Deloitte.

Global Future of Cyber Survey 2024

Cyber-Potenziale im DACH-Raum

MAKING AN IMPACT THAT MATTERS since 1845

Wie denken Top-Führungskräfte über Strategien, Wertpotenziale und Prioritäten rund um Cyber Security in ihren Organisationen? Darüber informiert der neue Global Future of Cyber Survey 2024. In dieser Analyse werden die Ergebnisse für Deutschland, Österreich und die Schweiz ausgewertet. Im Vergleich zum weltweiten Survey ergibt sich ein ähnliches Bild, doch in einigen Punkten sind DACH-Unternehmen weiter als ihre globalen Peers, etwa bei der Zunahme der Cyber-Investitionen.

Cyber Security wird heutzutage längst nicht mehr als reines IT-Thema betrachtet. IT-Sicherheit und Datenschutz haben im Zeitalter digitaler Geschäftsmodelle und datengetriebener Transformationen zentrale strategische Bedeutung. Wie schätzen Unternehmen das Potenzial von Cyber Security ein, welche Strategien verfolgen sie bei der Technologie-Implementierung, und wie entwickelt sich die Rolle der Führungsebene? Diese und viele weitere Fragen beantwortet Deloittes Global Future of Cyber Survey. Für die vierte Ausgabe wurden knapp 1200 Führungskräfte aus 43 Ländern befragt, davon 101 aus DACH-Ländern. Alle Befragten sind in Unternehmen tätig, die mehr als 1000 Angestellte und 500 Mio. USD Umsatz aufweisen. Zusätzlich wurden Interviews mit ausgewiesenen Expert:innen und Praktiker:innen aus dem Cyberfeld geführt.

Als Ergänzung zum globalen Survey wollen wir in dieser Analyse Gemeinsamkeiten und Unterschiede zwischen den globalen und den DACH-Ergebnissen aufzeigen, in Bereichen wie Maßnahmen, Strategie und Wertbeitrag, der Rolle der Chief Information Security Officers (CISOs), der Cyberaffinität der Führungsebene sowie der Bedeutung von Cyber Security für die technologische und geschäftliche Transformation. Manche Abweichungen der DACH-Auswertung dürften mit den strukturellen Besonderheiten dieses Wirtschaftsraums zusammenhängen, etwa die höhere Bedeutung von Cyber Security im Kontext der Industrierobotik. Darüber hinaus ist aber auch festzuhalten, dass Cyberstrategien und -aktivitäten der DACH-Unternehmen generell in vielen Bereichen ausgeprägter sind als in globaler Sicht, teilweise deutlich. Im Folgenden werden zunächst die globalen Ergebnisse knapp zusammengefasst, um dann die Besonderheiten des DACH-Raums ausführlicher herauszuarbeiten.

