Cyberangriffe und Datendiebstahl: virtuelle Gefahr – reale Schäden

Eine Befragung von 200 österreichischen Unternehmen

EY

Building a better working world

Inhalt

Vorwort

der Autoren von EY

„

In Zeiten der Digitalisierung sind Cyberangriffe zu einem der größten Risiken für Unternehmen geworden.

Die Digitalisierung ermöglicht schnellere, effizientere und einfachere Abläufe. Partner, Systeme und Maschinen sind über Unternehmensgrenzen hinweg vernetzt. Die Verlagerung von Anwendungen in die Cloud oder der Einsatz von Robotics gehören zum Produktionsalltag. Mit jeder Schnittstelle, jeder weiteren Zugriffsmöglichkeit steigt jedoch die Bedrohung durch Cyberangriffe. Für IT-Sicherheitsexpert:innen ist ein Hackerangriff keine Frage des Ob, sondern nur noch des Wann. Für professionell agierende Cyberkriminelle ist jedes Unternehmen ein interessantes Ziel.

Cybercrime und Datendiebstahl sind Bedrohungen, die österreichische Unternehmen zwar akzeptieren, aber nicht tatenlos hinnehmen müssen. An der Erkenntnis mangelt es in der Wirtschaft nicht, eher am konsequent daraus abgeleiteten Handeln. Cybersicherheit wird oft nur als notwendige Compliance-Aufgabe oder gar als reiner Kostenfaktor betrachtet. Dabei kann eine hohe Sicherheit bei digitalen Prozessen oder Produkten ein Mehrwert oder Wettbewerbsvorteil sein. Cloud-Systeme oder Plattformen etwa funktionieren nur zuverlässig, wenn sie von Grund auf sicher sind. Das Kundenvertrauen kann durch nachweislich existente Sicherheitsmaßnahmen gestärkt werden. Cybersicherheit ist so notwendig wie das Qualitätsmanagement.

Angreifer:innen sind schon lange keine Einzelpersonen mehr und besitzen heute ein umfassendes Expertenwissen oder können dies in den dunklen Ecken des Internets zukaufen. Oft werden Kund:innen über Tage und Wochen ausspioniert, um dann im entscheidenden Moment kontaktiert zu werden. Dann bleiben die Bildschirme schwarz, der Internetauftritt ist verschwunden, die Produktion lahmgelegt. Die Angreifer:innen fordern meist ein Lösegeld. Doch selbst wer zahlt, hat keine Garantie für die Wiederherstellung seiner Daten.

Die unternehmensinterne Verantwortung für Cybersicherheit und Datenschutz in all ihrer Komplexität gehört daher in die Hände von ausgewiesenen Cyber-Fachleuten mit entsprechender Entscheidungskompetenz und den notwendigen Ressourcen, oft auch ergänzt um externe Expertise. Denn der Schaden, der im Fall von Cyberangriffen und Datendiebstahl droht, kann für Unternehmen immens sein: Die Täter:innen haben es mittlerweile überwiegend auf Kundendaten und Know-how abgesehen – beides gehört zu den wichtigsten Werten eines Unternehmens. Hinzu kommt, dass die Bedrohungen aus dem Netz definitiv weiter ansteigen werden, wenn neue Technologien wie Blockchain und künstliche Intelligenz (KI) in unserem Arbeiten fest verankert sein werden. Im Darknet wird schon länger mit „Crime as a Service" geworben und Kriminalität als Dienstleistung verkauft.

Mehr zum Thema Cyberkriminalität sowie alle Zahlen, Details und Expertenmeinungen finden Sie auf den nachfolgenden Seiten dieser Studie.

“

Bei jeder Form von Angriff und Datenklau kommt es darauf an, schnell und überlegt reagieren zu können. Die Reaktionsfähigkeit muss regelmäßig trainiert werden.

Ihre Ansprechpartner

Gottfried Tonweber
Partner, Cybersecurity
& Data Privacy bei
EY Österreich

Bernhard Zacherl
Director, Cybersecurity
& Data Privacy bei
EY Österreich

Birgit Eschinger
Senior Manager, Cyber-
security & Data Privacy
bei EY Österreich

Thomas Steiner
Director, Cybersecurity
& Data Privacy bei
EY Österreich

Ermano Geuer
Senior Manager, Leiter
Corporate Law bei
EY Law Österreich

Robert Pölzelbauer
Manager, Leiter
Cyberforensik bei
EY Österreich

Ergebnisse auf einen Blick

76 %

... der befragten Führungskräfte erwarten in Zukunft eine steigende Gefahr durch Cyberangriffe und Datendiebstahl

In 16 % der Unternehmen gibt es konkrete Hinweise auf Cyberangriffe bzw. Datendiebstah in den vergangenen fünf Jahren, 7 % sogar mehrfach.

29 % der befragten Führungskräfte bereitet die Informationssicherheit des eigenen Unternehmens Sorgen und sie bewerten das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als eher oder sehr hoch.

Für die Zukunft ihres jeweiligen Unternehmens erwarten 76 % der befragten Führungskräfte eine steigende Gefahr durch Cyberangriffe und Datendiebstahl.

20 % fürchten Angriffe durch organisierte Verbrechergruppen, 18 % sehen ihr Unternehmen durch Hacktivist:innen wie Anonymous gefährdet.

Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Handels- und Konsumgüterunternehmen (29 %) und Unternehmen der Energiebranche (27 %)

Besonders angriffsgefährdete Stellen im Unternehmen sind der Vertrieb, der in beinahe jedem zweiten Fall betroffen war, und das Finanzwesen. Im Vertrieb gab es einen enormen Anstieg von 19% im Vorjahr auf 45 % in 2022.

Bei 30 % der Unternehmen konnten Spionageangriffe durch das interne Kontrollsystem identifiziert werden. Durch unternehmensinterne Hinweise wurden 13 % der Angriffe aufgedeckt. Jedoch wird trotz interner Kontrollmechanismen und anderer Aktivitäten immer noch fast jeder fünfte Angriff (19 %) rein zufällig entdeckt.

Während der Pandemie haben 17 % der Unternehmen ihre Cybersecurity-Maßnahmen verschärft, 14 % sogar sehr. Um sich während der Coronakrise vermehrt zu schützen, hat mehr als die Hälfte (56 %) der befragten Unternehmen ihre Mitarbeiter:innen sensibilisiert und ihre IT-Infrastruktur modernisiert (54 %). Außerdem hat mehr als ein Drittel der Unternehmen (36 %) neue organisatorische Regelungen aufgesetzt.

Mehr als die Hälfte der Unternehmen hat während der Coronapandemie Ihre Mitarbeiter:innen sensibilisiert.

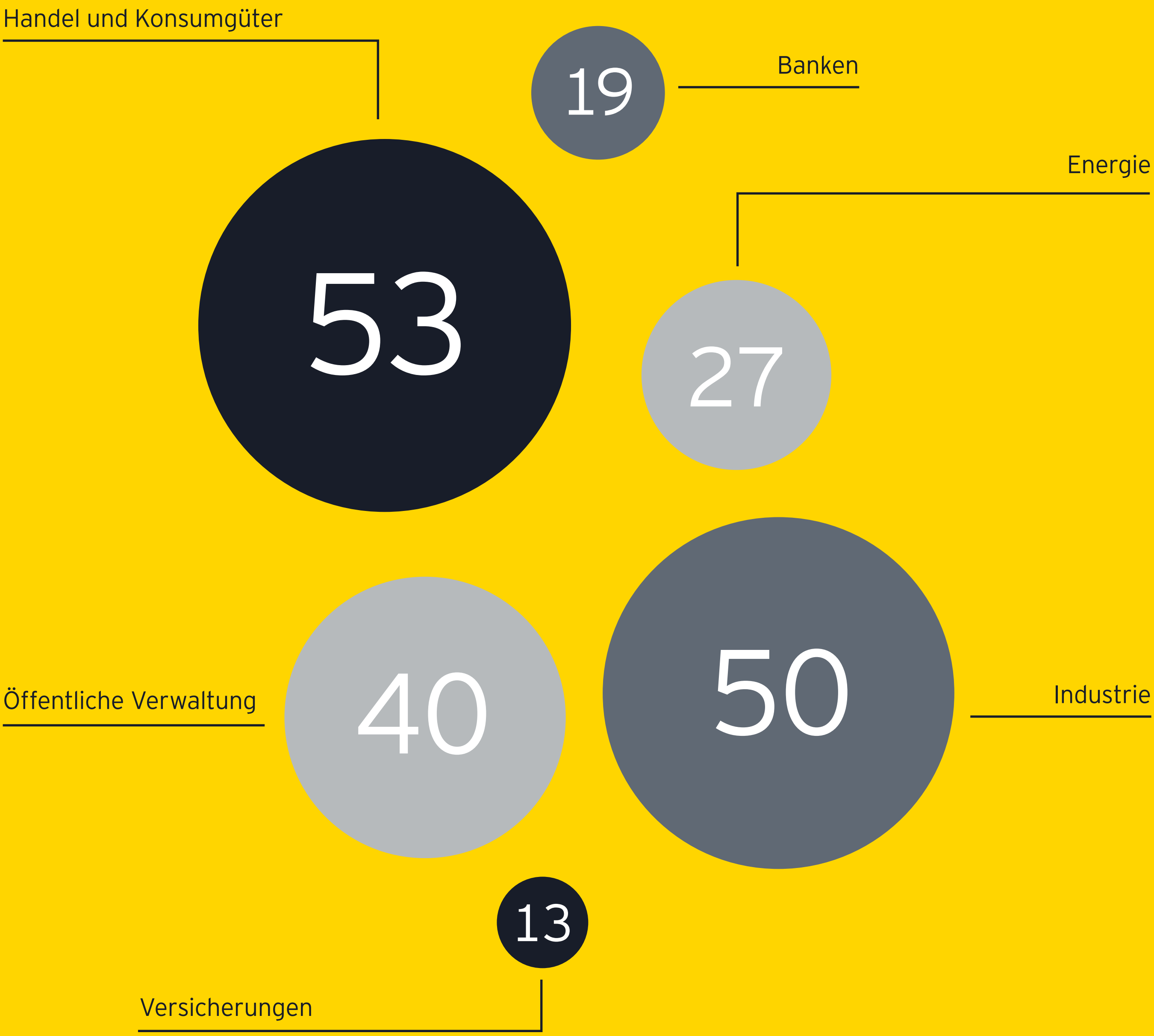
56 %

Design der Studie

Die nachfolgende Studie beruht auf den Ergebnissen einer repräsentativen telefonischen Befragung von 202 Führungskräften österreichischer Unternehmen ab 20 Mitarbeitenden. Es wurden Geschäftsführer:innen, Leiter:innen Konzernsicherheit oder Leiter:innen IT-Sicherheit von Unternehmen verschiedenster Größe (gemessen an Mitarbeiterzahl und Umsatzstärke) zum Thema Datenklau befragt.

Durchgeführt hat die Befragung das unabhängige Marktforschungsinstitut market Marktforschungs-Ges.m.b.H. & Co.KG, Linz im Jänner 2021. Die Ergebnisse sind repräsentativ für die folgenden Branchen:

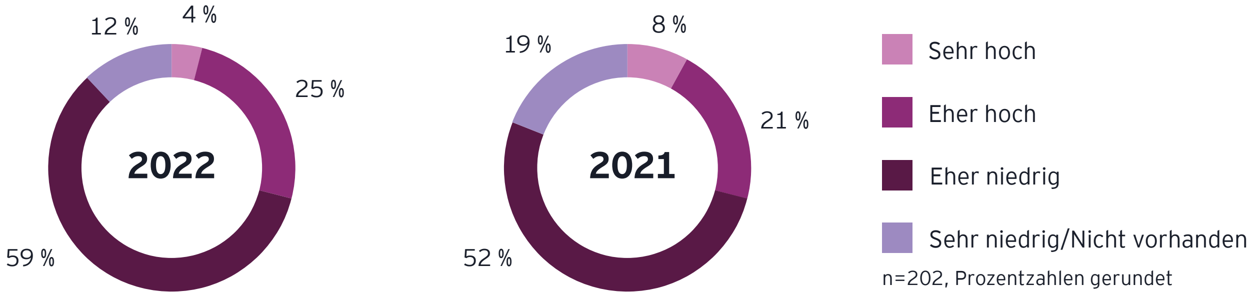
Anzahl der befragten Unternehmen je Branche



1

Einschätzung: Wie hoch ist die Gefährdung? Wie wird sie sich in Zukunft entwickeln?

1.1 Wie hoch schätzen Sie das Risiko für Ihr Unternehmen, Opfer von Cyberangriffen/Datendiebstahl zu werden?

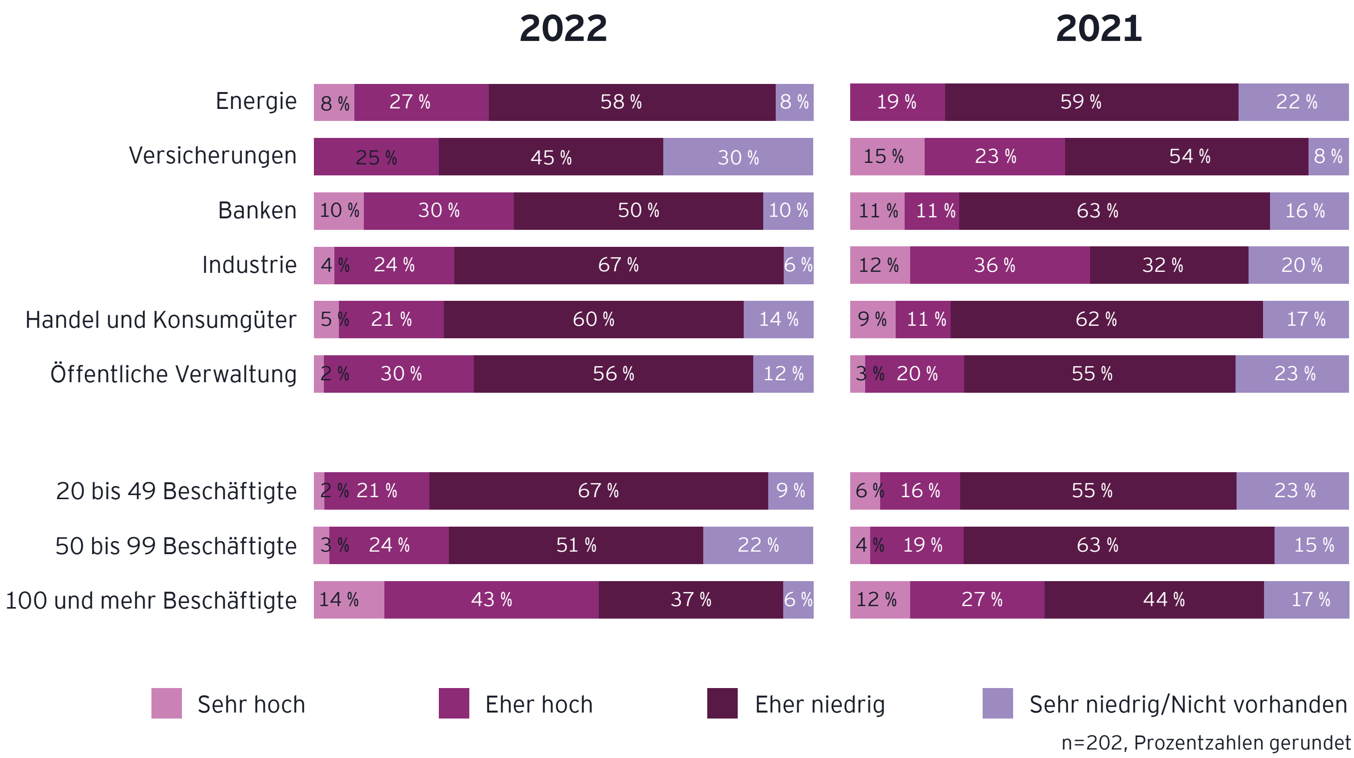


Weniger als ein Drittel der Manager:innen bewertet das Risiko, Opfer von Cyberangriffen zu werden, als eher hoch oder sehr hoch. Dabei zeigt sich, dass der Trend für dieses Gefahrenbewusstsein seit der letzten Befragung im vergangenen Jahr leicht gestiegen ist. Dagegen schätzt mehr als die Hälfte der Befragten das Risiko als eher niedrig ein. Viele Manager:innen erwarten, dass sie ihre gesteigerten Investitionen in Cybersicherheit unverwundbar machen. Dabei werden Angreifer:innen immer professioneller und unauffälliger.

