etablieren, regelmäßige Übungen auf Management-Ebene durchführen.

Lieferantensicherheit vertraglich fixieren:
Einheitliche Standards durchsetzen, mit regelmäßigen Audits absichern.

3.3 Dienstleistungen – Delegation und punktueller KI-Optimismus

Verantwortung erkannt, aber am häufigsten abgegeben
Dienstleistungsunternehmen verwalten große Mengen sensibler Kundendaten – dennoch delegieren viele Führungskräfte die Cybersicherheit in andere Unternehmensebenen: In Österreich 38 Prozent, in Deutschland 44 Prozent, in der Schweiz fast 46 Prozent. Das ist der höchste Wert aller Branchen.



KI: Skepsis dominiert – mit einer Ausnahme
Deutsche und österreichische Führungskräfte zeigen sich beim Thema KI überwiegend skeptisch oder abwartend. Nur eine Minderheit misst ihr bereits heute Bedeutung bei. Die Schweiz sticht heraus: Ein Viertel der Befragten hält es für wahrscheinlich, dass KI in den kommenden fünf bis zehn Jahren zentrale Aufgaben übernehmen könnte. Damit sind Dienstleistungsunternehmen die einzige Branche mit einer nennenswerten Gruppe von Befürwortern – auch wenn die Mehrheit weiterhin abwartend bleibt.

Österreich zeigt hohe Aktivität, Deutschland und die Schweiz bleiben zurückhaltend
Zwei Drittel der österreichischen Manager im Dienstleistungssektor haben Schutzmaßnahmen erweitert, fast 40 Prozent die Anforderungen an Partner verschärft. Deutschland und die Schweiz agieren deutlich verhaltener: In Deutschland haben nur rund ein Drittel zusätzliche Maßnahmen ergriffen, in der Schweiz noch weniger.

Fazit: Starke Delegation, in Österreich aber auch Vorreiterrolle bei Maßnahmen. In der Schweiz unerwarteter KI-Optimismus – ein Kontrast zu Deutschland, wo Zurückhaltung dominiert.

Drei Schritte für mehr Cybersicherheit im Dienstleistungssektor

Cybersicherheit im C-Level verankern:
Nicht allein Fachabteilungen überlassen – strategische Steuerung von oben.

Datenschutz als Vertrauensanker:
Identitätsschutz, Verschlüsselung und Schutz vor Datenabfluss systematisch ausbauen.

KI schrittweise erproben:
Pilotprojekte aufsetzen, Leitplanken definieren, Erkenntnisse in Prozesse überführen.

Kapitel 4 – Branchenvergleich

4.1 Cybersicherheit in Handel, Produktion und Dienstleistungen

Drei Branchen, drei Sicherheitskulturen
Handel, Produktion und Dienstleistungen unterscheiden sich spürbar in ihrem Umgang mit Cybersicherheit. Im Handel dominieren knappe Margen und Risikoabwägungen, in der Produktion die Abhängigkeit von Prozessen und Lieferketten. Dienstleister wiederum richten den Blick auf den Schutz sensibler Daten und regulatorische Vorgaben. Diese branchenspezifische Logik beeinflusst unter anderem, wie stark sich Führungskräfte persönlich einbringen – oder Verantwortung delegieren.

> „Jede Branche hat ihre eigene Sicherheitslogik, von Budgets und Vorfallerfahrung in der Produktion über Delegation im Dienstleistungssektor bis hin zum vorsichtigen Selbstvertrauen im Handel. Für Cybersicherheit gibt es keine Blaupause. Jede Branche braucht ihre eigene Strategie."
>
> *Michael Veit, Sicherheitsexperte bei Sophos*

Wie Führungskräfte konkret reagieren
Die Zahlen aus den vorangegangenen Kapiteln zeichnen ein klares Gesamtbild. Doch der konkrete Umgang mit Cyberrisiken unterscheidet sich fundamental – je nachdem, ob Führungskräfte im Handel, in der Produktion oder im Dienstleistungssektor tätig sind.