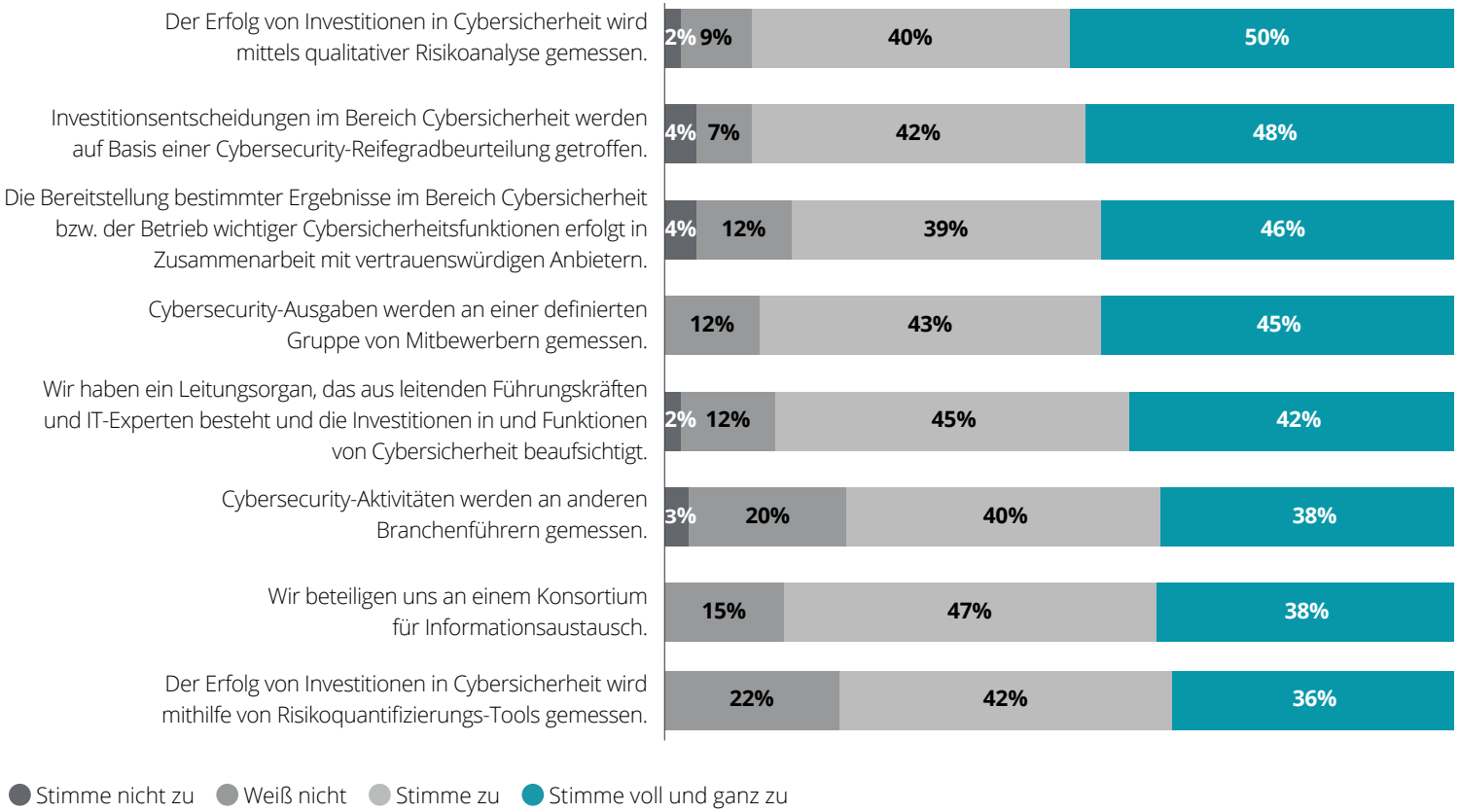
DIE STRATEGISCHE BEDEUTUNG VON CYBER SECURITY NIMMT ZU

Die zunehmende Konzentration auf Impact und Wertbeitrag der Cyber Security war schon in der letzten Ausgabe des globalen Survey zu beobachten (2023). Die jüngste Ausgabe bestätigt diesen Trend und zeigt darüber hinaus auf, dass Cyber Security nun verstärkt auch in die technologischen sowie geschäftlichen Transformationen integriert wird und diese aufwertet. Die Bedeutung der Cyberführungskräfte in den Organisationen nimmt ebenfalls zu. Strategisch denkende CISOs haben wachsenden Einfluss und beteiligen sich verstärkt an Diskussionen zu Technologie-Investitionen. Durch gezielte Strategien erhöhen Unternehmen ihren Cyberreifegrad, was mehr Resilienz und bessere Compliance schafft, aber auch eine bessere Bewältigung der wachsenden betrieblichen Komplexität und des permanenten Wandels im aktuellen Umfeld erlaubt. Vor diesem Hintergrund überrascht es etwas, dass nur 52 Prozent aller weltweit Befragten die Cyberfähigkeiten von Aufsichtsrat und Vorstand mit hoher Überzeugung als adäquat einschätzen. Bei Organisationen mit überdurchschnittlichem Cyberreifegrad sind es dagegen 82 Prozent.

CYBERTRENDS IM DACH-RAUM: ANSÄTZE UND INVESTITIONEN

Die enorme Wichtigkeit von Cyber Security in der vernetzten digitalen Welt von heute wird von den Unternehmen klar erkannt. Die große Mehrheit der Befragten berichtet von mittel bis stark ausgeprägten Maßnahmen ihrer Organisation in diesem Feld. Das gilt global ebenso wie in DACH-Sicht, allenfalls in der Priorisierung ergeben sich leichte Abweichungen. Während global gesehen die Etablierung von strategischen und operativen Cyberplänen an erster Stelle der implementierten Maßnahmen steht, rangiert dieser Punkt im DACH-Raum erst auf Platz drei. Noch wichtiger sind für DACH-Organisationen bei den in großem Umfang umgesetzten Maßnahmen die Punkte Schutz von Kundenidentitäten durch Zugriffskontrollen und Identitätsmanagement (Platz eins) sowie Softwarekomponenten-Inventare (Platz zwei). Auf Platz vier folgt der Punkt Erhebung und Nutzung von Kundenpräferenzen zu Cyber Security und Datenschutz.