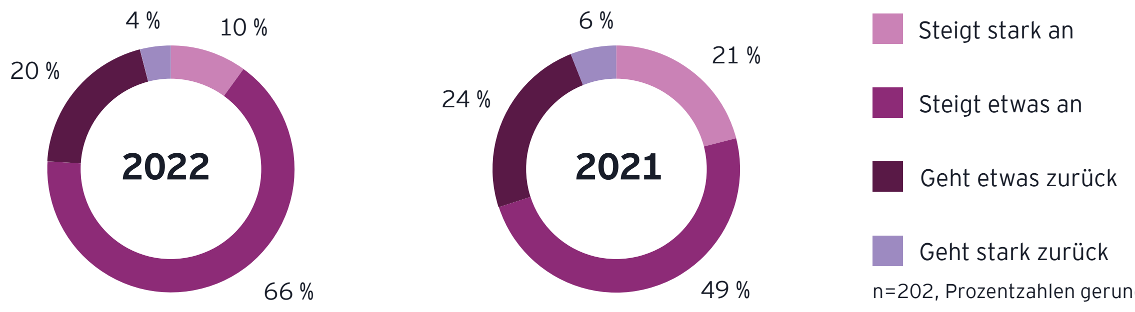
Je größer das Unternehmen, desto größer das Risiko: Etwa jedes siebte größere Unternehmen (14 %) mit mehr als 100 Beschäftigten schätzt das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als sehr hoch ein. Besonders gefahrenbewusst zeigen sich die Banken- und die Energiebranche. Hier sehen 10 % bzw. 8 % der befragten Führungskräfte ein sehr hohes Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, in der Handels- und Konsumgüterbranche 5 %, in der Industrie 4 %.

> ”
> 29 % der Manager:innen bereitet die Informationssicherheit des eigenen Unternehmens Sorgen – das sind weniger als im letzten Jahr.

Größere Unternehmen sehen ein höheres Risiko



1.2 Was meinen Sie, wie wird sich die Bedeutung des Problems Cyberangriffe/Datendiebstahl künftig entwickeln?



n=202, Prozentzahlen gerundet

”

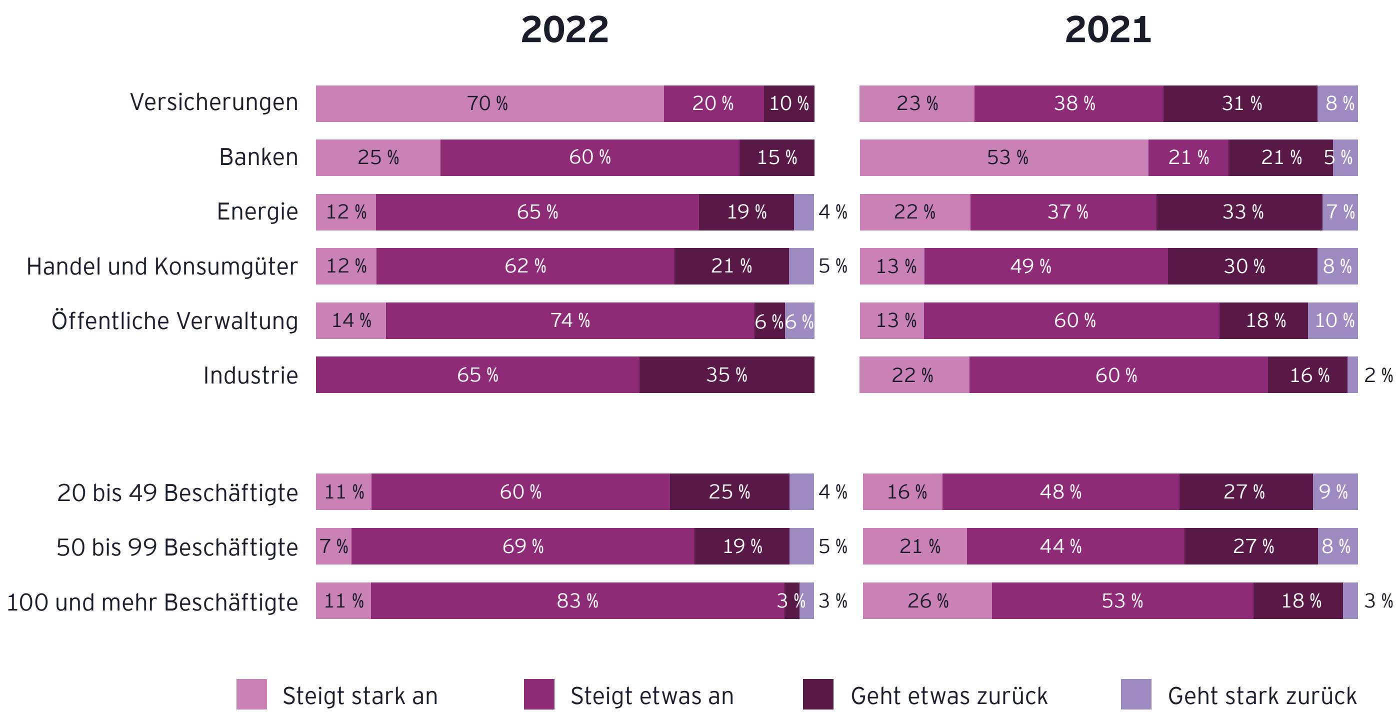
Immer noch rechnen 76 % der Unternehmen mit einer Verschärfung des Problems.

Auch in der aktuellen Umfrage gehen immer noch 76 % der Befragten davon aus, dass die Gefahr für Unternehmen, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, weiterhin zunehmen wird. Fast jede zehnte Führungskraft sieht sogar ein stark steigendes Risiko. 2021 waren die Zukunftsaussichten noch pessimistischer.

Wie bereits in den Jahren zuvor zeigen sich die Unternehmen alarmiert. Besonders Versicherungen, die bereits jetzt ein verhältnismäßig hohes Risiko sehen, erwarten für die kommenden Jahre eine stark zunehmende Bedrohung.

Jedes neunte größere Unternehmen mit 100 oder mehr Beschäftigten rechnet damit, dass sich die Problematik von Cyberangriffen bzw. Datendiebstahl weiter verschärfen wird. Bei mittleren Unternehmen steigt das Risikobewusstsein an.

Insbesondere Versicherungen sind alarmiert



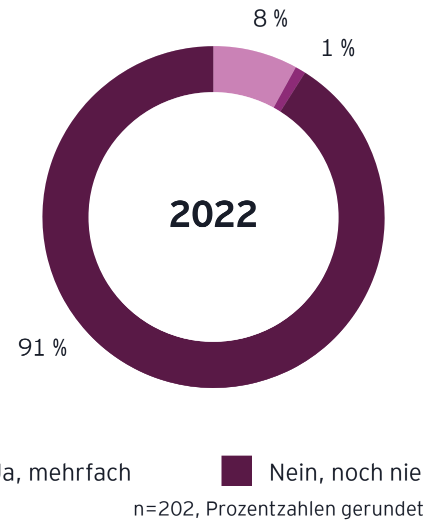
n=202, Prozentzahlen gerundet

1.3 Gab es jemals Erpressungsversuche gegenüber Ihrem Unternehmen, also Angriffe, bei denen Geld gefordert wurde?

8 % der Befragten waren bereits mit einem derartigen Angriff konfrontiert, nur 1 % mehrfach. Für die Angreifer:innen war dies jedoch selten von Erfolg gekrönt.

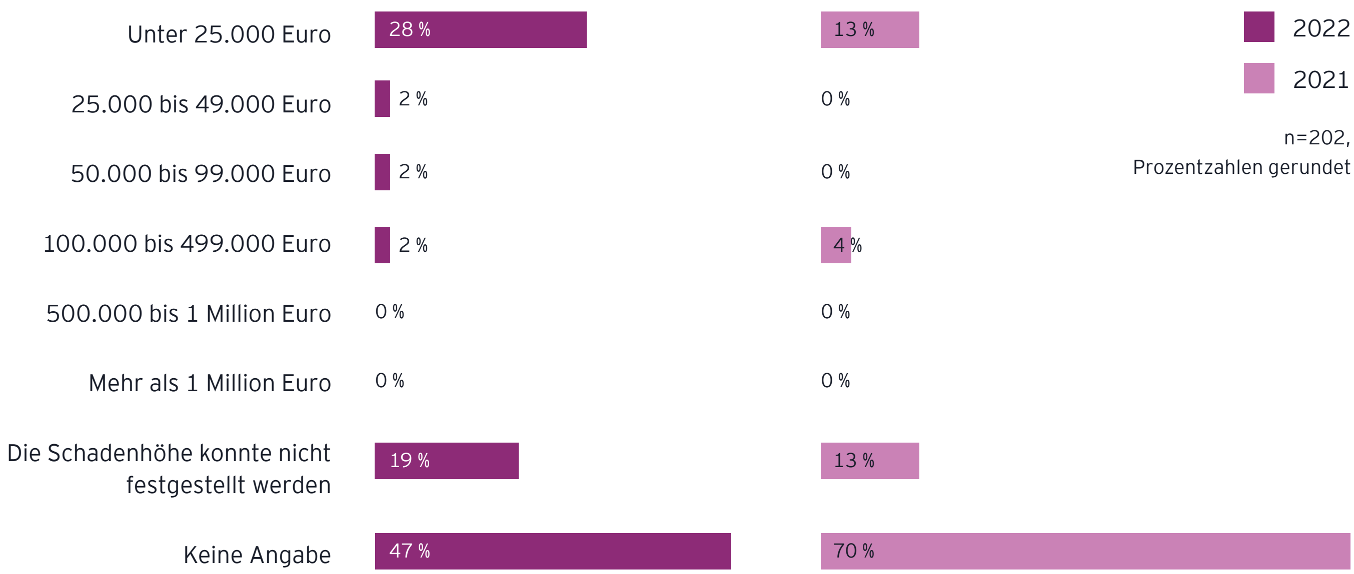
Eine besondere Form des Cyberangriffs ist der Einsatz von Ransomware oder Erpressungssoftware. Das sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder den Zugriff auf das ganze Computersystem verhindern kann. Für die Entschlüsselung fordern die Angreifer:innen Lösegeld.

8 % der Befragten waren bereits mit einem derartigen Angreifer:innen konfrontiert, nur 1 % mehrfach. Für die Angreifer war dies jedoch selten von Erfolg gekrönt: 25 % der Unternehmen möchten nicht sagen, ob sie bezahlt haben, 75 % haben dem Druck der Erpresser:innen nicht nachgegeben.



Falls ja, haben Sie bezahlt?

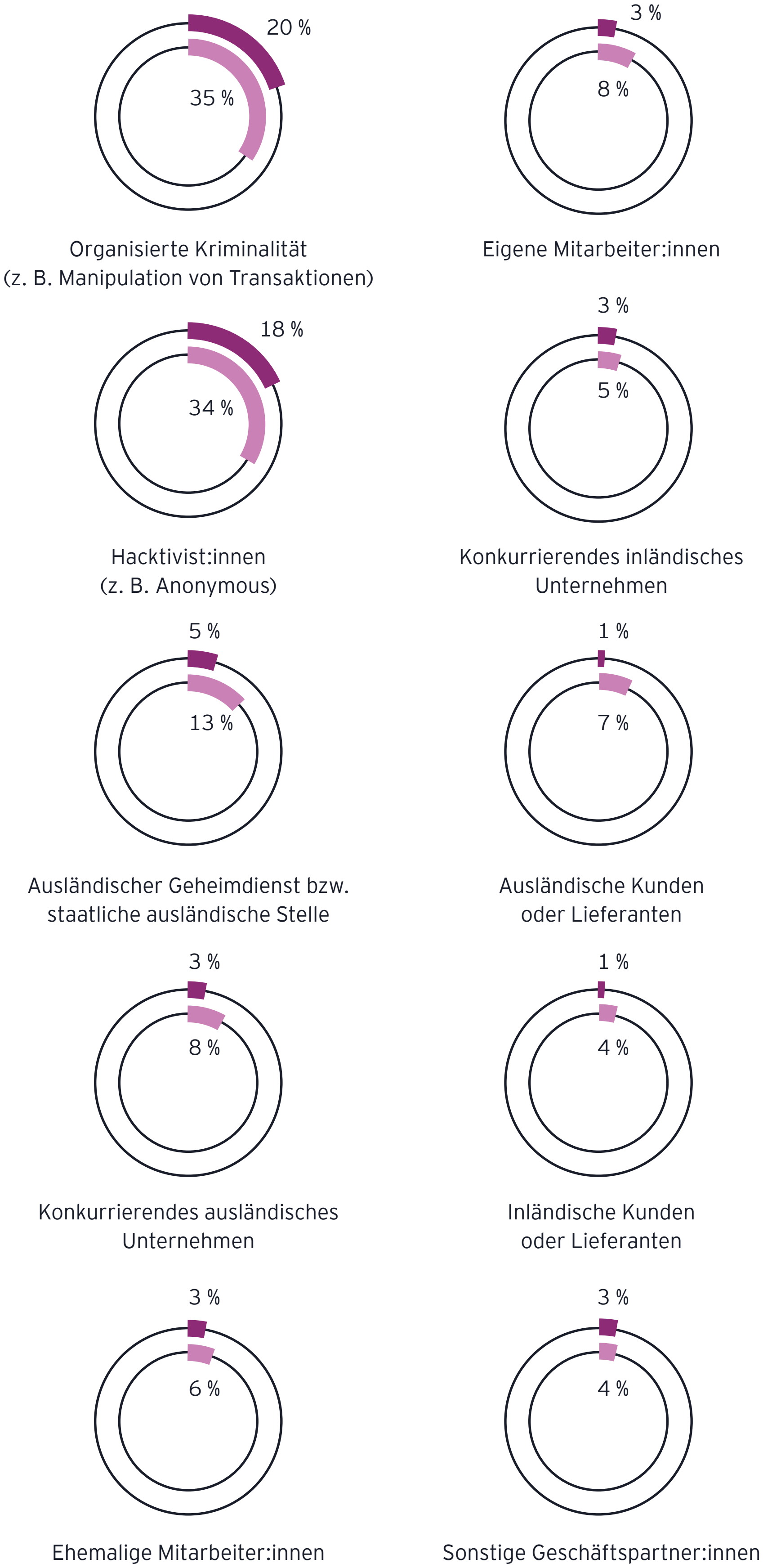
Wie hoch war der durchschnittlich höchste Schaden pro Datendiebstahl?



