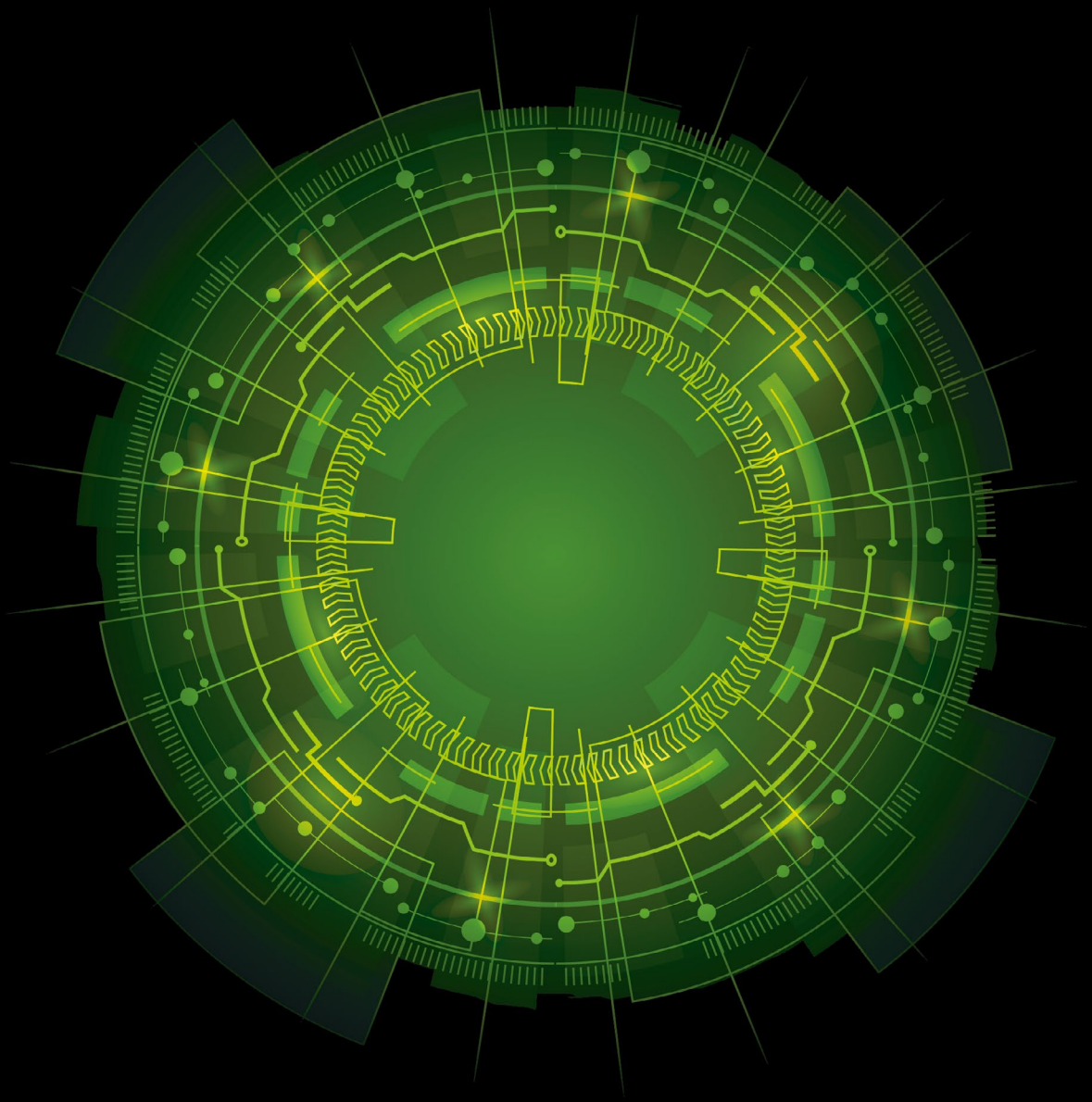
Deloitte.