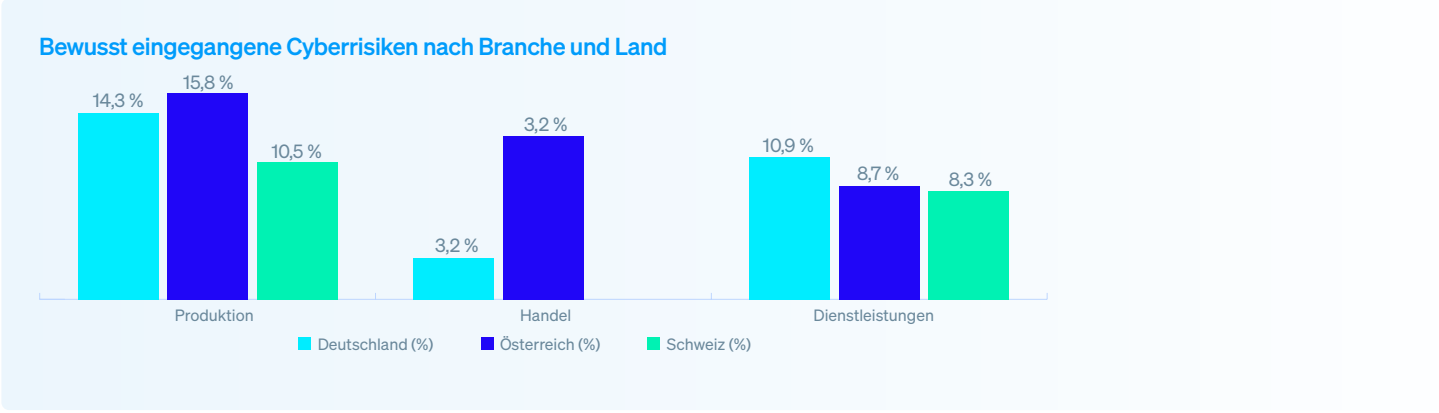
Handel: Vorsicht dominiert
Im Handel regiert die Risikoaversion. Knappe Margen lassen keinen Raum für Experimente. Diese Vorsicht prägt auch den Umgang mit neuen Technologien: Bei KI überwiegt deutliche Skepsis, Abwarten statt Ausprobieren. Zudem wird der strukturelle Nachteil kleinerer Unternehmen hier besonders stark wahrgenommen – vor allem in Österreich und der Schweiz, wo Budgethürden konkret genannt werden.

Produktion: Bedrohung der Kernprozesse holt Chefs ins Boot
In Produktionsbetrieben sind Cyberbedrohungen greifbar: Angriffe treffen Steuerungssysteme, stoppen Maschinen, unterbrechen Lieferketten. Entsprechend sind Führungskräfte persönlich involviert – besonders in Österreich und der Schweiz berichten sie überdurchschnittlich häufig von direktem Kontakt mit Vorfällen.

Diese Nähe zeigt sich auch in der Risikokultur: Produktionsunternehmen geben etwas häufiger an, bewusst Risiken eingegangen zu sein, etwa, um Prozesse nicht zu verzögern. Gleichzeitig nennen rund 16 Prozent Budgetgründe als Hindernis – mehr als in anderen Branchen. Pragmatismus überwiegt: Externe Unterstützung wird als realistische Option gesehen.

Dienstleistungen: Delegation und punktueller Optimismus
Im Dienstleistungssektor wird Cybersicherheit systematischer aus dem C-Level in Fachabteilungen ausgelagert: In Deutschland bei 44 Prozent der Befragten, in der Schweiz bei fast der Hälfte. Führungskräfte berichten hier seltener von direktem Kontakt mit Vorfällen als in den anderen Branchen.

Eine Überraschung: Während Handel und Produktion bei KI skeptisch bleiben, zeigt sich im Dienstleistungssektor – vor allem in der Schweiz – vereinzelter Optimismus. Ein Viertel der dortigen Führungskräfte erwartet, dass KI in fünf bis zehn Jahren zentrale Sicherheitsaufgaben übernehmen könnte.



Kapitel 5 – Handlungsempfehlungen: von Reaktion zu Resilienz

Cybersicherheit steht auf der Management-Agenda – wird jedoch noch zu oft reaktiv behandelt und häufig delegiert, insbesondere im Dienstleistungssektor. Budgetdruck prägt besonders die Produktion, und beim Thema Künstliche Intelligenz zeigen sich Unsicherheit und Nachholbedarf. Diese branchenspezifischen Muster eröffnen drei zentrale Handlungsfelder für die Führungsebene:

5.1 Verantwortung auf Vorstandsebene sichtbar verankern

In allen Branchen delegieren rund 36 bis 46 Prozent der Führungskräfte Cybersicherheit an andere Unternehmensbereiche. Klarheit über Zuständigkeiten und regelmäßige Berichterstattung an die Geschäftsführung sind entscheidend, um das Thema strategisch zu steuern. Ohne diese Verankerung bleibt Cybersicherheit überwiegend operativ und reaktiv.