2 Risikopotenziale und Tätergruppen

2.1 Wie bewerten Sie das Risiko, von folgenden Tätergruppen geschädigt zu werden?

Besonders gefürchtet: organisierte Kriminalität



n=202, Prozentzahlen gerundet

”

Österreichische Unternehmen fürchten insbesondere, Opfer von organisierter Kriminalität zu werden. So bewertet jede fünfte Führungskraft dieses Risiko als hoch oder sehr hoch.

Im Vergleich zu 2021 ist das Risikobewusstsein der österreichischen Unternehmen gesunken. Viele heimische Manager:innen fühlen sich durch Investitionen in die Cybersicherheit besser gegen Angriffe gerüstet und schätzen die Gefahr als geringer ein.

Österreichische Unternehmen fürchten insbesondere, Opfer von organisierter Kriminalität zu werden. So bewertet jede fünfte Führungskraft dieses Risiko als hoch oder sehr hoch.

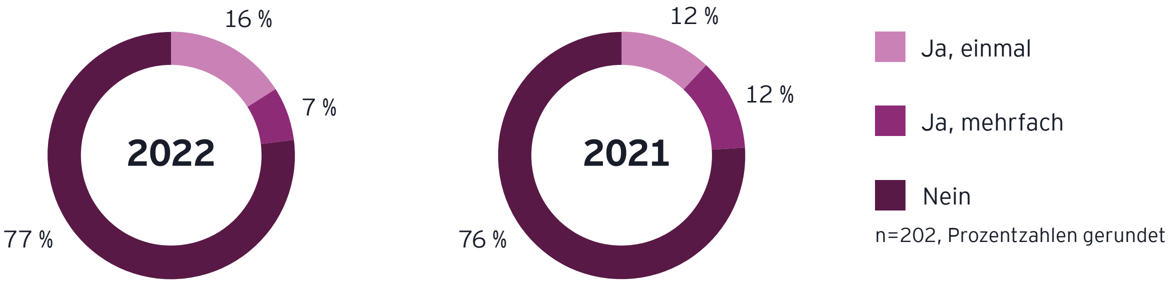
Auch das Risiko, von Hacktivist:innen oder ausländischen Geheimdiensten/staatlichen ausländischen Stellen geschädigt zu werden, wird als vergleichsweise hoch eingeschätzt.

Als gefährlich stufen die Befragten auch wieder den Datendiebstahl durch eigene Mitarbeiter:innen ein. Die Weiterbildung und Schulung von Mitarbeitenden ist hier wichtig, um sie für dieses Thema zu sensibilisieren.

3

Wer wurde Opfer?
Wer sind die Täter:innen?

3.1 Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Cyberangriffe bzw. Datenklau innerhalb der vergangenen fünf Jahre?



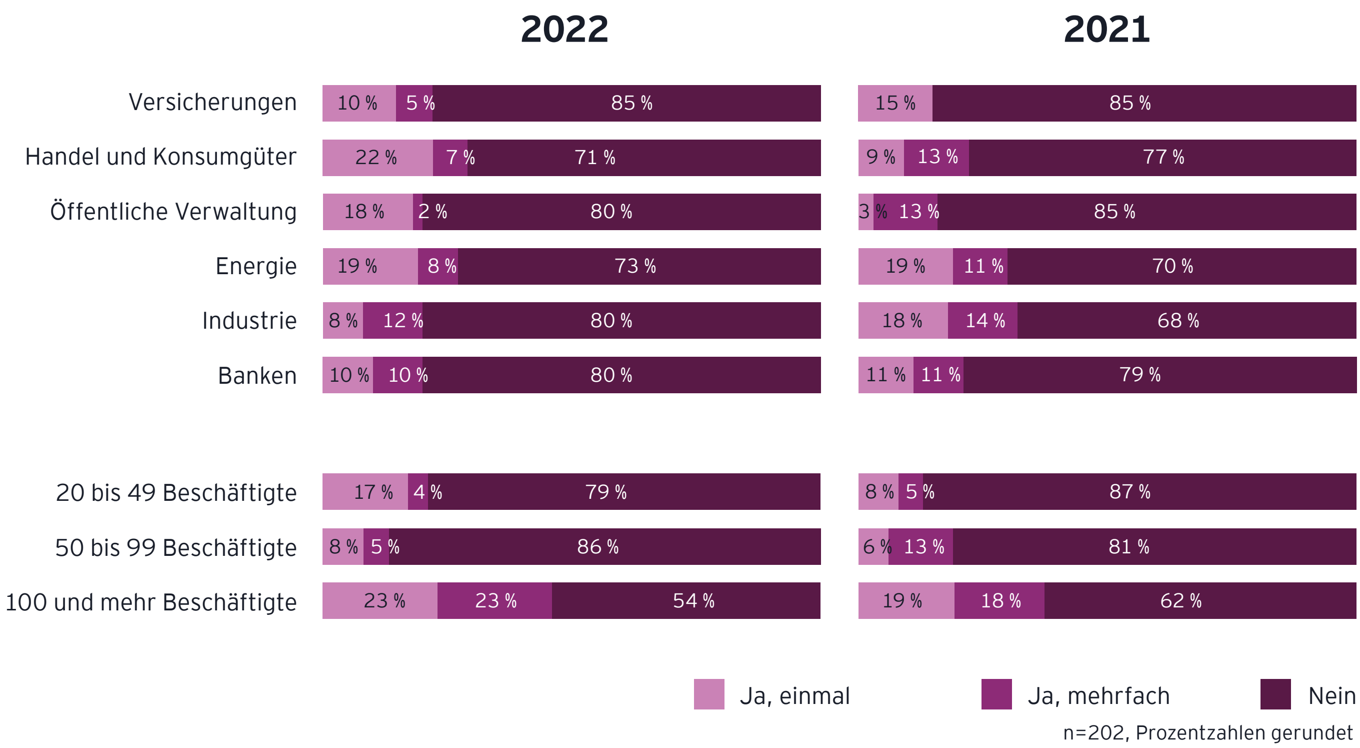
Bei 23 % der Unternehmen hat es in den vergangenen fünf Jahren konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gegeben.

11 % der befragten Unternehmen gaben an, dass kriminelle Handlungen nur durch Zufall aufgedeckt worden seien. Die Dunkelziffer der tatsächlich erfolgten Fälle von Cyberangriffen bzw. Datenklau dürfte demnach deutlich höher sein. Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Handels- und Konsumgüter-Unternehmen und bei Unternehmen der öffentlichen Verwaltung. Hier berichten 29 % bzw. 20 % der befragten Führungskräfte von Hinweisen auf Cyberattacken.

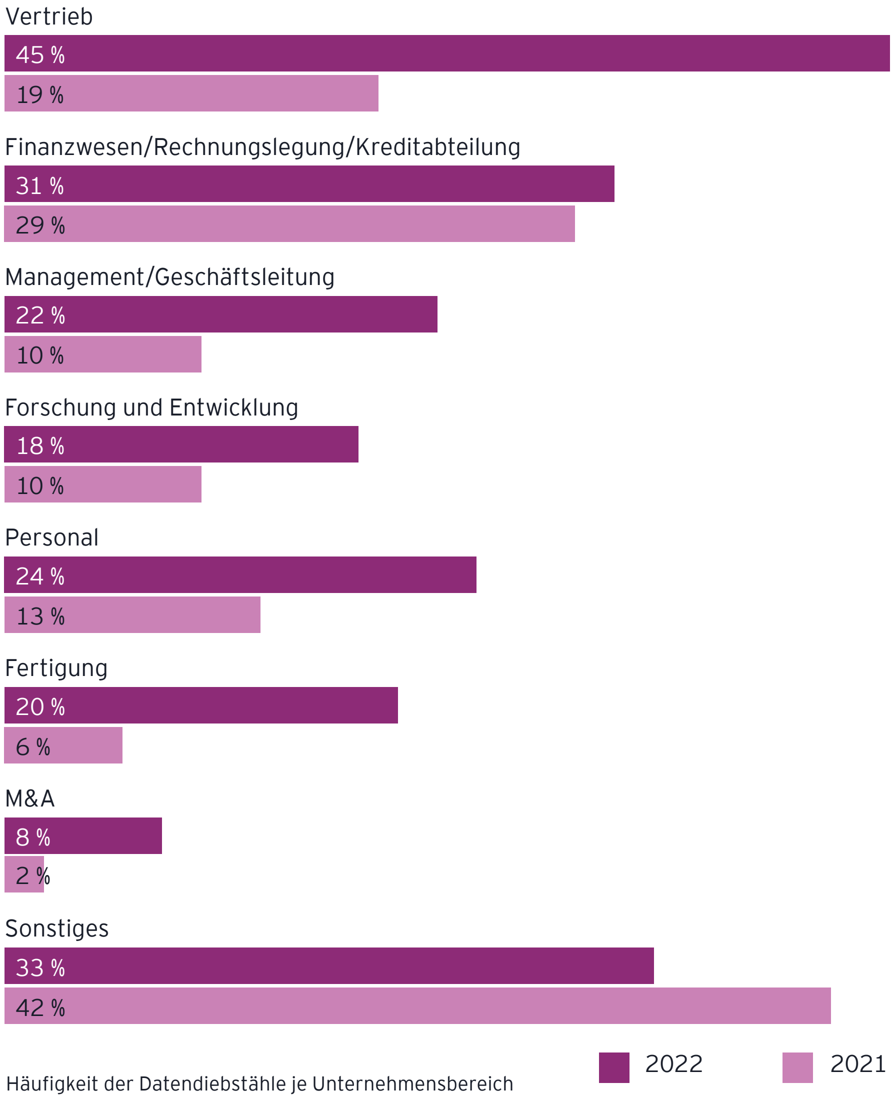
Vor allem größere Unternehmen mit 100 oder mehr Beschäftigten hat es besonders getroffen. In 46 % der Unternehmen dieser Größe gab es zuletzt Hinweise auf Attacken. An dieser Stelle ist zu berücksichtigen, dass mit der Größe des Unternehmens die Investitionsbereitschaft in Schutzmechanismen zunimmt. Erst durch diese bereits etablierten und erprobten Schutzmechanismen steigt die Wahrscheinlich keit, Angriffe zu entdecken.

> ”
>
> In fast jedem vierten österreichischen Unternehmen gibt es konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl.

Größere Unternehmen sind deutlich stärker betroffen



3.2 Welcher Bereich war vom Datendiebstahl betroffen bzw. wo ergab sich dieser Verdacht?



Häufigkeit der Datendiebstähle je Unternehmensbereich (Mehrfachantworten möglich)

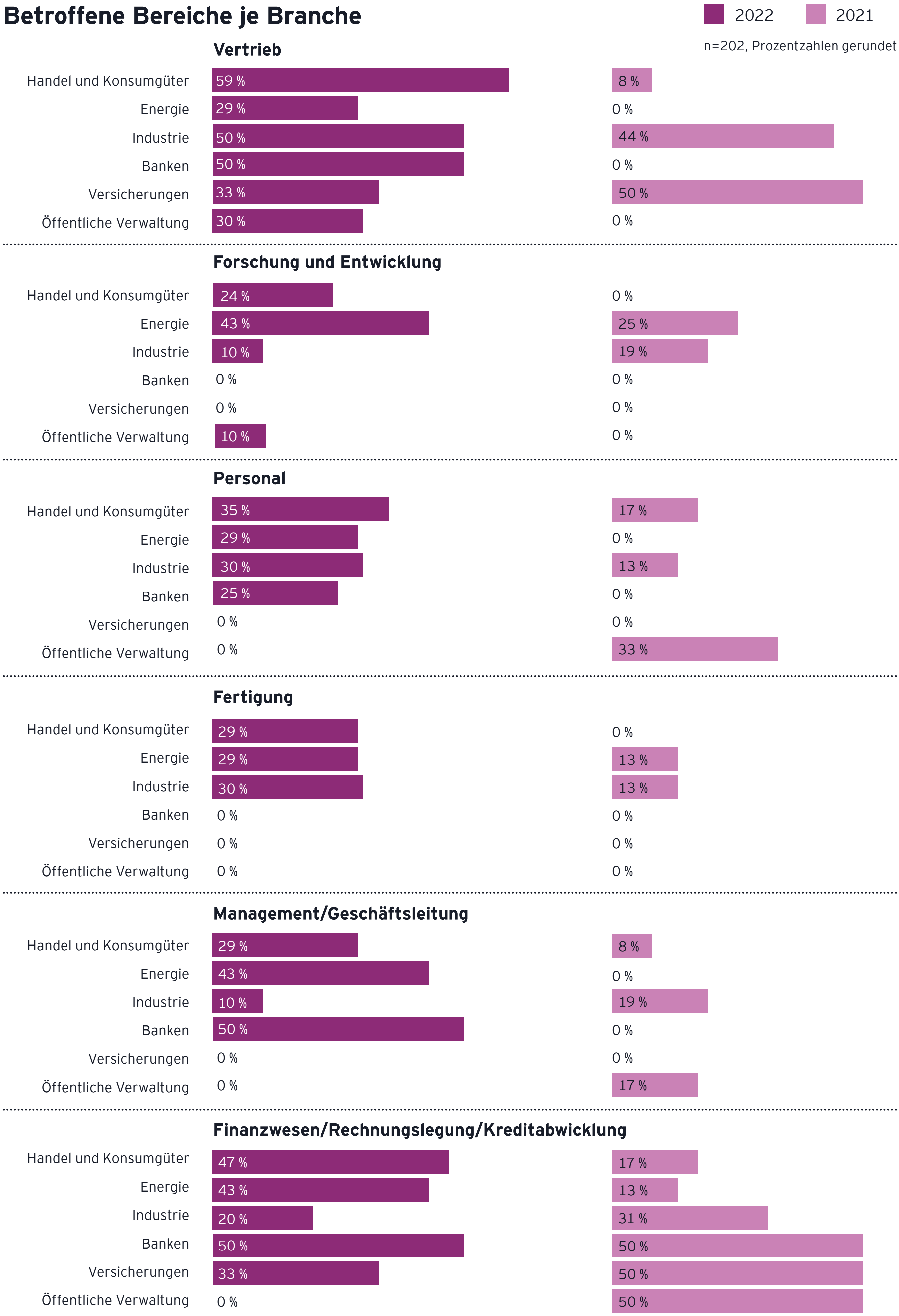
n=202, Prozentzahlen gerundet

> Über alle Branchen hinweg gibt es beliebte Angriffsziele – den Vertrieb und das Finanzwesen mit Rechnungslegung und Kreditabteilung.