Die Cybersicherheitsstrategien der Unternehmen (n=101) (Abbildung 1)
F2. Bitte bewerten Sie, inwieweit die folgenden Aussagen Teil der Cybersicherheitsstrategie Ihres Unternehmens sind.



Hinweis: Die angegebenen Prozentwerte ergeben in der Summe nicht immer exakt 100%. Diese Ungenauigkeit resultiert aus dem Runden auf ganze Zahlen.

In der Studie wurde außerdem nach den implementierten Cyberstrategien gefragt, wobei sich interessante Unterschiede ergeben

Diese Strategien werden in DACH-Unternehmen zum Teil intensiver verfolgt. An erster Stelle der Strategien steht für sie die qualitative Risikoabschätzung zur Messung des Wertbeitrags von Cyber-Investments. 50 Prozent der DACH-Unternehmen geben hierbei ein hohes Engagement an, global sind es nur 39 Prozent. Es folgen Cyber-Security-Reifegrad-Assessments als Grundlage für Cyberinvestitions-entscheidungen (DACH: 48 Prozent, global: 39 Prozent) und Kooperationen mit Providern etwa im operativen Cyberbereich (DACH: 46 Prozent, global: 39 Prozent).

Auch beim finanziellen Einsatz sind die DACH-Unternehmen aktiver als der globale Schnitt. 67 Prozent prognostizieren eine Zunahme ihrer Cyberinvestitionen in den nächsten ein bis zwei Jahren (global: 57 Prozent). Im Schnitt betragen die IT-Budgets im DACH-Raum jährlich 171 Mio. bis 267 Mio. USD, was wenig von den globalen Werten abweicht (147 Mio. bis 266 Mio. USD). Davon werden lokal wie global 19 Prozent für Cyber Security aufgewendet. Beim Umfang des erwarteten Zuwachses der Cyberbudgets liegen DACH-Unternehmen mit 5 Prozent aber erneut vor den globalen Peers (3 Prozent).

Bei Investitionen sind DACH-Unternehmen aktiver als der globale Schnitt.

VIELFÄLTIGE CYBERANGRIFFE, GESCHÄFTSVORTEILE DURCH MEHR SICHERHEIT

Die Cyberbedrohungen sind zahlreich, werden immer raffinierter und unterliegen einer kontinuierlichen Weiterentwicklung. Lokal wie global werden von den Befragten insbesondere Cyberkriminelle und -terroristen als die bedrohlichste Tätergruppe genannt. Bei der als am bedrohlichsten eingeschätzten Angriffsmethode stehen für DACH-Unternehmen Attacken auf Platz eins, die auf Datenverlust zielen (34 Prozent, global: 28 Prozent), während global Phishing, Ransomware und Malware als bedrohlichste Angriffsart genannt werden (34 Prozent, DACH: 33 Prozent). Bei den Cyber Incidents ist der DACH-Raum teils etwas stärker exponiert: 44 Prozent der Unternehmen haben hier im letzten Jahr sechs bis zehn Cybervorfälle öffentlich bekannt gemacht (global: 40 Prozent). Aufschlussreich sind daneben die Aussagen zu den negativen Konsequenzen vergangener Cybervorfälle. Global wie im DACH-Raum steht der Vertrauensverlust in die Integrität von Technologien an erster Stelle. Dieser Aspekt legt gegenüber der Erhebung von 2023 zu, was die strategische Bedeutung von Cyber Security für die Unternehmen im Kontext der voranschreitenden digitalen Transformation unterstreicht. In der globalen Auswertung 2024 folgen auf Rang zwei und drei dann allerdings operative Disruption und Reputationsschäden, im DACH-Raum Umsatzeinbußen und Kursverluste der Aktie.