Deloitte Cyber Security Report 2023

Wie die Unternehmenswelt auf die steigende Cyber-Bedrohungslage reagiert

Eine Studie von Deloitte Österreich in Kooperation mit SORA

MAKING AN IMPACT THAT MATTERS since 1845

Impressum

Herausgegeben von Deloitte Services Wirtschaftsprüfungs GmbH
Autor:innen: Karin Mair / Deloitte, Georg Schwondra / Deloitte,
Christoph Hofinger / SORA und David Laumer / SORA
unter redaktioneller Mitarbeit von Armin Nowshad, Theresa Kopper und Maria Hofer
Grafik und Layout: Claudia Hussovits

Vorwort

Beinahe wöchentlich schaffen es Cyber-Angriffe auf österreichische Unternehmen in die Schlagzeilen der Medien: Hacker, die sich Zugriff auf persönliche Daten von Millionen Kundinnen und Kunden eines Mobilfunkanbieters verschaffen. Cyber-Attacken, die die Buchungs-Homepage einer großen Verkehrsbüro-Gruppe über mehrere Tage zum Erliegen bringen. Aber auch fehlerhafte Software-Updates oder Konfigurationsfehler verursachen immer wieder unerwartete Ausfälle kritischer Dienstleistungen. Mit dem Ausbruch des russischen Angriffskrieges auf die Ukraine hat sich die Situation nochmals verschärft.

Gleichzeitig nimmt die Verbreitung und Nutzung digitaler Informations- und Kommunikationstechnik seit Jahren kontinuierlich zu. Automatisierung und der schnelle Austausch von Daten bergen enorme Möglichkeiten zur Effizienzsteigerung. Auch sicherheitskritische Bereiche können deshalb nicht mehr auf sie verzichten.

Doch wissen die österreichischen Unternehmen über die angespannte Sicherheitslage Bescheid? Wie gut sind sie für den Ernstfall aufgestellt? Und welche Maßnahmen setzen sie, um die Risiken zu minimieren? Bereits zum vierten Mal beantworten wir diese und weitere Fragen im Rahmen unseres jährlichen Cyber Security Report, für den wir in Zusammenarbeit mit dem Forschungsinstitut SORA im März 2023 350 Mittel- und Großunternehmen befragt haben. Das Ergebnis: Österreichs Unternehmen sind auf die zunehmende Professionalität der Cyber-Angriffe in vielen Fällen noch nicht ausreichend vorbereitet. Wo jetzt konkret Handlungsbedarf besteht, erfahren Sie in unserer Studie.

Wir wünschen eine spannende Lektüre!

Karin Mair
Managing Partner |
Risk Advisory & Financial Advisory

Georg Schwondra
Partner | Risk Advisory

Christoph Hofinger
SORA

Key Findings

Professionalität der Angriffe nimmt zu

Während sich die Zahl der Cyber-Vorfälle im Vergleich zum Vorjahr auf annähernd gleichem Niveau hielt, reduzierte sich die Zahl der Angriffe, die durch technische Infrastrukturmaßnahmen verhindert werden konnten, beinahe um die Hälfte. Ebenso konnten um 30 % weniger Daten wiederhergestellt beziehungsweise ganz oder zumindest zu einem großen Teil wieder entschlüsselt werden. Diese Zahlen machen deutlich: Die Qualität der Angriffe hat sich in den vergangenen Monaten gesteigert.

Unternehmen fokussieren Prävention, vernachlässigen aber Detektion und Business Continuity Management