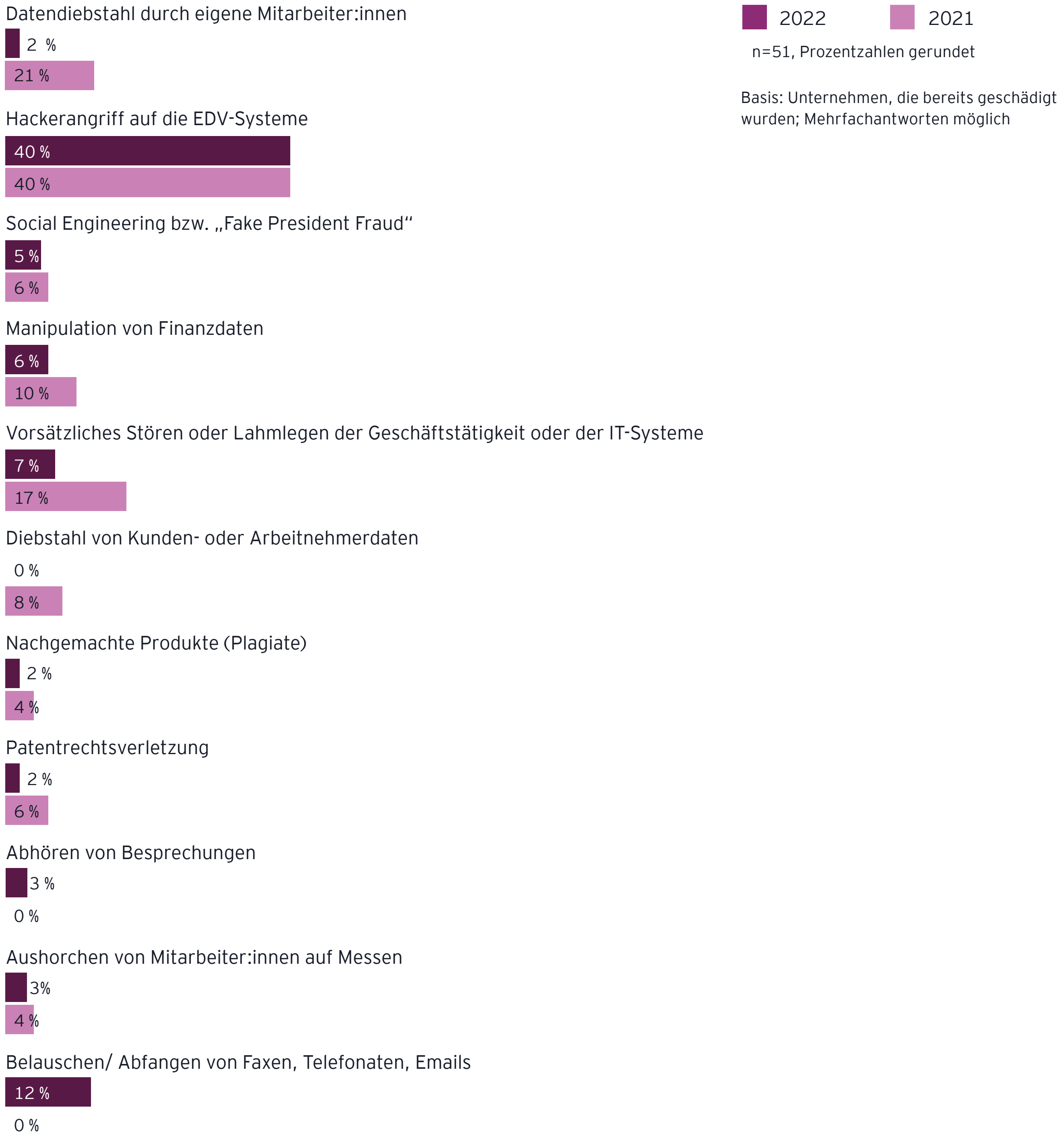
Besonders angriffsgefährdete Stellen im Unternehmen sind der Vertrieb, der in beinahe jedem zweiten Fall betroffen war, und das Finanzwesen. Im Vertrieb gab es im Vergleich zu 2021 einen starken Zuwachs, von 19 % auf 45 %.

Über alle Branchen hinweg gibt es ein beliebtes Angriffsziel – das Finanzwesen mit Rechnungslegung und Kreditabteilung. Bei Industrieunternehmen und Versicherungen ist auch der Bereich Vertrieb inkl. Kundendaten betroffen. Bei Industrieunternehmen steht zudem der Bereich Forschung und Entwicklung im Fokus. In der Handels- und Konsumgüter-Branche und in der öffentlichen Verwaltung sind auch Personaldaten vermehrt im Visier der Angreifer:innen.

Betroffene Bereiche je Branche



3.3 Welche konkreten Handlungen fanden statt?



Wie bereits in den Jahren zuvor sind die mit Abstand meisten Attacken Hackerangriffe auf die IT-Systeme (40 %). Auch wenn Hackerangriffe auf und das vorsätzliche Lahmlegen von IT-Systemen noch immer am meisten verbreitet sind, sind die Zahlen im Vergleich zum letzten Jahr eindeutig gesunken. Dabei umfasst das vorsätzliche Stören oder Lahmlegen der Geschäftstätigkeiten oder der IT-Systeme auch die Verschlüsselung und den darauffolgenden Verlust des Zugriffs auf die eigenen Daten durch sogenannte Ransomware. Dabei handelt es sich um eine bösartige Schadsoftware (Malware), die den Zugriff auf Daten unmöglich macht und Benutzer:innen auf diese Weise sogar vom Gerät aussperren kann.

”

Fast jede dritte Attacke zielte auf vorsätzliches Stören der IT-Systeme ab.

Die Evolution von Ransomware

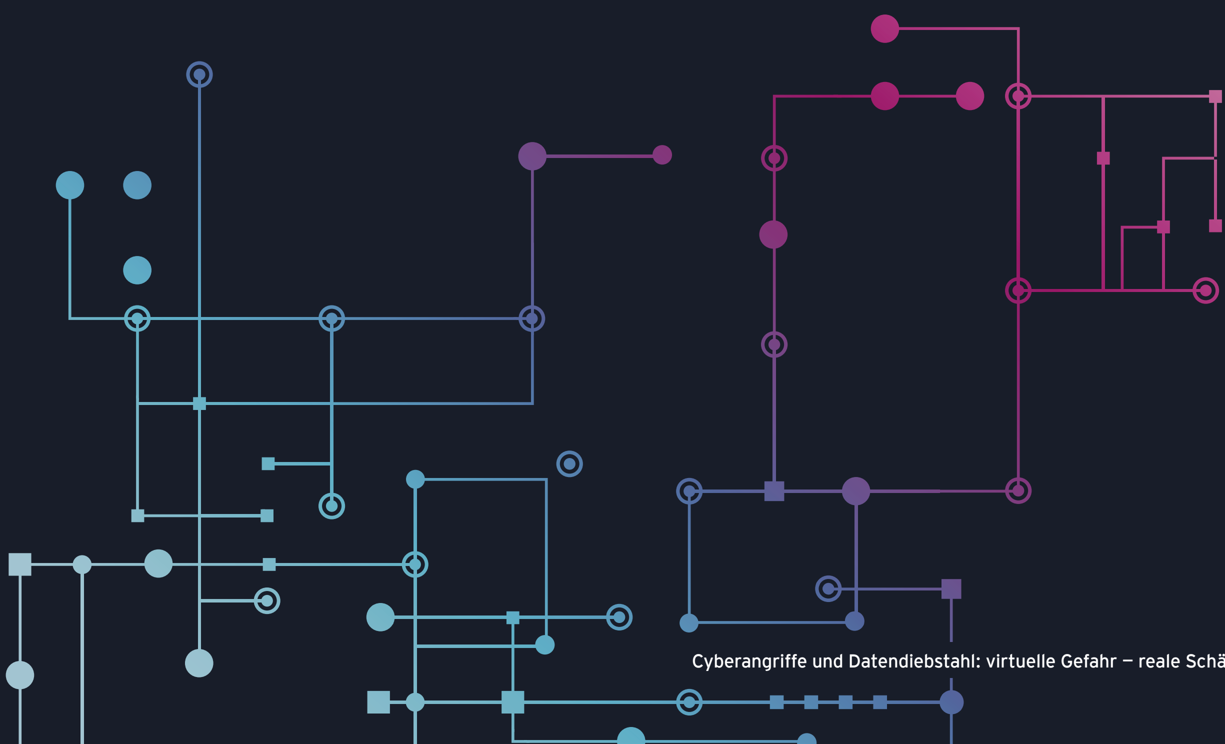
Aus der Praxis

Ransomware verwehrt Personen oder Unternehmen den Zugriff auf ihre Daten oder Systeme. Ziel dieses Angriffs ist es, anschließend Lösegeld zu erpressen. Die Konsequenzen dieser Attacke(n) sind aber weitreichender als gedacht, da durch die Verschlüsselung der Daten und IT-Systeme Ausfallzeiten in der Produktion auftreten können. Zudem kann ein Diebstahl personenbezogener Daten zu einer Verletzung der Datenschutz-Grundverordnung führen. Zudem müssen Unternehmen strenge Fristen bei Meldungen an den Datenschutz einhalten.

Im Jahr 2017 waren breit gestreute, hochgradig automatisierte Angriffe wie „WannaCry" an der Tagesordnung, begleitet von als Ransomware getarnten Sabotageangriffen wie „NotPetya". Heute werden Incident-Response-Teams vermehrt mit deutlich komplexeren Angriffsstrategien konfrontiert. Angriffsziele werden dabei über Wochen und Monate hinweg gezielt ausgespäht. Der tatsächliche Angriff erfolgt schnell und systematisch. Derzeit werden dabei auch unterschiedliche Strategien kombiniert. In einem jüngeren Fall wurden nicht nur kritische Unternehmensdaten verschlüsselt, sondern gleichzeitig sensible Daten gestohlen. Die folgenden Lösegeldforderungen für die Herausgabe der Kryptoschlüssel wurden dann durch die Androhung einer Veröffentlichung der gestohlenen Daten ergänzt. Zusätzlich werden nicht nur die Opfer selbst, sondern auch deren Kund:innen kontaktiert. Durch dieses Vorgehen erhoffen sich die Angreifer:innen eine höhere Quote an zahlenden Opfern. Der tatsächliche Schaden für das Unternehmen lag deutlich über der Forderung der Täter:innen.

Diese modernen Angriffsstrategien stellen Verantwortliche vor erhebliche Herausforderungen, da hierbei unterschiedlichste Methoden vom klassischen Hacking über maßgeschneiderte Malware bis hin zu Social Engineering eingesetzt werden. Psychologische Aspekte spielen dabei eine immer größere Rolle. Rein technische Sicherheitslösungen reichen nicht aus, Risikoszenarien müssen strategisch betrachtet und Maßnahmen ganzheitlich umgesetzt werden.

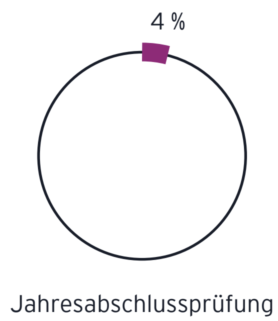
> ”
> Rein technische Sicherheitslösungen reichen nicht aus, Risikoszenarien müssen strategisch betrachtet und Maßnahmen ganzheitlich umgesetzt werden.



3.4 Wie wurden die kriminellen Handlungen aufgedeckt?

n=202, Prozentzahlen gerundet

Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachantworten möglich

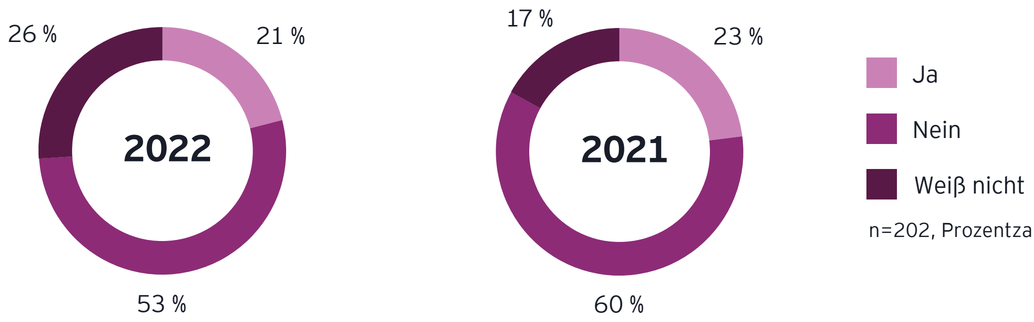


Wie schon 2021 werden Angriffe in den häufigsten Fällen durch das interne Kontrollsystem identifiziert. Durch interne Routineprüfungen wurden im Vergleich zum letzten Jahr (6 %) nun 11 % der Angriffe aufgedeckt. Die Dunkelziffer nicht aufgedeckter Angriffe wird höher sein, denn trotz interner Kontrollmechanismen und staatlicher Aktivitäten wird gut jeder fünfte Angriff rein zufällig aufgedeckt.

”

30 % aller Angriffe werden durch das interne Kontrollsystem erkannt.

Ist der Angriff außerhalb der Organisation, z. B. bei Kund:innen oder Geschäftspartner:innen, bekannt geworden?

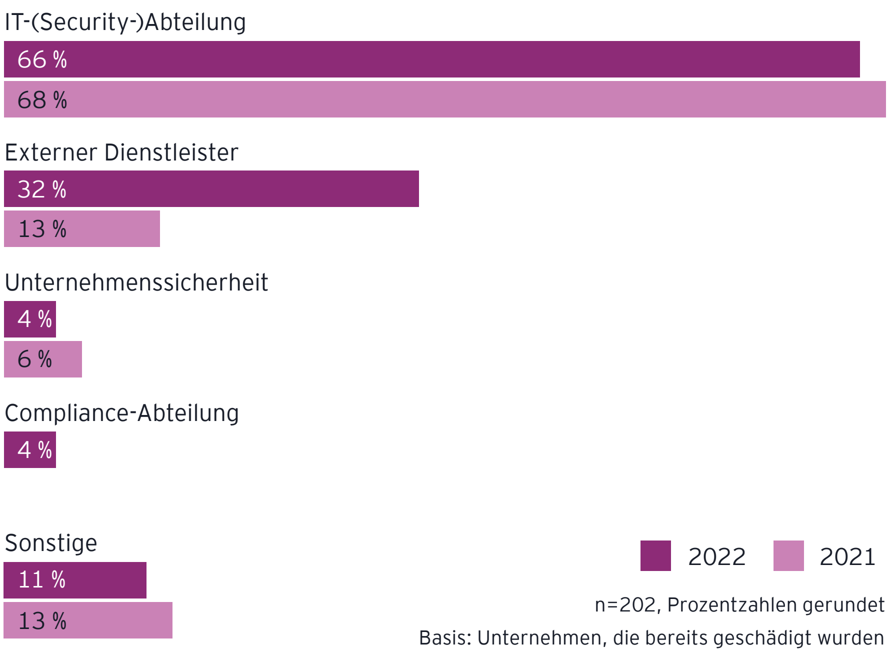


n=202, Prozentzahlen gerundet

3.5 Wer wurde mit der Aufklärung beauftragt?

> Aufklärer Nummer eins ist die eigene IT-Abteilung, aber: Es wird vermehrt auf externe Dienstleister gesetzt.

Wird ein Cyberangriff bekannt, ist die IT-Abteilung in 66 % der Fälle die erste Anlaufstelle. Im Vergleich zum letzten Jahr werden mehr externe Dienstleister von Unternehmen zur Aufklärung von Angriffen hinzugezogen. Die eigene Unternehmenssicherheit wird in knapp jedem 20. Fall mit der Aufklärung des Cyberangriffs beauftragt.



n=202, Prozentzahlen gerundet
Basis: Unternehmen, die bereits geschädigt wurden

EY ist eine

NIS-qualifizierte Stelle

Wir führen in sämtlichen Sicherheitskategorien NIS-Audits gemäß § 11 NISV durch

Was ist das NISG und welche Unternehmen sind davon betroffen?

Die europäische NIS-Richtlinie (Netz- und Informationssystemsicherheit) wurde Ende 2018 in das österreichische NISG (Netz- und Informationssystemsicherheitsgesetz) überführt. Ziel ist es, das Sicherheitsniveau für kritische Infrastruktur in Betrieben zu gewährleisten beziehungsweise zu erhöhen. Dazu wurden entsprechend strenge Sicherheitsauflagen für die betroffenen Unternehmen definiert.