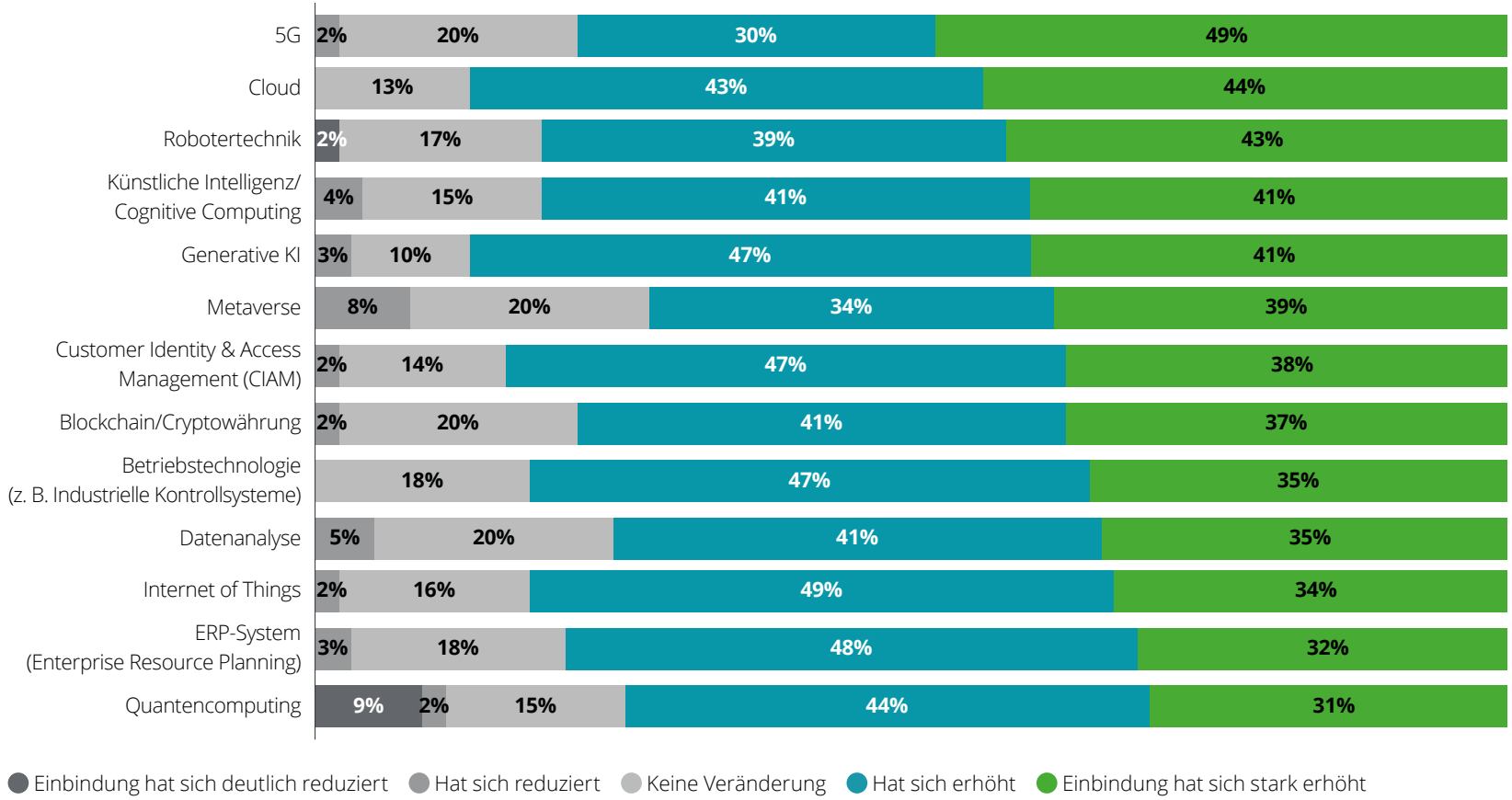
Unterschiede zeigt außerdem die Einschätzung der Befragten zu den geschäftlichen Vorteilen, die sie sich von Cyberinitiativen versprechen. Einen umfangreichen Business-Benefit durch Cyber Security erwarten die Befragten aus dem DACH-Raum am häufigsten für das Erreichen der Unternehmensmission („Purpose“, 54 Prozent), gefolgt von Umsatzwachstum (51 Prozent), mehr Resilienz (49 Prozent) sowie erhöhter Effizienz und Agilität (48 Prozent). Global sind die am häufigsten genannten Benefits der Schutz geistigen Eigentums (46 Prozent), verbesserte Detection- und Response-Prozesse (44 Prozent), erhöhte Effizienz und Agilität (44 Prozent) sowie bessere Kundenerfahrung (43 Prozent).