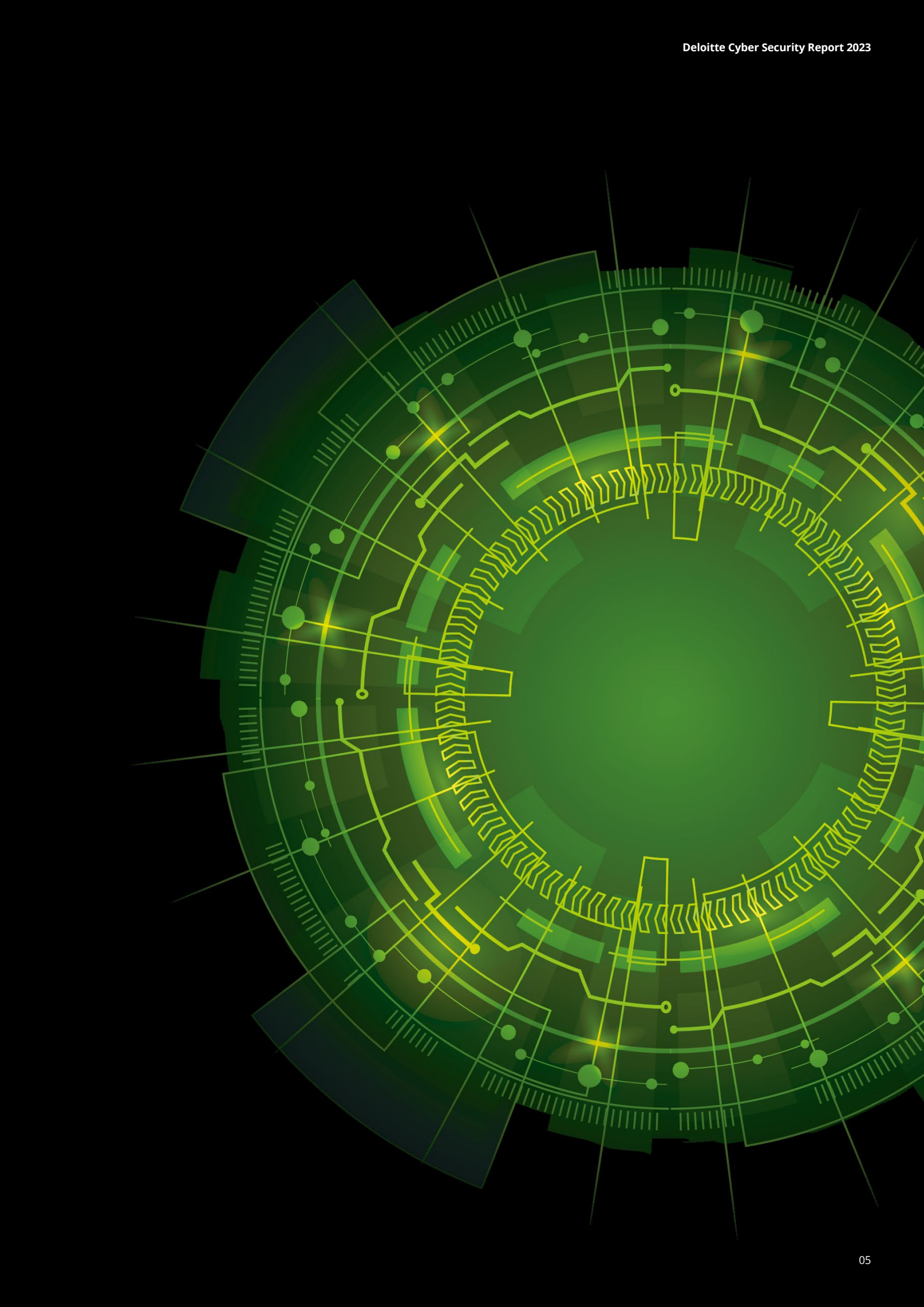
Um sich entsprechend zu wappnen, wollen Unternehmen künftig in Sachen Cyber Security vor allem auf den Schutz vor Angriffen aus dem Internet setzen. So planen etwa 20 % den Traffic mit Antivirus-Software und Firewalls zu filtern, 19 % wollen durch Schulungen für Awareness der Mitarbeiterinnen und Mitarbeiter hinsichtlich Phishing-Angriffe sorgen. Lediglich 4 % der Befragten hingegen arbeiten an der Implementierung von Krisen- oder Notfallplänen. Business Continuity Management (BCM) wird also noch deutlich unterschätzt.

Ukraine-Krieg verschärft die angespannte Situation, viele handeln aber nicht

Die Cyber-Sicherheitslage hat sich aufgrund des russischen Angriffskrieges weiter zugespitzt. Mehr als die Hälfte der Befragten ist derzeit von den Folgen des Konfliktes betroffen. Nur 15 % haben deshalb aber ihre Investitionen in Cyber Security erhöht.

Personalmangel und Lieferengpässe gefährden Sicherheit und Business Continuity

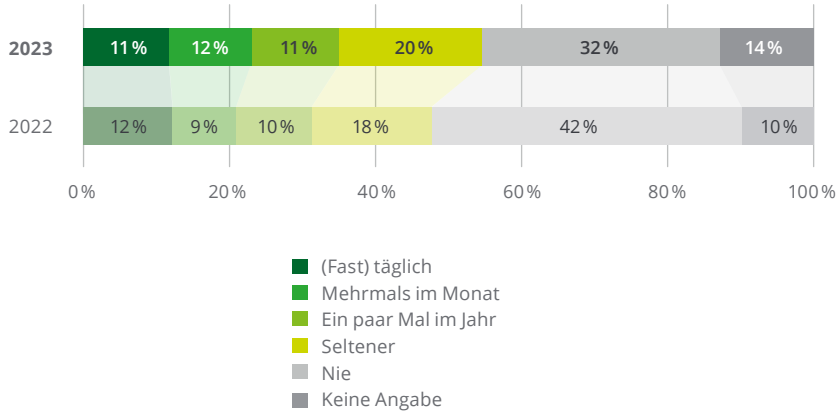
Der anhaltende Fach- und Arbeitskräftemangel macht Österreichs Wirtschaft seit Jahren zu schaffen. So geben 38 % der befragten Unternehmen an, dass es an Personal fehlt. Rund die Hälfte war deshalb sogar schon mit Betriebsausfällen konfrontiert. Der Cyber-Security-Bereich ist vom Fehlen der Talente stark betroffen, die Business Kontinuität wird davon maßgeblich beeinflusst. Hinzu kommen auch Probleme mit den Lieferketten: Fast die Hälfte der Betriebe meldete Lieferengpässe bei benötigter Hardware, bei 20 % kam es dadurch schon zu betrieblichen Ausfällen.