Das NISG fordert die unverzügliche Meldung von Sicherheitsvorfällen, eine regelmäßige Überprüfung der kritischen Infrastrukturen und die Implementierung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen. Die Betreiber kritischer Dienstleistungen sind verpflichtet, dem Bundesministerium für Inneres mindestens alle drei Jahre entsprechende Prüfberichte vorzulegen. Das NISG bezieht sich in der Version 1.0 auf Betreiber wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur sowie auf Anbieter digitaler Dienste.

Durch die sich rasch ändernden Prämissen – Stichwort: erhöhte Cyberangriffe in der Pandemie – wurde von der Europäischen Kommission bereits die zweite Version der NIS-Richtlinie (NIS 2.0) erarbeitet. Im ersten Entwurf der NIS 2.0 wurden vor allem die betroffenen Sektoren genauer spezifiziert und durch acht zusätzliche erweitert – somit sind wohl durch die neue Regelung deutlich mehr Unternehmen in Österreich betroffen.

Was ist eine „qualifizierte Stelle“?

Die regelmäßige Überprüfung und die Nachweiserstellung (Prüfberichte) müssen durch akkreditierte „qualifizierte Stellen“ durchgeführt werden.

EY hilft als qualifizierte Stelle seinen Kunden mit fachlicher Expertise im Bereich Informationssicherheit bei der Absicherung ihrer IT-Netzwerke durch Beratung und Überprüfung aller vom NISG beziehungsweise von der NISV betroffenen Unternehmensbereiche:

1. Governance und Risikomanagement
2. Umgang mit Dienstleistern, Lieferanten und Dritten
3. Sicherheitsarchitektur
4. Systemadministration
5. Identitäts- und Zugriffsmanagement
6. Systemwartung und Betrieb
7. Physische Sicherheit
8. Erkennung von Vorfällen
9. Bewältigung von Vorfällen
10. Betriebskontinuität
11. Krisenmanagement

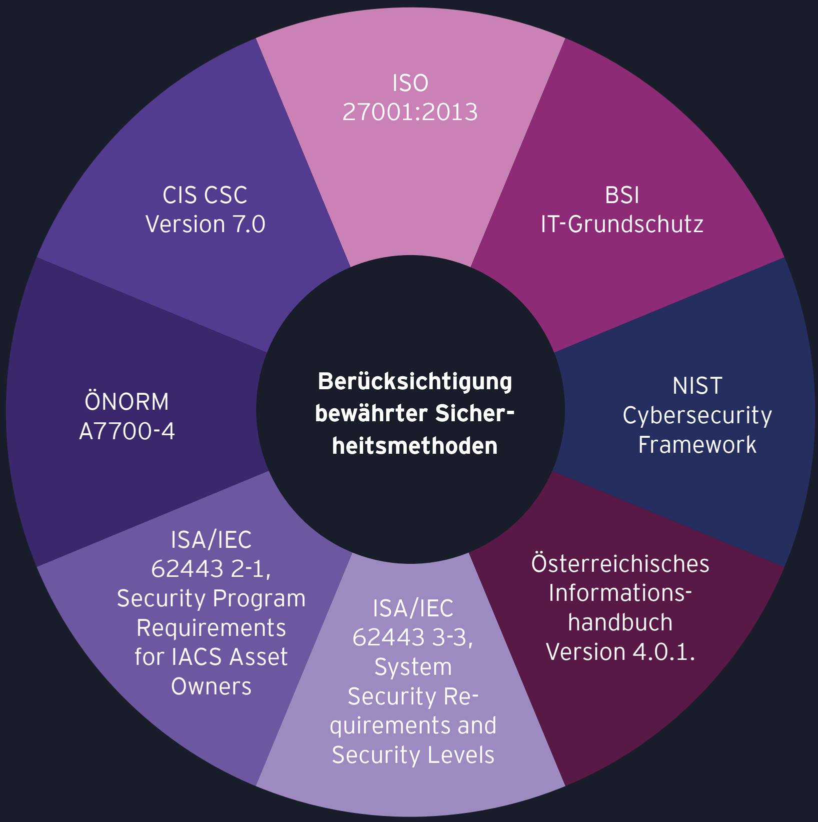
Ablauf einer Prüfung gemäß § 11 NISV

Phase 1:
Vorbereitung und Kick-off

Phase 2:
Prüfung der Sicherheitsmaßnahmen und Prozesse

Phase 3:
Berichterstellung und -erstattung

Integrierter Prüfungsansatz der NIS-Konformität mit Blick auf bewährte Sicherheitsstandards, Normen und Best-Practice-Erfahrungen:



Warum EY?

Um den hohen Anforderungen des NISG und der NISV gerecht zu werden, begleiten wir unsere Kunden entlang des gesamten Prozesses: von der Vorbereitung über die Beseitigung der identifizierten Sicherheitsmängel bis hin zur Prüfung in allen elf Kategorien.

Unsere langjährige Prüferfahrung und Expertise bei Zertifizierungsprozessen, beispielsweise bei ISMS (Information Security Management Systems) und DSGVO, sowie eine Vielzahl an Security-Fachleuten ermöglichen uns eine strukturierte Prüfung der geforderten Maßnahmen und Prozesse.

Dank unserer Expertise können wir die Anwendungen des NISG mit Blick auf die ISO 27001 prüfen. Inhaltlich fordern das NISG und die NISV großteils identische Sicherheitsmaßnahmen wie die internationale Norm für Informationssicherheit ISO 27001.

Wir unterstützen Sie bei folgenden Aufgaben:

- Maturity Assessment der bereits vorhandenen Sicherheitsmaßnahmen sowie Meldeprozesse und Definition der Handlungsfelder, um die Anforderungen des NISG zu erfüllen
- Erstellung einer Roadmap und Implementierung der identifizierten Handlungsfelder
- Durchführung der Prüfung gem. § 11 NISV und Erstellung einer detaillierten Auflistung potenzieller Sicherheitsmängel

Auf dem Weg zur Compliance das Rad nicht neu erfinden

Unsere langjährige Erfahrung in der Auswahl und Implementierung von Software-Tools im Security-Bereich hat uns gelehrt, wie wichtig digitale Integration ist. Neue regulatorische Anforderungen bergen das Risiko, neue, kostspielige Parallelstrukturen aufzubauen.

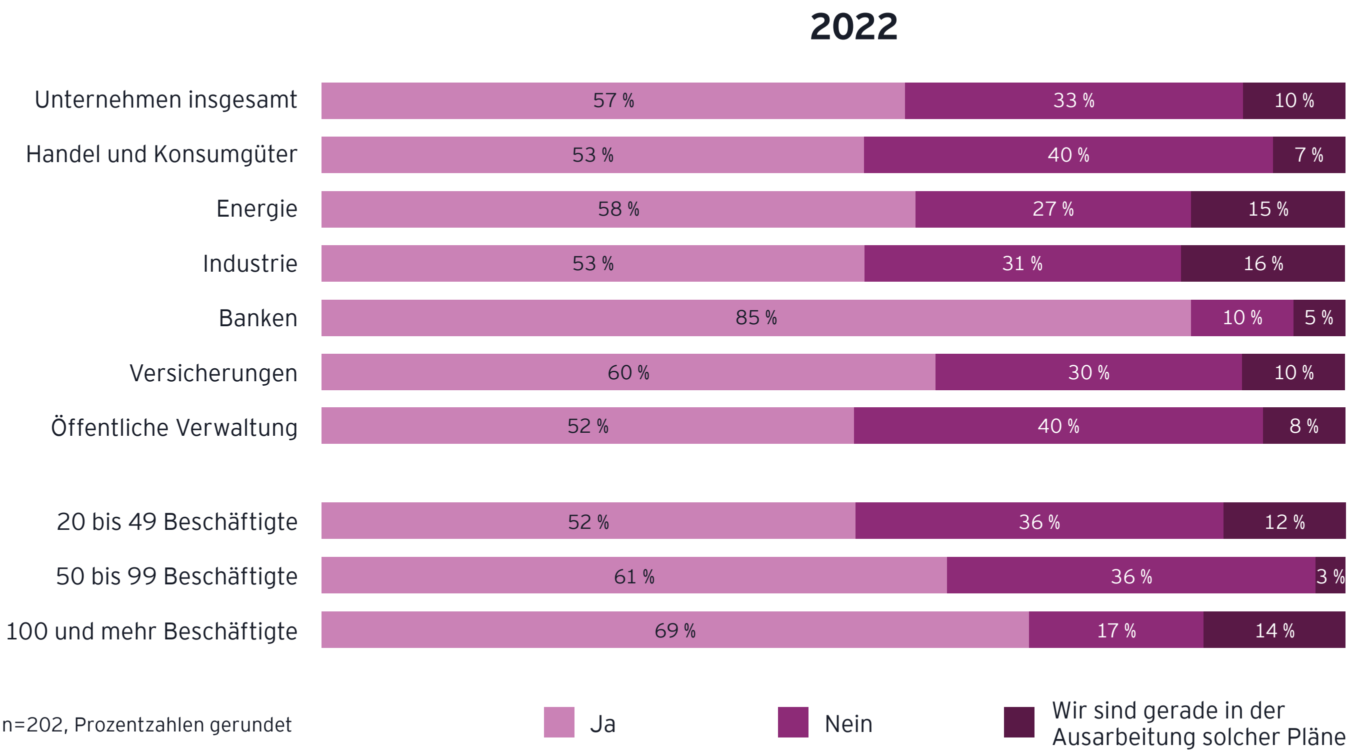
Um dem entgegenzuwirken, bieten wir die Auswahl, Einführung und Implementierung integrativer Software-Tools für die operative Umsetzung der NIS-Anforderungen.

Dabei berücksichtigen wir von Anfang an den zukünftigen Einsatz von NIS-Tools und richten unsere Handlungsempfehlungen an einer integrierten Umsetzung mit bestehenden Security-Prozessen aus.

4

Prävention, Abwehr und Aufklärung: Schützen sich die Unternehmen ausreichend?

4.1 Gibt es in Ihrem Unternehmen Krisenpläne zur Reaktion auf Cyberattacken?

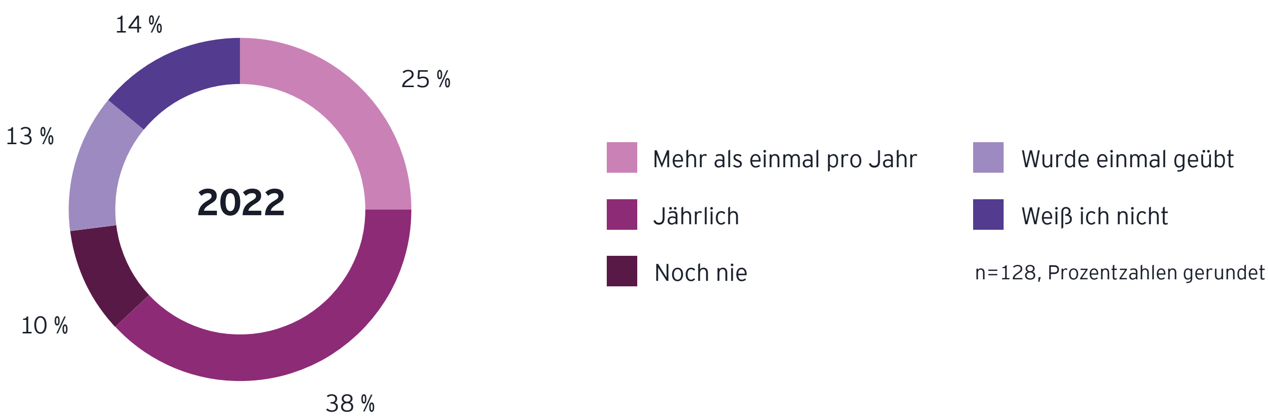


n=202, Prozentzahlen gerundet

”

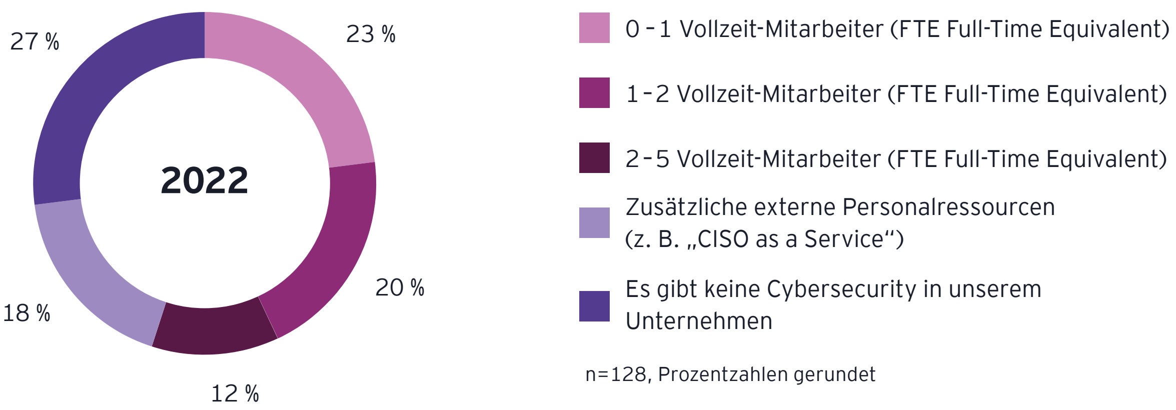
Mehr als die Hälfte der Unternehmen hat einen Krisenplan zur Reaktion auf Cyberattacken und übt diesen jährlich oder mehr als einmal pro Jahr.

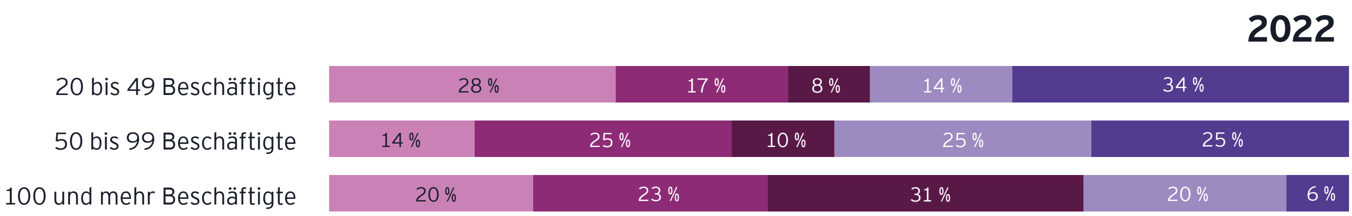
Wie häufig werden die Abläufe des Krisenplans geübt?



n=128, Prozentzahlen gerundet

4.2 Wie viele Personalressourcen intern stehen Ihnen generell im Bereich Cybersecurity zur Verfügung?



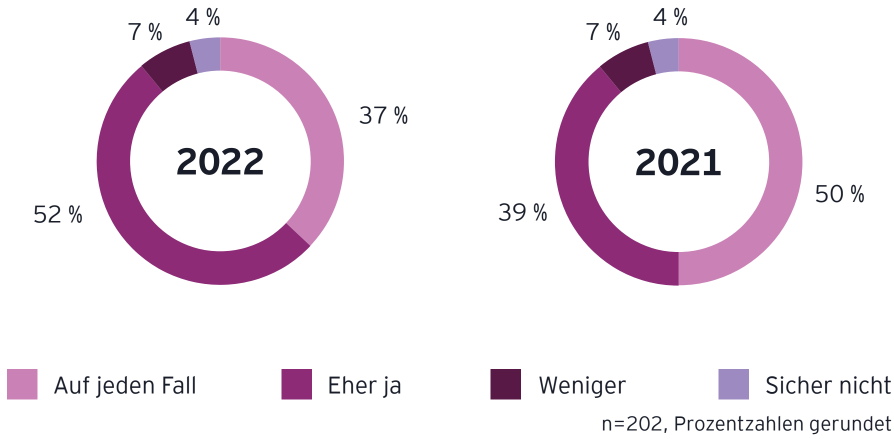


4.3 Sind aus Ihrer Sicht die präventiven Vorkehrungen im Unternehmen ausreichend, um sich wirkungsvoll gegen Informationsabfluss zu schützen?