Bei den Risiken steht der Vertrauensverlust in die Integrität von Technologien an erster Stelle.

DER EINFLUSS VON CISOS UND FÜHRUNGSGREMIEN

In den Unternehmen der Teilnehmer:innen tragen häufig CISOs die Hauptverantwortung für Cyberaktivitäten, doch auch Chief Information Officers (CIOs) nehmen diese Rolle in vielen Fällen ein. Die meisten CISOs bzw. Cyberleiter:innen berichten an die CIOs, vor allem im DACH-Raum: Hier liegt der Wert mit 41 Prozent deutlich höher als im globalen Durchschnitt (27 Prozent). Entsprechend der wachsenden Bedeutung der CISO-Rolle berichten viele CISOs bzw. Cyberleiter:innen auch direkt an die CEOs. Im DACH-Raum ist das allerdings mit 15 Prozent etwas weniger ausgeprägt als global (20 Prozent).

Einbindung des CISO/Verantwortlichen für Cybersicherheit in Strategiegespräche über technische Fähigkeiten (Abbildung 2)
F26. Inwieweit hat sich die Einbindung Ihres CISO (bzw. Verantwortlichen für Cybersicherheit) in Strategiegespräche in Bezug auf die folgenden technischen Fähigkeiten im vergangenen Jahr verändert?



Ein weiterer wichtiger Trend aus dem Survey 2024 bestätigt den wachsenden Einfluss von CISOs bzw. Cyberleiter:innen

Sie beteiligen sich zunehmend an strategischen Diskussionen rund um geschäftskritische Technologie-Investitionen. Dabei ist festzuhalten, dass diese Entwicklung im DACH-Raum insgesamt stärker ausfällt als global. Das Feld, bei dem die Beteiligung von CISOs im DACH-Raum am deutlichsten zunimmt, ist der Bereich 5G mit einer signifikanten Zunahme bei 49 Prozent der Befragten (global: 33 Prozent). Global ist das prominenteste Feld für vermehrte CISO-Beteiligung der Bereich Cloud mit deutlich niedrigeren 34 Prozent (DACH: Platz 2, 44 Prozent). An dritter Stelle steht im DACH-Raum die Industrierobotik (43 Prozent) global: (Platz 13, 27 Prozent). Der im Vergleich mit dem globalen Survey höhere Wert könnte damit zusammenhängen, dass im DACH-Raum Technologieprogramme rund um Industrie 4.0 besonders hohen Stellenwert haben. Es folgen künstliche Intelligenz (KI) und generative KI (GenAI, beide 41 Prozent, global: beide 34 Prozent) sowie das Metaverse (39 Prozent, global: 28 Prozent, Platz 12).

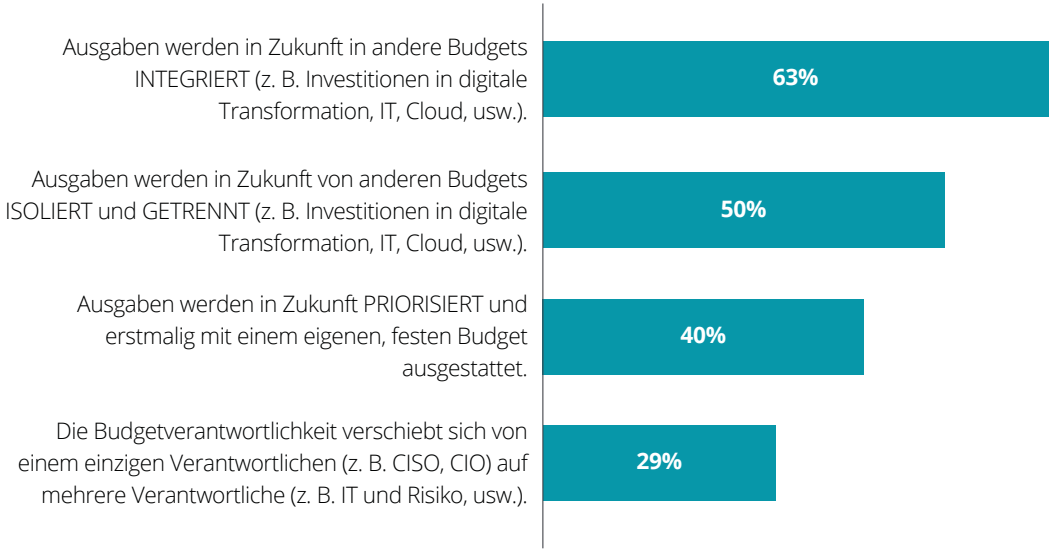
Etwas positiver als im globalen Durchschnitt ist es laut Einschätzung der DACH-Unternehmen auch um die Cyberfähigkeiten von Vorstand und Aufsichtsrat bestellt. Die Befragten betrachten sie zu 56 Prozent mit hoher Überzeugung als adäquat (global: 52 Prozent). Einen Vorsprung verzeichnen die DACH-Unternehmen darüber hinaus bei der Regelmäßigkeit der Thematisierung von Cyberthemen in den Gremien. Während diese sich im globalen Schnitt zu 88 Prozent mindestens einmal im Quartal mit Cyber Security befassen, sind es im DACH-Raum 96 Prozent.