Professionalität der Angriffe steigt

Rund die Hälfte der Unternehmen mit über 50 Mitarbeitenden gibt aktuell an, schon einmal Ransomware-Attacken erlebt zu haben. 11 % sind fast täglich damit konfrontiert, weitere 23 % werden zumindest mehrmals im Jahr davon getroffen.

Häufigkeit von Ransomware-Attacken

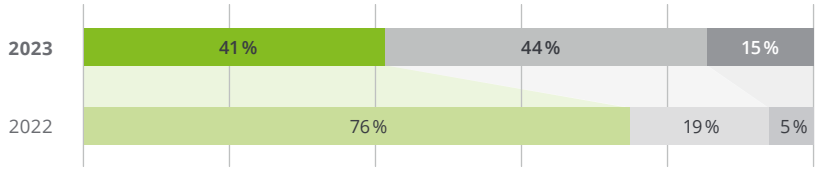


Die Zahl an Cyber-Vorfällen hat sich im Vergleich zum Vorjahr zwar kaum erhöht, die Qualität der Angriffe hat sich aber deutlich gesteigert: So reduzierte sich die Zahl der Attacken, die durch technische Infrastrukturmaßnahmen verhindert werden konnten, um fast die Hälfte. Außerdem konnten etwa ein Drittel weniger Daten über eine Sicherung wiederhergestellt beziehungsweise ganz oder zumindest zu einem großen Teil entschlüsselt werden.

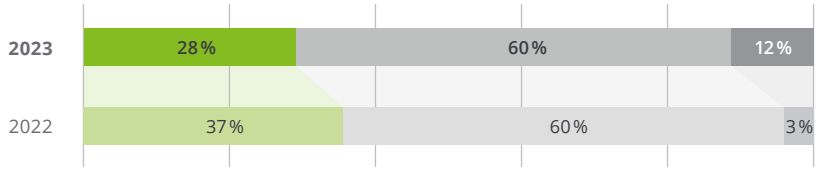
Hinzu kommt, dass sich Ransomware mittlerweile schwieriger entfernen lässt. Die Erfolgsquote der unternehmensinternen IT liegt bei 38 % und jene der externen IT-Expertinnen und -Experten bei 36%. Und dies, obwohl knapp die Hälfte der Unternehmen das Budget für Cyber-Security in den vergangenen Monaten aufstockte.

Auswirkungen von Ransomware-Attacken

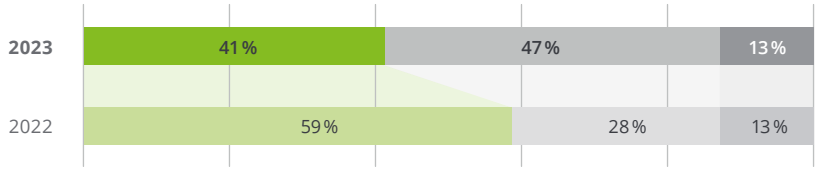
Ausbreitung wurde durch technische Infrastrukturmaßnahmen verhindert



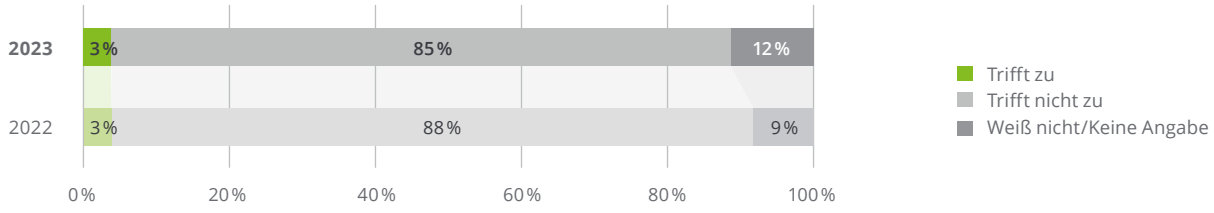
Es kam schon einmal zu einer Verschlüsselung von Daten