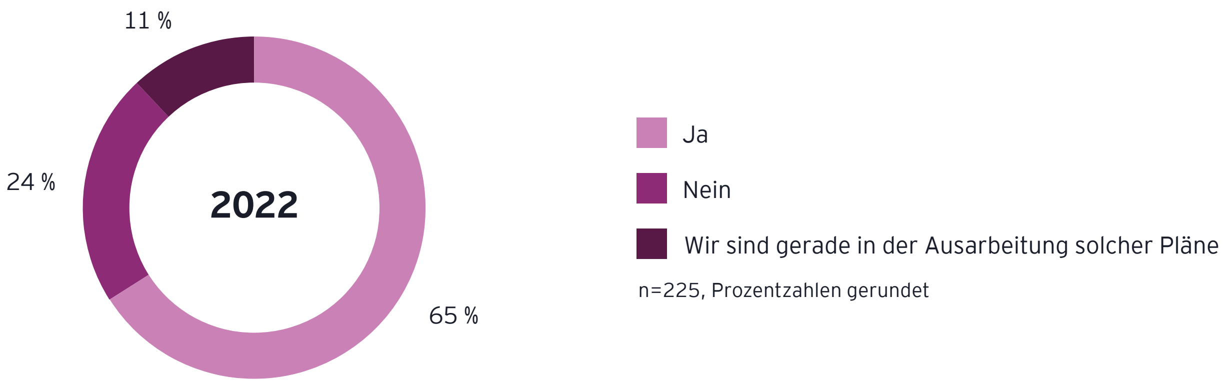
"

37 % der Unternehmen fühlen sich vollkommen sicher vor Cyberangriffen und Datendiebstahl – mehr als die Hälfte immerhin „eher" sicher.

Trotz der Bedrohung fühlen sich 52 % der Befragten zumindest eher gut vor Cyberangriffen und Datendiebstahl geschützt. Vollkommen ruhig schlafen können allerdings nur 37 % der Befragten. Jedes dritte Unternehmen hat nach eigener Aussage keine Krisenpläne zur Reaktion auf Cyberattacken. Die gefühlte Sicherheit ist bei Unternehmen aller untersuchten Branchen und Größen vergleichbar hoch.

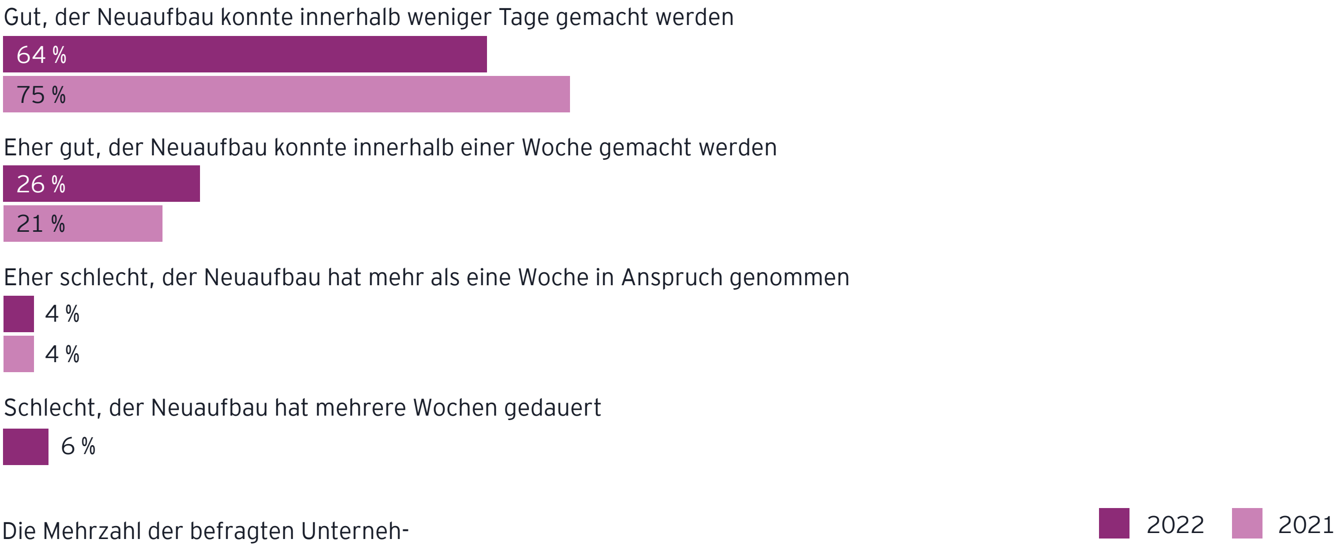


4.4 Gibt es in Ihrem Unternehmen Pläne für die Wiederherstellung der Infrastruktur nach einem Cyberangriff?



n=225, Prozentzahlen gerundet

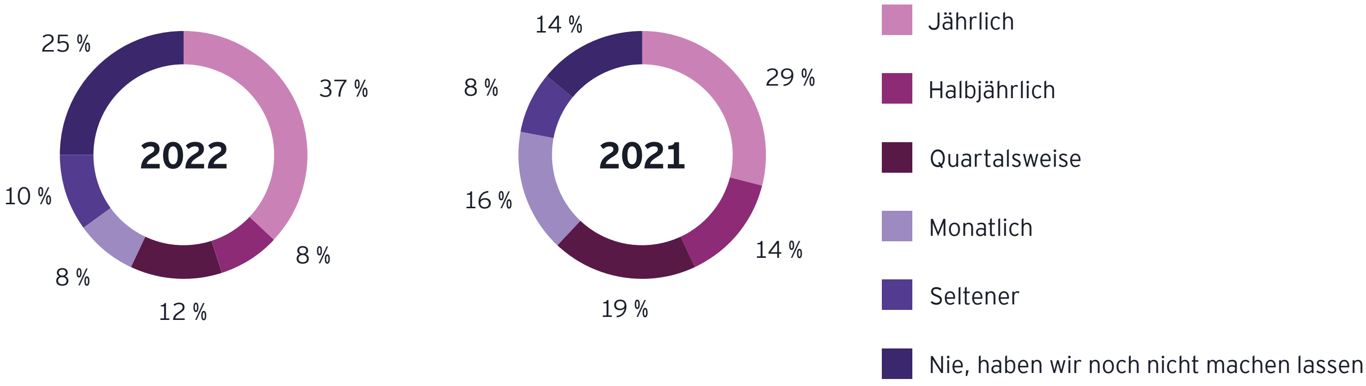
4.5 Wie ist die Wiederherstellung des Betriebs und der Sicherheit nach dem Angriff gelaufen?



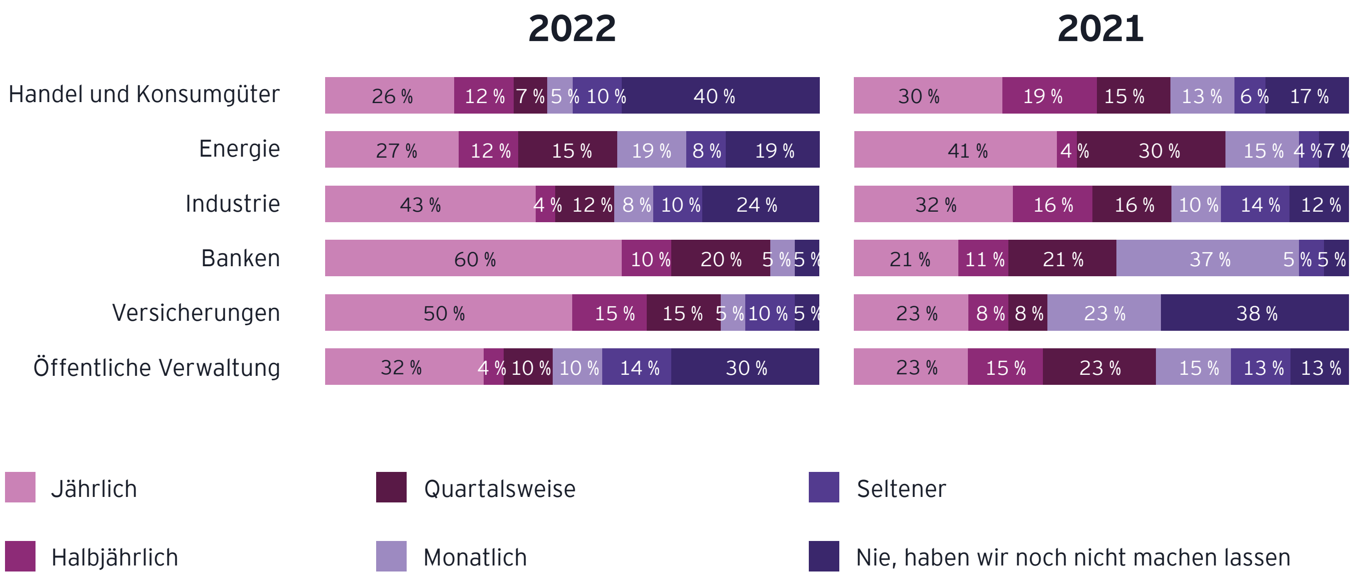
Die Mehrzahl der befragten Unternehmen (64 %) konnte den Betrieb und die Sicherheit innerhalb weniger Tagen wiederaufbauen.

n=202, Prozentzahlen gerundet
Basis: Unternehmen, die bereits geschädigt wurden

4.5 Lässt sich Ihr Unternehmen regelmäßig (extern und/oder intern) auf Schwachstellen im Hinblick auf Cyberangriffe/ Datendiebstahl testen?

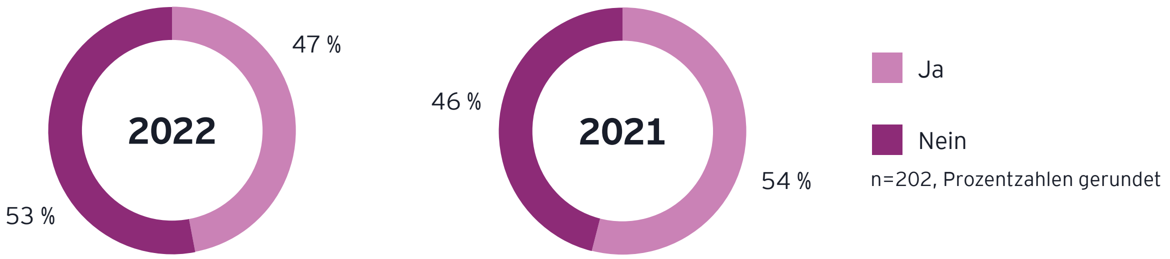


n=202, Prozentzahlen gerundet



n=202, Prozentzahlen gerundet

4.6 Hat Ihr Unternehmen eine Versicherung gegen digitale Risiken (Hackerangriffe etc.) abgeschlossen?

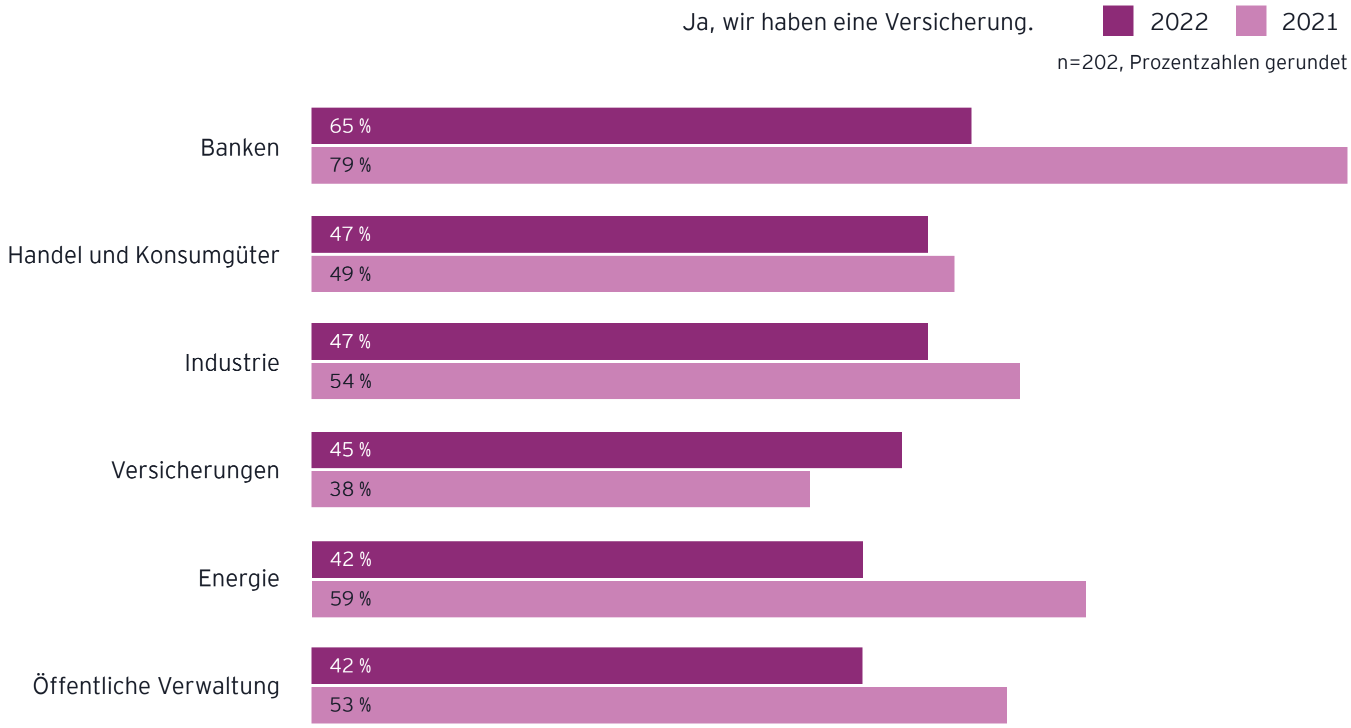


"

Weniger als die Hälfte der Unternehmen ist gegen digitale Risiken versichert.

Digitale Risiken sind für Unternehmen weiterhin nicht zu unterschätzen. Im Schadensfall können dabei Kosten in Millionenhöhe entstehen. Zum Schutz vor diesen schwerwiegenden Folgen schließen immer mehr Unternehmen Versicherungen gegen Cyberrisiken ab: 47 % der befragten Unternehmen haben inzwischen nach eigenen Angaben eine solche Versicherung abgeschlossen.