CYBERIMPLIKATIONEN FÜR TECHNOLOGIE-PROGRAMME UND DIGITALE BUSINESS-TRANSFORMATIONEN

Die Grenzen der Cyber Security als Unternehmensbereich verschwimmen zunehmend. Wenn Organisationen verstärkt Daten und Systeme mit Partnerunternehmen und Drittparteien teilen, erhalten Datenschutz und IT-Sicherheit viel größere Bedeutung. Auch digitale Businesstransformationen können ihren Wachstumsbeitrag letztlich nur dann entfalten, wenn eine entsprechende Cyberstrategie das Fundament dafür liefert. Die Unternehmen reagieren darauf, indem sie Cyber Security zunehmend in Business- und Technologiebereiche integrieren. Dies haben die DACH-Unternehmen insgesamt etwas häufiger in großem Umfang umgesetzt als die globalen Peers. An erster Stelle steht hier global wie lokal die Berücksichtigung von Datenschutz schon bei der Entwicklung von Produkten und Services (DACH: 45 Prozent, global: 40 Prozent). Im DACH-Raum folgen die Priorisierung ethischer Aspekte bei der Cyberstrategie (42 Prozent, global: 37 Prozent, Platz fünf) und die Umsetzung von Datenschutz im Hinblick auf Kundennutzen und Wertbeitrag (42 Prozent, global: 39 Prozent, Platz drei).

Die zunehmende Integration von Cyber Security in die diversen Businessdimensionen zeigt sich auch bei der Finanzierung von Cyberausgaben. In vielen Unternehmen werden Cyberinvestitionen verstärkt in andere Budgets integriert (etwa Budgets für IT, Cloud oder digitale Transformation). Erneut liegt bei diesem Trend der DACH-Raum etwas vor dem globalen Durchschnitt (DACH: 63 Prozent, global: 58 Prozent). Sehr verbreitet ist zugleich allerdings auch die Beibehaltung von separaten Budgets (DACH: 50 Prozent, global: 55 Prozent). Manche Teilnehmer:innen wählten bei dieser Frage beide Antworten aus, was darauf hindeutet, dass teilweise in ein und demselben Unternehmen gemischte Finanzierungsstrategien verfolgt werden. Wie der globale Survey vermerkt, ist die Integration von Cyberinvestitionen in relevante andere Budgets grundsätzlich empfehlenswert, da dieser Ansatz zu einer umfassenderen Cyberstrategie und zu besseren Ergebnissen bei der Umsetzung führen kann. Dies kann allerdings auch dazu führen, dass der spezifische Wertbeitrag von Cyber Security nicht mehr gesehen wird – ein Risiko, das Verantwortliche im Auge behalten sollten.

Auswirkungen einer sich wandelnden digitalen Landschaft auf die Ausgaben für Cybersicherheit (Abbildung 3)
F14. Wie wird sich die wandelnde digitale Landschaft auf die Cybersecurity-Ausgaben Ihres Unternehmens auswirken?