Die Daten konnten über eine Sicherung (Backup) wiederhergestellt werden



Es wurde Lösegeld gezahlt



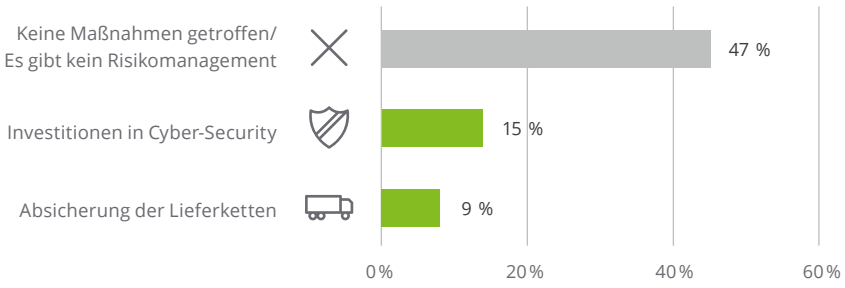
Die Ergebnisse des Cyber Security Report decken sich auch mit den Daten von cert.at. Der aktuelle Lagebericht des Computer Emergency Response Teams verzeichnet im Vergleich zum Vorjahr eine überdurchschnittlich hohe Zahl an widerrechtlichen Zugriffen auf Accounts und bestätigt damit eine Qualitätssteigerung der Angriffe.

Der Krieg in der Ukraine verschärft die Situation

Die ohnehin schon angespannte Cyber-Sicherheitslage hat sich mit dem Ausbruch des russischen Angriffskriegs auf die Ukraine noch weiter zugespitzt. Mehr als die Hälfte (57 %) der Betriebe gibt an, von den Folgen des Konfliktes im Bereich Cyber Security betroffen zu sein. Die Unternehmen leiden deshalb beispielsweise unter Datendiebstählen, Lieferengpässen oder vermehrten Ransomware-Attacken.

Die aktuelle geopolitische Lage veranlasst nur wenige Unternehmen zum Handeln. Lediglich rund 15 % haben aufgrund des Konfliktes Investitionen in die Cyber-Sicherheit getätigt. Auch dem Risikomanagement wird in diesem Zusammenhang noch wenig Bedeutung beigemessen. Bei insgesamt 47 % wurden keine Maßnahmen getroffen oder es gibt kein Risikomanagement.

Sicherheitsmaßnahmen aufgrund des Krieges



Geplante Cyber-Security-Maßnahmen greifen zu kurz

Um sich für die zunehmende Bedrohungslage zu wappnen, konzentrieren sich die befragten Unternehmen derzeit vor allem auf den Schutz vor Angriffen aus dem Internet. So planen im kommenden Jahr 20 % eine Filterung des Traffics mit Antivirus-Software und Firewalls, weitere 19 % fokussieren die Awareness der Mitarbeitenden durch regelmäßige Schulungen. Zudem setzen 17 % der Unternehmen auf Kontrollen ihrer Systeme durch die interne IT-Abteilung oder externe Expertinnen und Experten. Großen Aufholbedarf gibt es bei der Implementierung gezielter technischer Maßnahmen: Lediglich 11 % der Unternehmen wollen derzeit ihre Systeme updaten oder verbessern, 5 % haben vor Zugriffsrechte für Benutzerinnen und Benutzer einzugrenzen.