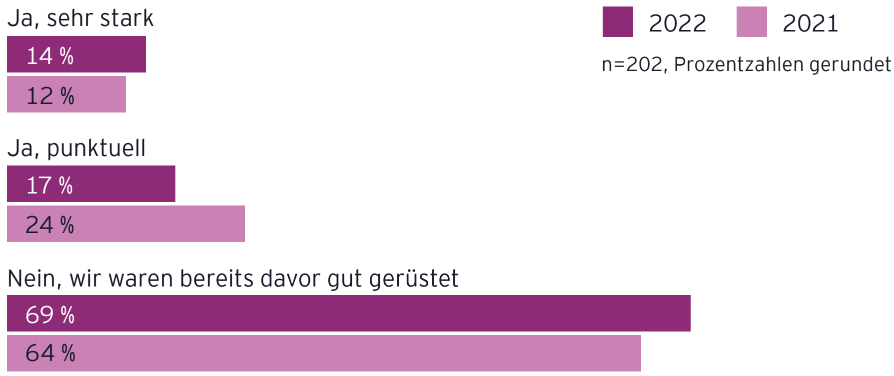
Besonders hoch ist der Anteil der Unternehmen mit Versicherungsschutz bei Banken, in der Handel- und Konsumgüterbranche und in der Industrie.



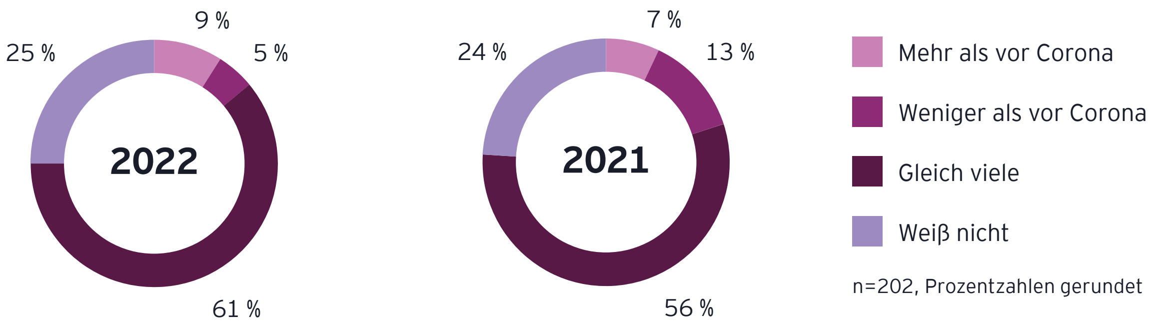
5 Auswirkungen der Coronapandemie

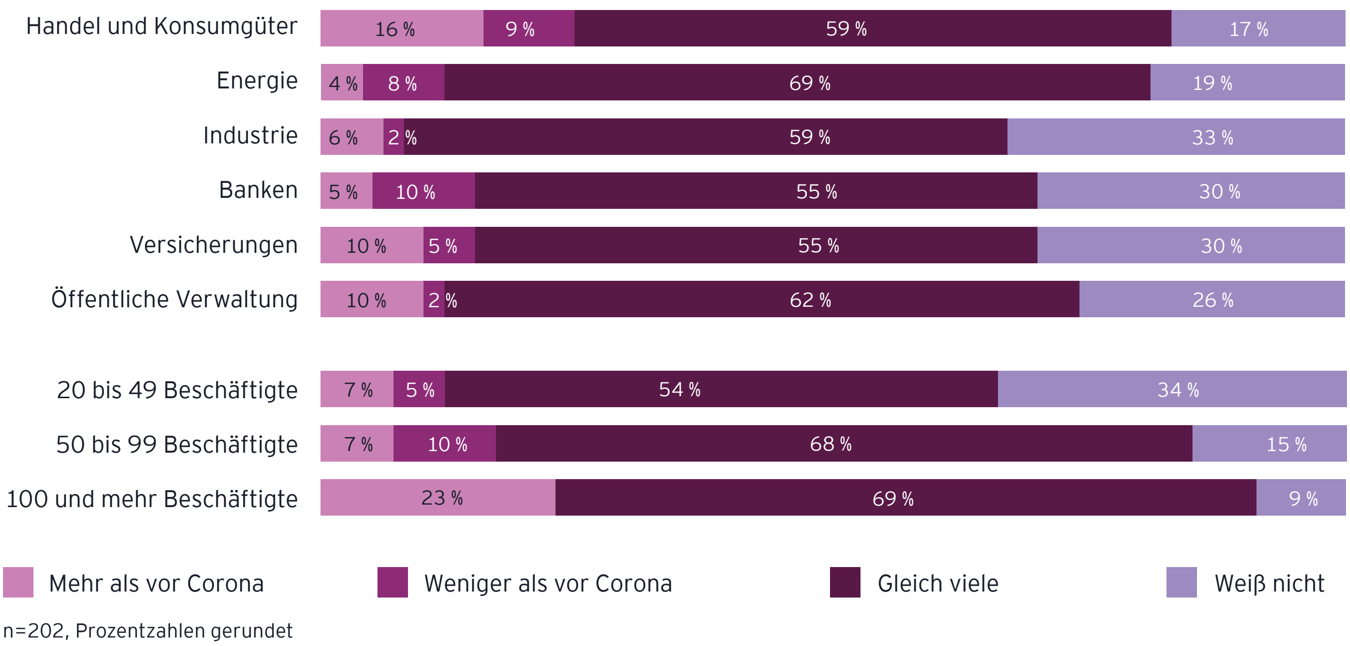
5.1 Haben Sie in der Folge der Coronakrise und des Lockdowns Ihre Cybersecurity-Maßnahmen verschärft?

Das Homeoffice kann für viele Unternehmen zum Risikofaktor werden: Neue Software musste installiert werden und private Laptops sind nicht mit derselben Software geschützt wie Firmen-PCs. Programme funktionieren nicht, IT-Mitarbeiter:innen versuchen, dies remote zu lösen, und dabei können Schwachstellen in der IT-Umgebung entstehen. Daher haben 17 % der Unternehmen ihre Cybersecurity-Maßnahmen punktuell verschärft, 14 % sogar sehr.

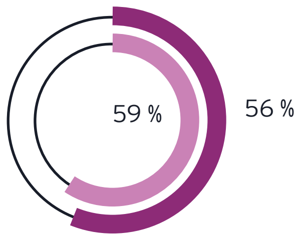


5.2 Haben Sie seit dem Ausbruch der Coronakrise und den damit verbundenen Maßnahmen wie vermehrtes Homeoffice eine Veränderung bei Security Incidents bzw. Cyberangriffen (z. B. Phising Mails, Spam festgestellt?

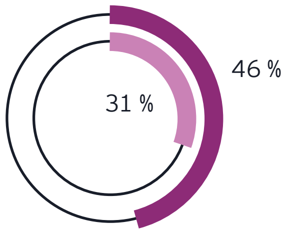




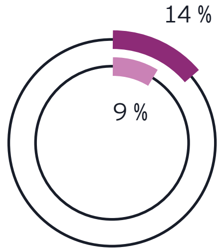
5.3 Wie haben die verstärkten Cybersecurity-Maßnahmen ausgesehen?



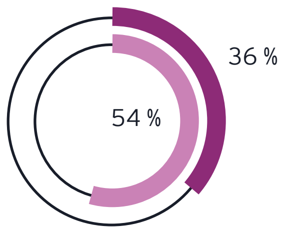
Sensibilisierung der Mitarbeiter:innen



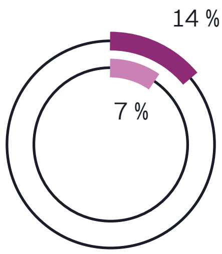
Verschärfung der Sicherheitsrichtlinien/-settings



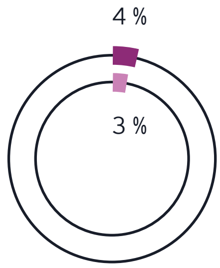
Papierloses Büro bis zum Umzug in die Cloud



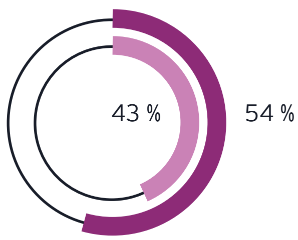
Neue organisatorische Regelung (Policies)



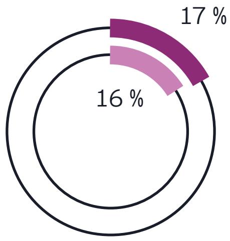
Prozessuale Anpassungen



Andere Maßnahmen



Modernisierung der IT-Infrastruktur (z. B. neue Tools/Überwachungsmechanismen)



Zusätzliche Software wie Mehrfaktorenauthentifizierung; Intrusion-Prevention-/-Detection-Systeme (Systeme, die Hackerangriffe erkennen/abwehren)

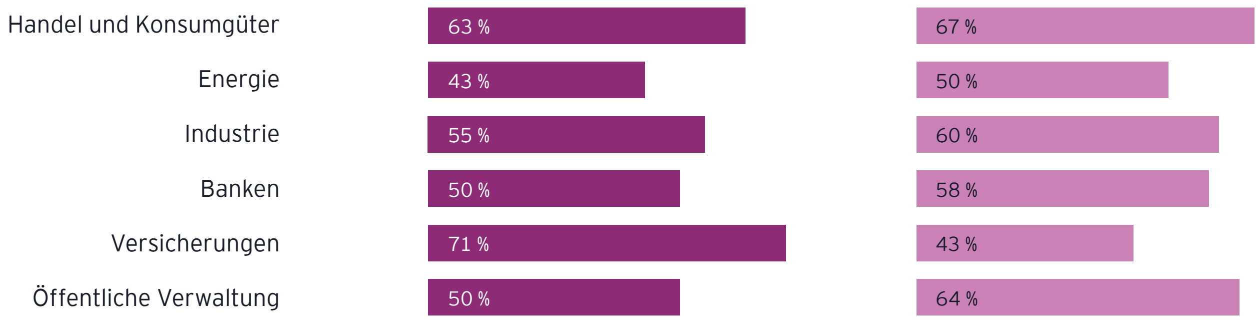
2022 2021

n=202, Prozentzahlen gerundet

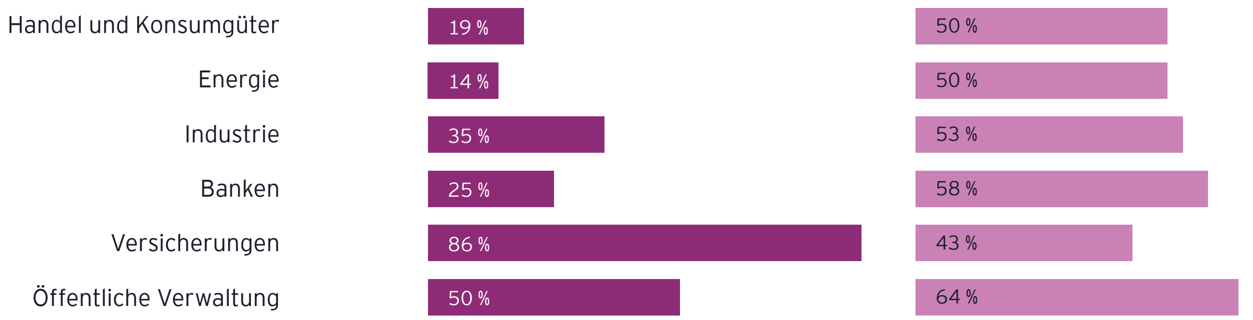
Um sich während der Coronakrise vermehrt zu schützen, hat mehr als die Hälfte (56 %) der befragten Unternehmen seine Mitarbeiter:innen sensibilisiert und seine IT-Infrastruktur modernisiert (54 %). Außerdem hat mehr als jedes dritte Unternehmen neue organisatorische Regelungen aufgesetzt (36 %).

> Mehr als jedes zweite Unternehmen hat seine Mitarbeiter:innen während der Coronakrise sensibilisiert und seine IT-Infrastruktur modernisiert.

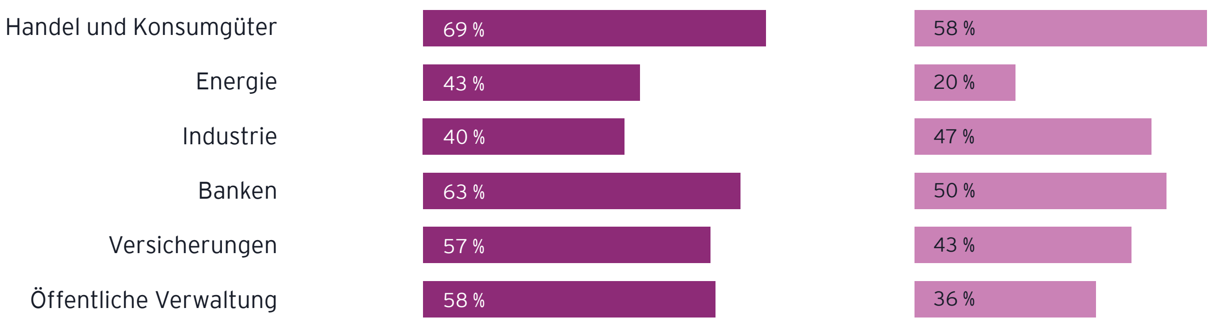
Sensibilisierung von Mitarbeiter:innen



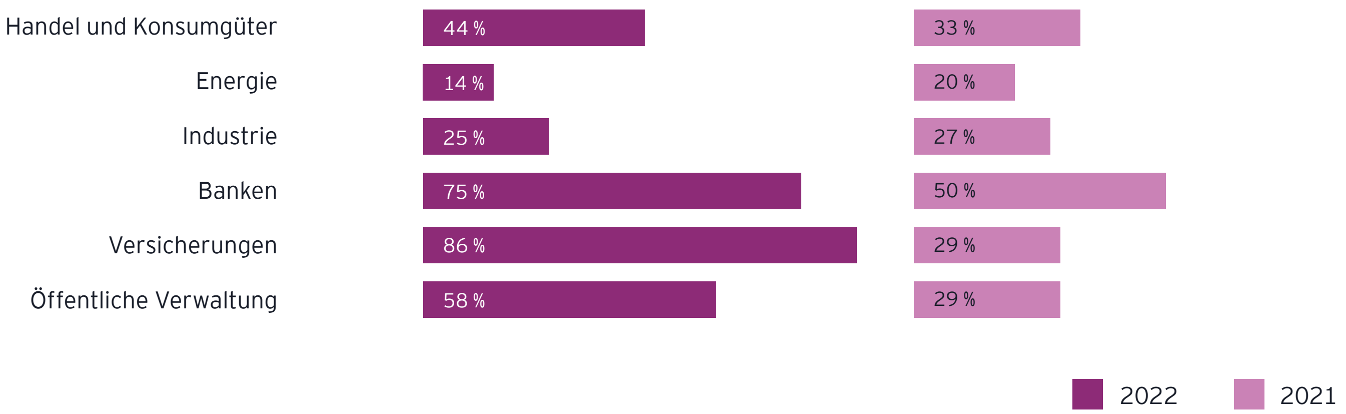
Neue organisatorische Regelungen (Policies)



Modernisierung der IT-Infrastruktur (z. B. neue Tools/Überwachungsmechanismen)



Verschärfung der Sicherheitsrichtlinien/-settings



n=202, Prozentzahlen gerundet

Prozessuale Anpassungen

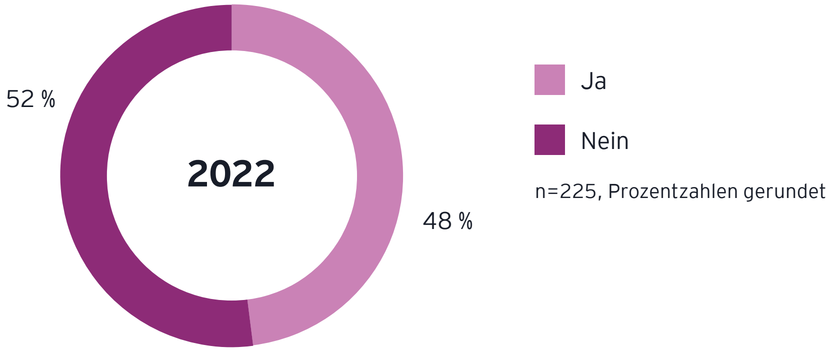
Zusätzliche Software wie Mehrfaktorauthentifizierung; Intrusion-Prevention-/-Detection-Systeme (Systeme, die Hackerangriffe erkennen/abwehren)