Branchenspezifisch:

- Handel: Direkter Zugang zur Vorfalls- und Risikoübersicht schafft Transparenz.
- Produktion: Die bereits hohe Führungseinbindung durch strukturierte Incident-Reviews festigen.
- Dienstleistungen: Delegation anerkennen, jedoch klares Eskalations- und Berichtswesen etablieren.

5.2 Strukturelle Ungleichheiten aktiv adressieren

Große Unternehmen profitieren bei Budget, Personal und Fachkräfteattraktivität, während KMU sich oft benachteiligt fühlen – besonders im Handel. Managed Security Services, cloudbasierte Lösungen und Wissenstransfer sind Schlüssel, um diese Lücke zu schließen. Ein kooperatives Sicherheitsökosystem fördert die Sicherheit aller Beteiligten.

Branchenspezifisch:

- Handel: Gemeinsame Branchenstandards und Initiativen stärken kleinere Akteure, besonders in Österreich und der Schweiz.
- Produktion: Große Betriebe sollten Zulieferer mit klaren Sicherheitsanforderungen unterstützen.
- Dienstleistungen: Externe Partner als aktive strategische Ressourcen einbinden, nicht nur reaktiv.

5.3 Orientierung im Umgang mit Künstlicher Intelligenz schaffen

KI polarisiert in den Führungsetagen: Skepsis dominiert, aber punktuell besteht Optimismus – vor allem in der Schweizer Dienstleistungsbranche. Schrittweise Kompetenzentwicklung durch Pilotprojekte, gezielte Briefings und klare Leitplanken helfen, Chancen strukturiert zu nutzen und Risiken zu steuern.

Branchenspezifisch:

- Handel: Low-Risk-Anwendungen wie Anomalieerkennung im Zahlungsverkehr vorsichtig testen.
- Produktion: KI-Überwachung von OT-Umgebungen mit fundierter Risikoabwägung prüfen.
- Dienstleistungen: Sieger nutzen den Optimismus durch strukturierte Pilotprojekte und Erfolgskriterien.

Konkrete, branchenübergreifende Maßnahmen zum Start

Kurzfristig (0–3 Monate):

- Risikoanalyse auf Managementebene durchführen
- Quick Wins umsetzen: MFA, gehärtete Admin-Accounts, Backup-Tests
- Erste Tabletop-Übung mit Vorstand und CISO durchführen

Mittelfristig (3–12 Monate):

- Mehrjährige Roadmap verabschieden
- Mindeststandards für Lieferanten definieren
- Erstes KI-Pilotprojekt starten (falls relevant)
- Regelmäßige Reviews im Vorstandskalender festschreiben

Diese Empfehlungen unterstützen Führungskräfte dabei, Cybersicherheit fest in der Organisation zu verankern, strukturelle Herausforderungen zu meistern und neue Technologien sicher und zielgerichtet zu integrieren. So entsteht aus einer reaktiven Pflicht eine strategische Chance für nachhaltigen Unternehmenserfolg.