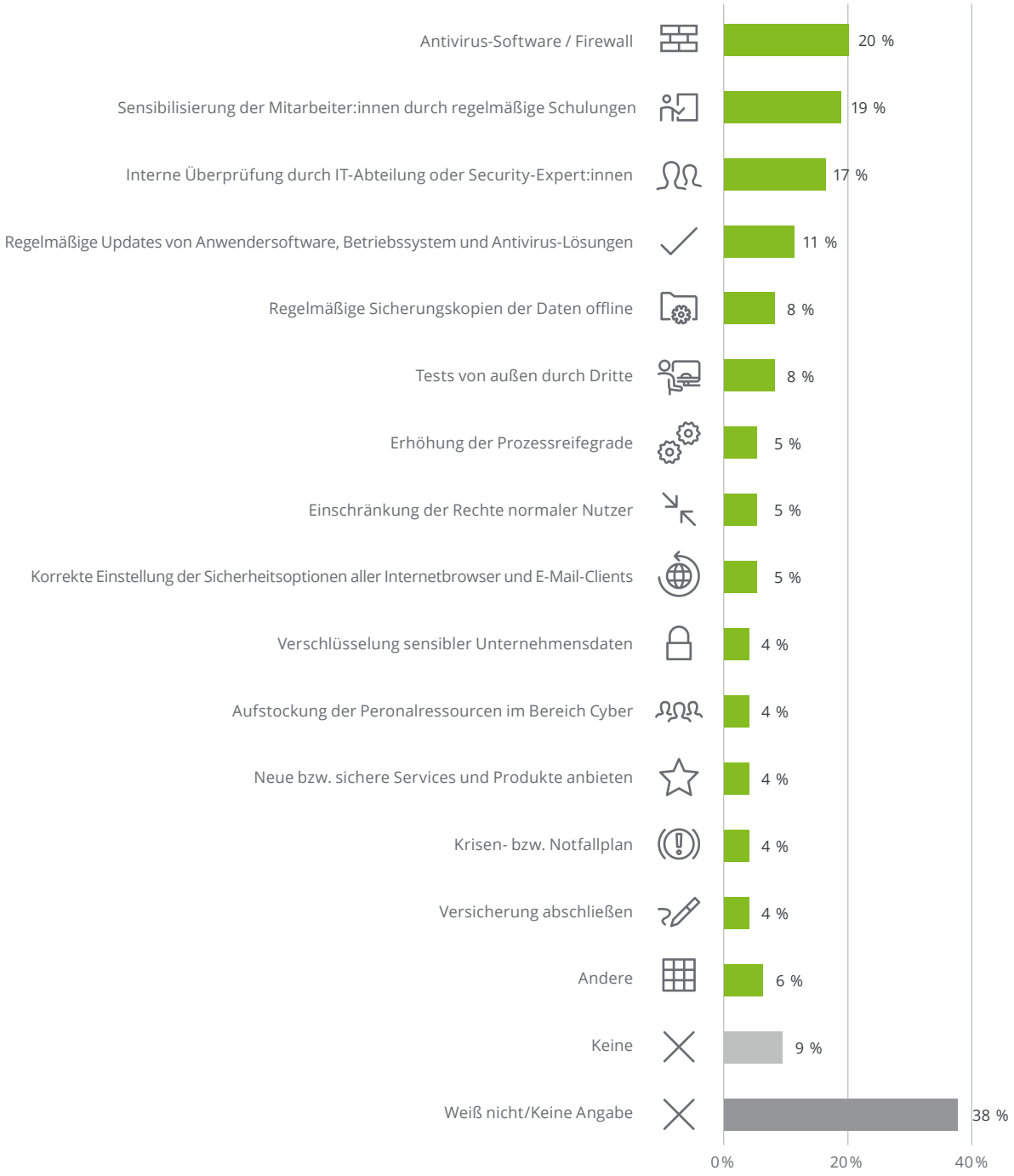
Auffallend ist, dass sich die aktuell geplanten Maßnahmen nicht von jenen aus dem Vorjahr unterscheiden. Die Unternehmen verfolgen nach wie vor eine Cyber-Security-Strategie, die auf Prävention basiert. Da die Qualität der Angriffe allerdings steigt und Phishing-E-Mails damit für Userinnen und User immer schwerer zu identifizieren sind, reicht dieser Ansatz heute nicht mehr aus. Vielmehr braucht es reaktives Handeln, um beispielsweise Sicherheitslücken zu schließen.

Zudem wird dem Thema Business Continuity Management von den befragten Betrieben bisher noch sehr wenig Bedeutung beigemessen. Gerade einmal 4 % der Unternehmen wollen künftig Krisen- oder Notfallpläne implementieren.

„Unsere Beratungspraxis zeigt, dass nur wenige Unternehmen die Wirksamkeit ihrer Krisen- und Notfallpläne für Cyber-Sicherheit auch regelmäßig testen. Gerade darauf kommt es aber an, um im Ernstfall entsprechend reagieren zu können."