CYBER SECURITY ALS TECHNOLOGIE-ENABLER

Cyber Security spielt außerdem eine wachsende Rolle bei der Sicherstellung von wesentlichen Technologiefähigkeiten in den Organisationen. In DACH-Unternehmen sind die drei wichtigsten Bereiche, bei denen Cyber Security in großem Umfang dazu beiträgt, Cloud-Technologie (50 Prozent, global: 48 Prozent), Industrierobotik (50 Prozent, global: 30 Prozent) und Enterprise-Resource-Planning-Systeme (ERP, 45 Prozent, global: 36 Prozent). Im globalen Schnitt haben Robotik und ERP somit eine wesentlich geringere Bedeutung in der Rangliste der Technologien, deren Implementierung durch Cyber Security wesentlich vorangebracht wird. Deutlich höher rangiert dort dafür GenAI (41 Prozent, Platz 2, DACH: 33 Prozent, Platz 12). Bei der Bedeutung von Cyber Security für Investitionen in das Internet of Things liegt der DACH-Raum leicht vorn (IoT, DACH: 43 Prozent, global: 39 Prozent), bei Data Analytics minimal (DACH: 43 Prozent, global: 41 Prozent).

Cloud-Technologie ist derzeit ein besonders wichtiges Technologiefeld für die Unternehmen. Es hat jedoch teilweise die Kehrseite einer erhöhten Komplexität. Um diese zu reduzieren, wird in vielen Organisationen auch zu Cyberaktivitäten gegriffen.

Im DACH-Raum sind die beiden häufigste Cybermaßnahmen zur Komplexitätsreduktion von Cloud-Ökoystemen die Optionen Identitäts- und Zugangskontrollen (45 Prozent) und Security-Automatisierung (43 Prozent); global die Punkte lösungsübergreifendes Cloud-Ökosystem-Monitoring (46 Prozent) und konsistente Security-Prozesse (45 Prozent).

Unternehmen sehen sich aktuell zudem mit einer wachsenden Bedrohung durch KI-gestützte Cyberangriffsvektoren konfrontiert. Zugleich ermöglichen KI-gestützte Cyberlösungen aber auch eine schlagkräftigere Abwehr. In großem Umfang nutzen 48 Prozent der DACH-Unternehmen KI für das Security-bezogene Monitoring digitaler Infrastruktur (global: 42 Prozent), 47 Prozent für Realtime-Security-Datenanalysen (global: 39 Prozent) und 46 Prozent für die automatisierte Security Response (global: 38 Prozent). Insgesamt nutzen mit 43 Prozent etwas mehr DACH-Unternehmen KI in großem Umfang für die Cyberabwehr als der globale Durchschnitt (39 Prozent). Neue Cybergefahren drohen außerdem durch Quantentechnologie, mit der kriminelle Akteure beispielsweise kryptografische Verfahren aushebeln können. Nicht alle Unternehmen sind schon darauf vorbereitet. Im DACH-Raum implementieren aber immerhin 27 Prozent der Organisationen Lösungen im größeren Maßstab oder zumindest im Betastadium (global: 30 Prozent).

DIE ZUKUNFT DER CYBER SECURITY

Zunehmende Integration von Cyber Security in Businessbereiche und Technologie-Implementierung, wachsender Einfluss der CISOs und Zuwachs der Investitionen: Diese Analyse zeigt, dass diese global dominierenden Trends auch im DACH-Raum die aktuelle Entwicklung und die mittelfristige Perspektive prägen. In einigen Dimensionen sind DACH-Organisationen dabei aber merklich weiter fortgeschritten als der globale Durchschnitt. Für weitere Details und Ergebnisse verweisen wir auf die globale Auswertung, etwa im Hinblick auf den Einfluss des Cyberreifegrads auf den erwarteten Wertbeitrag von Cybermaßnahmen. Dort finden Sie außerdem übergreifende Handlungsempfehlungen für die strategische Erhöhung des Cyberreifegrads in der Organisation.

Ihre Kontakte

Marius von Spreti
Partner
Risk Advisory
Tel: +49 89 29036 5999
mvonspreti@deloitte.de

Volker Burgers
Partner
Risk Advisory
Tel: +49 211 8772 3200
vburgers@deloitte.de

Georg Schwondra
Partner
Risk Advisory
Tel: +43 1 537 00 3760
gschwondra@deloitte.at

Klaus Julisch
Managing Partner
Risk Advisory
Tel: +41 58 279 6231
kjulisch@deloitte.ch

Deloitte.

Stand 10/2024