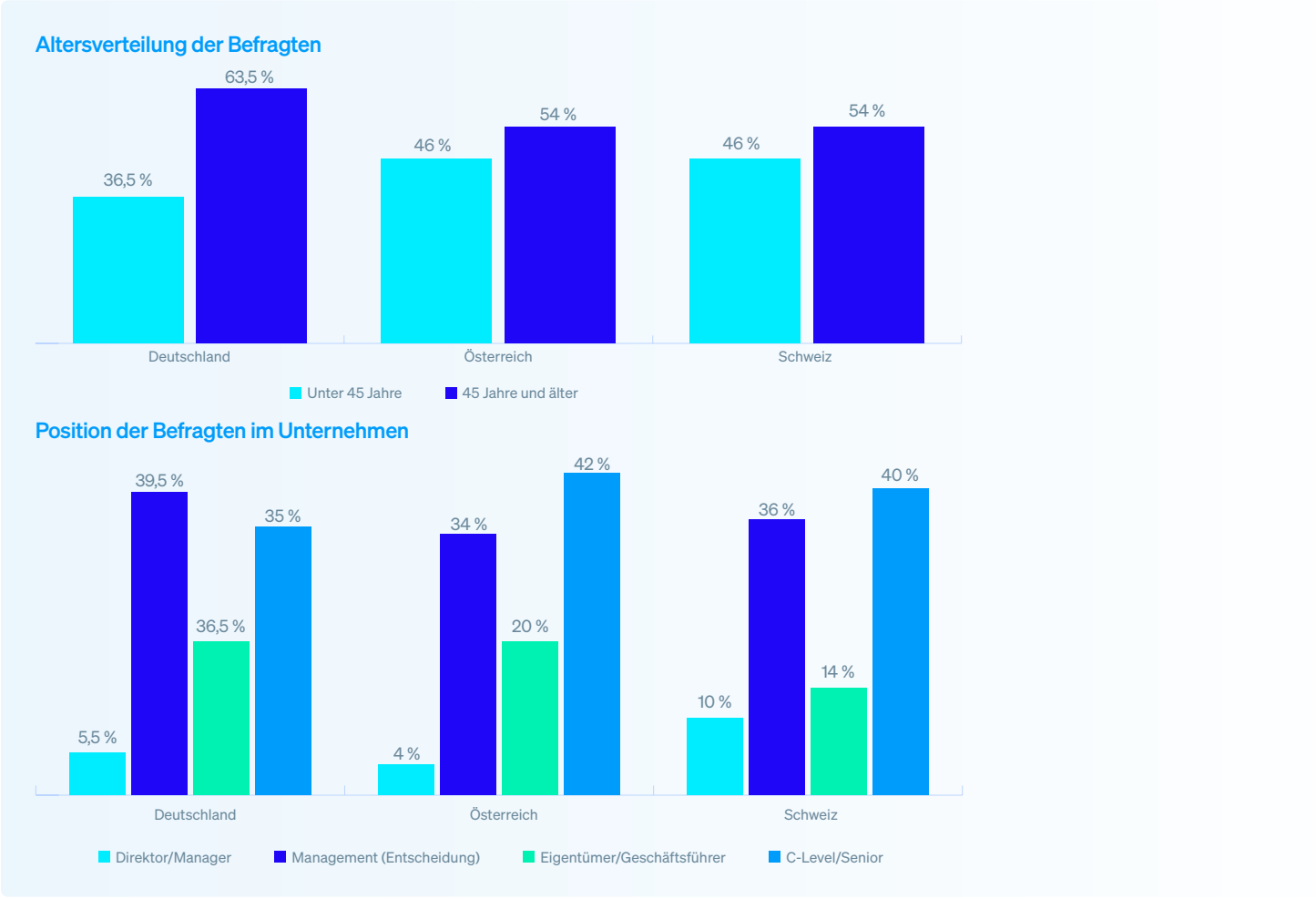
„Cybersicherheit ist heute weit mehr als eine technische Frage – sie ist ein Ausdruck vorausschauender Führung. Auf C-Level eröffnet sie die Möglichkeit, Strategien nachhaltig zu verankern, den bewussten Umgang mit neuen Technologien zu fördern und so nicht nur Schutz, sondern auch Vertrauen zu schaffen. Auf diese Weise wird Cybersicherheit auch zu einem Motor für Resilienz, Wettbewerbsfähigkeit und Zukunftsfähigkeit."

Michael Veit, Sicherheitsexperte bei Sophos

Über die Studie

Die Studie basiert auf einer ausgewogenen Mischung aus 300 mittelgroßen und größeren Unternehmen. In Deutschland nahmen 200 Führungskräfte teil – davon 150 aus Unternehmen mit 50 bis 199 Mitarbeitenden und 50 aus Organisationen mit mehr als 200 Beschäftigten. In Österreich setzten sich die 50 Befragten aus 36 mittelgroßen und 14 größeren Unternehmen zusammen. Für die Schweiz gaben 33 Führungskräfte aus Unternehmen mit 50 bis 199 Mitarbeitenden und 17 aus Betrieben mit 200 und mehr Beschäftigten Auskunft. Die Stichprobe setzt sich ausschließlich aus Personen des C-Levels, der Geschäftsführung und des oberen Managements zusammen.

Altersverteilung und Rollen im Unternehmen:



Bereit, Ihr Cybersicherheits-programm zu bewerten?

Sprechen Sie noch heute mit einem Sophos-Experten.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel: +49 611 5858 0
E-Mail: sales@sophos.de

2025-11-04 WP (NP)

SOPHOS