Georg Schwondra | Partner | Risk Advisory

Geplante Maßnahmen zum Schutz vor Cyberattacken

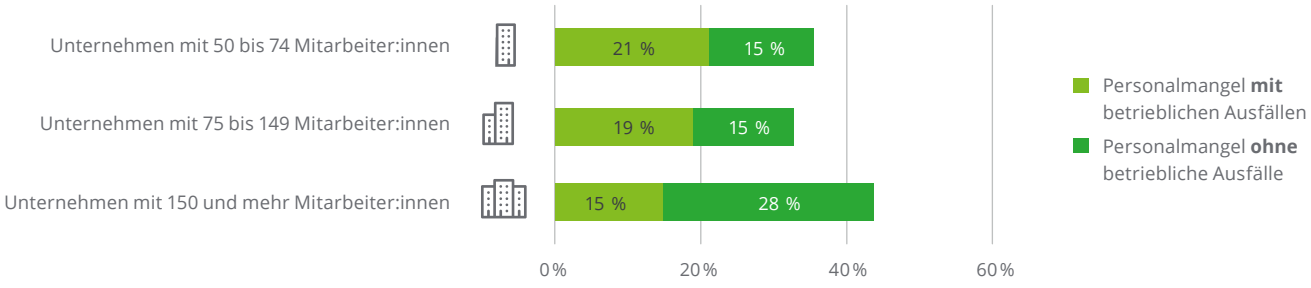


Personalmangel und Lieferengpässe gefährden Sicherheit und Business Continuity

Der anhaltende Fach- und Arbeitskräftemangel beschäftigt die österreichische Wirtschaft mehr denn je. Das zeigt auch die vorliegende Studie: Bei 38 % der Befragten fehlt es an Personal. Rund die Hälfte davon kämpft deshalb sogar mit betrieblichen Ausfällen.

Auf welche Art Unternehmen von Personalmangel betroffen sind, hängt auch mit ihrer Größe zusammen. Betriebliche Ausfälle kommen vordergründig in kleineren Unternehmen vor. Über Personalmangel an sich klagen dagegen vor allem große Unternehmen mit über 150 Mitarbeiterinnen und Mitarbeitern.

Herausforderungen durch Personalmangel in Abhängigkeit von der Unternehmensgröße



„Aufgrund der dünneren Personaldecke sind kleinere Unternehmen anfälliger für betriebliche Ausfälle. Größere Unternehmen verfügen zwar über eine breitere Mitarbeiter:innenbasis und sind deshalb auch stabiler, haben aber einen deutlich höheren Personalbedarf."

Karin Mair | Managing Partner | Financial Advisory & Risk Advisory

Der Mangel an Mitarbeitenden beeinflusst auch die Cyber-Sicherheit der Unternehmen. Gesucht werden in diesem Zusammenhang vor allem Fachkräfte, die Skills in den Bereichen Identity und Access Management, Application Security, Infrastruktur und Netzwerksicherheit sowie Cyber Defense und Cloud Security mitbringen. Um an die Talente zu gelangen, brauchen die Unternehmen neben einer guten Recruiting-Strategie auch ein entsprechendes Weiterbildungsangebot. Mitarbeiterinnen und Mitarbeiter profitieren nicht nur von unternehmensinterner Aus- und Weiterbildung, auch externe Schulungen sind empfehlenswert.

Zusätzlich zum Personalmangel stellen auch Lieferengpässe Herausforderungen für die Unternehmen dar: So fehlt es 45 % der Befragten an dringend benötigter Hardware. Bei knapp der Hälfte davon kam es infolgedessen zu betrieblichen Ausfällen. Auch hier zeigt sich, dass die Abhängigkeit von funktionierenden Lieferketten mit zunehmender Zahl an Mitarbeiterinnen und Mitarbeiter steigt.

Betriebliche Ausfälle aufgrund von Lieferengpässen in Abhängigkeit von der Unternehmensgröße

16 %
in Unternehmen mit **50 bis 74 Mitarbeiter:innen**

20 %
in Unternehmen mit **75 bis 149 Mitarbeiter:innen**

23 %
in Unternehmen mit **150 und mehr Mitarbeiter:innen**

Handlungsempfehlungen

Effiziente Maßnahmen setzen

Aktuelle Prognosen deuten darauf hin, dass sowohl die Anzahl als auch die Qualität der Ransomware-Angriffe in den kommenden Monaten weiter steigen werden. Um sich effizient zu schützen, sollten Unternehmen jetzt in die Verbesserung der Infrastruktur und die Implementierung technischer Maßnahmen, wie beispielsweise Multifaktor Authentifizierung oder Segmentierung, investieren. Ebenso sind Ransomware-sichere Back-ups, die nicht durch Angreifer erreichbar sind, unerlässlich, um nach einer Cyber-Attacke Daten wiederherstellen zu können.

Angriffe rechtzeitig erkennen

Unternehmen sollten sich nicht nur auf die Abwehr von Cyber-Angriffen fokussieren, die Detektion potenzieller Gefahren ist mindestens genauso wichtig und kann großen Schaden verhindern. Investitionen in entsprechende Werkzeuge wie Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) sind in diesem Zusammenhang sinnvoll. Diese machen es möglich, ungewöhnliche Muster im Netzwerk zu erkennen oder sogar zu bekämpfen. Ähnliches kann auch die Verwendung von User Behavioral Analytics leisten, welche auffällige Tätigkeiten von Mitarbeitenden erkennen und melden. Weiters kann ein Abgleich von unternehmenseigenen Accounts mit im Dark Web zum Verkauf angebotenen Accounts hilfreich sein.

Krisenpläne entwickeln und testen

Angesichts der steigenden Bedrohungslage ist die Entwicklung von Krisen- und Notfallplänen ein Gebot der Stunde. Dabei gilt es, in regelmäßigen Abständen Krisenübungen und Simulationen durchzuführen und Sicherheitsstrategien nicht ausschließlich auf präventive Maßnahmen zu beschränken. Denn im Falle eines Cyber-Angriffes ist die Fähigkeit zur schnellen Reaktion unerlässlich.

Fachkräfte suchen und halten

Eine sichere IT-Landschaft basiert auf ausreichend personellen Ressourcen. Da Fachkräfte derzeit rar sind, brauchen Unternehmen wirksame Strategien zur Anwerbung neuer und zum Halten bestehender Talente. Zudem gilt es abzuwägen, woher man die entsprechende Expertise beziehen möchte. In Unternehmen kann es sinnvoll sein, bestehendes Personal in diesem Zusammenhang aus- und weiterzubilden. In anderen ist ein Zukauf des Know-hows durch externe Partner empfehlenswert.

Lieferketten absichern

Zur Vermeidung von Lieferengpässen empfiehlt es sich, Lieferketten abzusichern und Kaufverhalten anzupassen. Ein funktionierendes Third Party Risk Management hilft bei der Risikoeinschätzung in Bezug auf Lieferanten.

Methode und Sample

Zielpopulation: Mittel- und Großunternehmen in Österreich (ab 50 Beschäftigte)

Erhebungsmethode: Standardisierte Telefonbefragung (CATI)

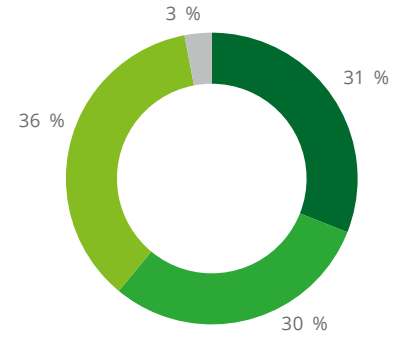
Befragungszeitraum: März 2023

Stichprobe: 350 Unternehmen

Gewichtung: Nach Anzahl der Mitarbeiter:innen und Region

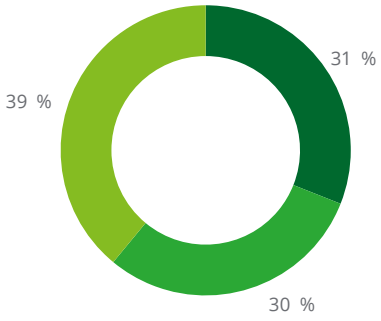
Hinweis: Geringfügige Abweichungen von Sollwerten (z.B. 99 % oder 101 % statt 100 %) sind auf Rundungseffekte zurückzuführen.

Branche



- Produktion, Landwirtschaft, Energieversorgung
- Bau, KFZ, Verkehr
- Gastronomie, Dienstleistungen, Verwaltung
- Andere

Unternehmensgröße



- 50 bis 74 Mitarbeiter:innen
- 75 bis 149 Mitarbeiter:innen
- ab 150 Mitarbeiter:innen

Kontakt

Karin Mair
Managing Partner |
Risk Advisory & Financial Advisory

+43 1 537 00-4840
kmair@deloitte.at

Georg Schwondra
Partner | Risk Advisory

+43 1 537 00-3760
gschwondra@deloitte.at

Zum digitalen Download der Studie:

Deloitte.