Papierloses Büro bis zum Umzug in die Cloud

Andere Maßnahmen

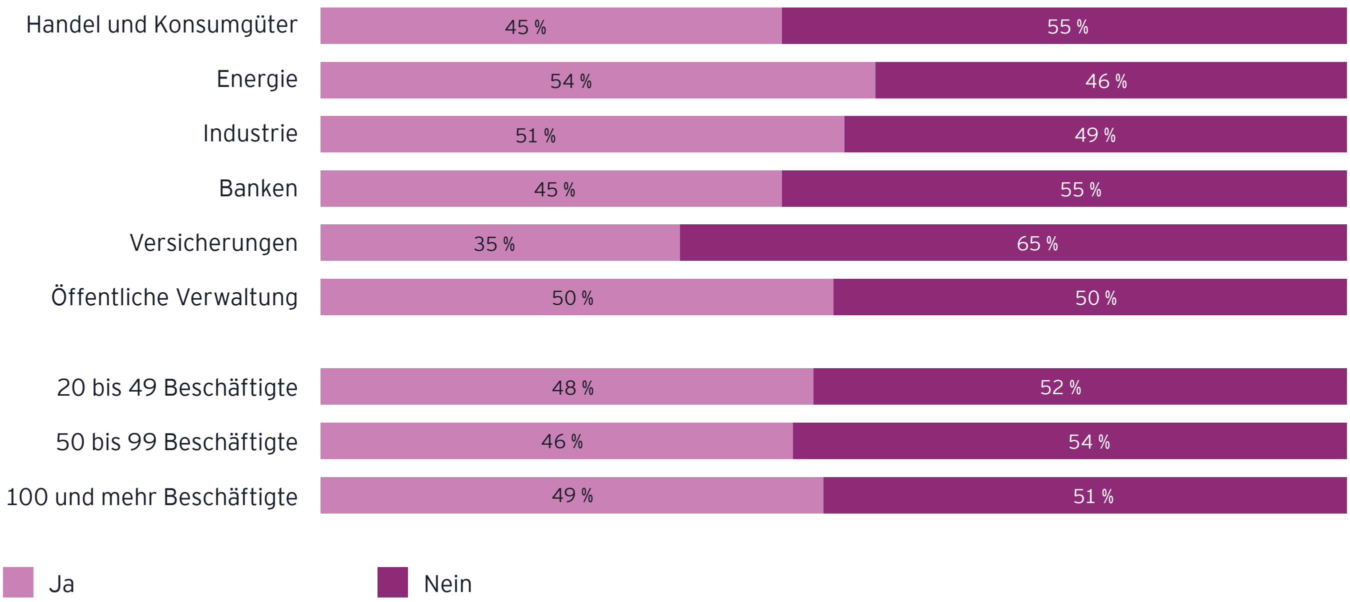
2022 2021 n=202, Prozentzahlen gerundet

5.4 Haben Sie Cloud Services im Einsatz?



n=225, Prozentzahlen gerundet

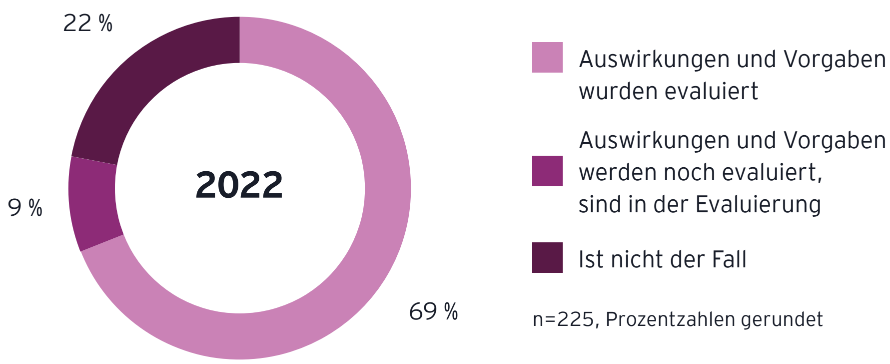
In den letzten Jahren wurde im Rahmen der Digitalisierung die Cloud-Technologie immer wichtiger. Aus der Befragung geht hervor, dass fast jedes zweite Unternehmen (48 %) Cloud Services im Einsatz hat.



n=202, Prozentzahlen gerundet

5.5 Haben Sie beim Einsatz von Cloud Services die Datenschutz- und Datensicherheitsauswirkungen evaluiert?

Das Thema Security ist beim Einsatz von Cloud Services von besonderer Bedeutung. Unternehmen bleiben fachliche Eigner und haben Datenschutz, Zugriffsschutz, Risikomanagement etc. sicherzustellen. 69 % aller befragten Unternehmen haben die Datenschutz- und Datensicherheitsauswirkungen evaluiert.



n=225, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Handel und Konsumgüterindustrie

„Wo sensible und persönliche Daten von Konsument:innen im Spiel sind, muss Cybersicherheit gewährleistet werden. Das trifft besonders auf den Handel und die Konsumgüterindustrie zu.

Martin Unger
Leiter Konsumgüter und Handel bei EY Österreich und Leiter EYCarbon

Gefahrenpotenzial

26 % schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

74 % erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (17 %), Personal (17 %) und Vertrieb (8 %)

22 % entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

7 % wurden mehrfach Opfer von Angriffen

9 % wurden bereits erpresst

Prävention

31 % sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

47 % haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

16 % geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

69 % konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

17% haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=58, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Industrie

„Lahmgelegte Produktionsanlagen, gestohlene Patente, geleakte Finanzen: Damit Industriebetriebe lieferfähig bleiben, müssen sie sich gegen die Gefahren aus dem Netz ausreichend schützen."

Axel Preiss
Leiter Consulting und Advanced Manufacturing & Mobility bei EY Österreich und Europe West

Gefahrenpotenzial

28 % schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

65 % erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurden: Vertrieb (44 %), Finanzwesen (31 %), Management sowie Forschung und Entwicklung (jeweils 19 %)

8 % entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

12 % wurden mehrfach Opfer von Angriffen

8 % wurden bereits erpresst

Prävention

22 % sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

47 % haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

6 % geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

69 % konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

12 % haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=51, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Energie

„Energie wird immer digitaler - und damit auch angreifbarer für Cyberattacken. Werden Smart Meter gehackt, folgt das Blackout. Cybersecurity ist für Energieversorger daher essenziell."

Christina Khinast
Leiterin Energy & Resources bei EY Österreich

Gefahrenpotenzial

35 %
schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

77 %
erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurden: Forschung und Entwicklung (25 %), Finanzwesen (13 %) und Fertigung (13 %)

19 %
entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

8 %
wurden mehrfach Opfer von Angriffen

12 %
wurden bereits erpresst

Prävention

35 %
sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

42 %
haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

4 %
geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

43 %
konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

4 %
haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=26, Prozentzahlen gerundet

Spot on Sector

Die wichtigsten Ergebnisse

Öffentliche Verwaltung

„Kriege wandern immer mehr in den Cyberspace, wie auch die zahlreichen Cyberattacken im Zuge des Ukraine-Kriegs zeigen. Die öffentliche Verwaltung muss sich darauf vorbereiten.

Christoph Harreither
Leiter Government & Public Sector bei EY Österreich

Gefahrenpotenzial

32 % schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

88 % erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (50 %), Personalwesen (33 %) und Management (17 %)

18 % entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

2 % wurden mehrfach Opfer von Angriffen

12 % wurden bereits erpresst

Prävention

56 % sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

42 % haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

10 % geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

58 % konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

14 % haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=50, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Banken

"Wo Geld im Spiel ist, sind auch Kriminelle nicht weit. Banken verwalten täglich Tausende Transaktionen. Diese richtig zu schützen muss immanenter Bestandteil der Dienstleistung sein."

Armin Schmitt
Leiter Banking bei EY Österreich

Gefahrenpotenzial

40 % schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

85 % erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurde: Finanzwesen (50 %)

16 % entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

7 % wurden mehrfach Opfer von Angriffen

5 % wurden noch nicht erpresst

Prävention

50 % sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

65 % haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

5 % geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

75 % konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

25 % haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=20, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Versicherungen

„Versicherer müssen sich nicht nur selbst gegen Cyberattacken schützen, sondern können darin auch eine Chance für das Portfolio sehen und entsprechende Versicherungsprodukte anbieten.

Ali Aram
Leiter Versicherungen bei EY Österreich

Gefahrenpotenzial

25 % schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

70 % erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (50 %) und Vertrieb (50 %)

10 % entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

5 % wurden nicht mehrfach Opfer von Angriffen

5 % wurden noch nicht erpresst

Prävention

85 % sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

45 % haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

10 % geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

86 % konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

25 % haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2022 n=20, Prozentzahlen gerundet

Fazit und Ausblick

Cyberangriffe werden in Zukunft weiter zunehmen, darüber sind sich alle einig: Die überwiegende Mehrheit der Unternehmen in Österreich (76 %) geht davon aus, dass die Gefahren durch Cyberangriffe oder Datendiebstahl in Zukunft steigen werden. Expert:innen bestätigen diesen Trend, der durch die fortschreitende Digitalisierung und durch vermehrtes Homeoffice in Zeiten der Pandemie in allen Bereichen begünstigt wird. Die Digitalisierung bietet der Cyberkriminalität ein beinahe grenzenloses Wachstums- und Schadenspotenzial. Während der Pandemie haben 17 % der Unternehmen ihre Cybersecurity-Maßnahmen verschärft, 14 % sogar sehr. Um sich zu schützen, haben mehr als die Hälfte (56 %) der befragten Unternehmen ihre Mitarbeiter:innen sensibilisiert und ihre IT-Infrastruktur modernisiert (54 %). Außerdem hat mehr als ein Drittel der Unternehmen auch neue organisatorische Regelungen aufgestellt (36 %).

Die gute Nachricht: Das Gefahrenbewusstsein der Unternehmen ist inzwischen hoch. Knapp ein Drittel von ihnen sieht ein (erhöhtes) Risiko, selbst Opfer von Cyberangriffen und Datendiebstahl zu werden. Nicht zu Unrecht, denn 23 % der Befragten haben laut eigenen Angaben in den letzten fünf Jahren einen Angriff auf ihr Unternehmen entdeckt – die Dunkelziffer ist deutlich höher.

Aber: Trotz der zunehmenden Gefahr durch Cyberkriminalität fühlen sich die meisten Unternehmen gut abgesichert. Immerhin 37 % der Unternehmen fühlen sich vollkommen sicher vor Cyberangriffen und Datendiebstahl. Mehr als die Hälfte der Unternehmen fühlt sich „eher" sicher.

Es werden definitiv zu wenig Cyberkriminelle gefasst und noch immer werden viele Vorfälle nur zufällig entdeckt: In 30 % der Unternehmen griff das interne Kontrollsystem und deckte die kriminellen Handlungen auf. 19 % der befragten Unternehmen gaben an, dass kriminelle Handlungen nur durch Zufall aufgedeckt worden seien. Die Dunkelziffer der tatsächlich erfolgten Cyberangriffe dürfte demnach deutlich höher sein. Auch bleiben die Verantwortlichen meist unerkannt.

Ob die Unternehmen für die künftigen Herausforderungen gewappnet sind, ist fraglich. Ein wichtiger Schritt in die richtige Richtung wäre es, die Investitionen in eine erfolgreiche Cyberabwehr zu erhöhen und wirkungsvolle Maßnahmen für das Sicherheitsbewusstsein in allen Unternehmensbereichen umzusetzen. Auf dem Spiel stehen letzten Endes insbesondere auch wertvolle Kund:innendaten – denn darauf haben es die Täter:innen vermehrt abgesehen. Für manche Organisationen bedeutet dies eine kontinuierliche Verbesserung bestehender Maßnahmen, für andere vielleicht sogar eine komplette Neuausrichtung.

In jedem Fall ist es wichtig und notwendig, ein systematisches und umfassendes Vorgehen zur Prävention und zum Umgang mit Krisensituationen zu etablieren und sich die entsprechenden externen Hilfen zu holen.

”

Es gilt schließlich, der Gefahr durch Cyberkriminalität auf Augenhöhe begegnen zu können, um das eigene Unternehmen weiter auf Kurs zu halten.
Die Verantwortlichen sollten sich definitiv auf stürmische Gewässer einstellen!

Digitalisierung hat ihre Tücken

Passgenaue Lösungen sind gefragt

Wir liefern die Antworten auf dringende Fragen

EY ist seit vielen Jahren ein weltweit führender Anbieter für Cybersicherheit sowie für digitale Forensik und Investigation und bündelt die Kompetenzen eines globalen Netzwerks. In fast jedem Land der Welt sind unsere Projektteams rund um die Uhr für Sie einsatzbereit. Ganz nach Ihren individuellen Bedürfnissen und für konkrete Aufgabenstellungen stehen Ihnen Branchenkenner:innen und Fachleute für ausgewählte Themenbereiche zur Verfügung. So treffen etwa IT-Berater:innen und Security-Fachleute auf Fachmitarbeiter:innen aus den klassischen EY-Bereichen Wirtschaftsprüfung, Steuer- und Rechtsberatung, aber auch auf Kriminalist:innen und Soziolog:innen.

Die über 7.200 global vernetzten Cyberprofessionals von EY, unterstützt durch zwölf weltweit verteilte Security-Center, betrachten Risiken aus wirtschaftlicher und geopolitischer Perspektive. Dies verhilft Ihnen zu einem realistischen und umfassenden Risikoverständnis, auf dessen Basis Sie intelligente und zukunftssichere Entscheidungen treffen können.

Transparenz, Integrität und Effizienz – darum muss es bei der Prävention, der Detektion und der Reaktion in Bezug auf Krisensituationen gehen. Dafür stehen unsere Leistungen und darauf zielen sie ab, ganz gleich ob wir dabei Routinetätigkeiten übernehmen oder Sie aktiv bei der Abwehr von Angriffen unterstützen.

Krisen managen, Vertrauen stärken

Zur Etablierung eines erfolgreichen Krisenmanagements helfen wir Ihnen, krisenmanagementrelevante Risiken zu identifizieren und zu bewerten. Unsere Fachleute erstellen gemeinsam mit Ihnen geeignete Präventionskonzepte, bauen eine effektive Krisenmanagementorganisation auf und qualifizieren Ihre Funktions- und Entscheidungsträger:innen. Unser Ziel ist es, Risiken zu minimieren, Ihre Krisenfestigkeit zu erhöhen, Ihnen im Ernstfall Stabilität zu geben und Vertrauen aufzubauen. Wir möchten, dass Sie auf unerwartete Ereignisse mit Schadenspotenzial schnell und effektiv reagieren können und sich so Wettbewerbsvorteile sichern. Außerdem beraten wir Sie natürlich auch umfassend während und nach konkreten Krisenereignissen.

Jede unserer Leistungen hat das Ziel, Antworten auf dringende Fragen rund um Cybersecurity und Krisenmanagement zu finden. Folgende Fragen sollten Sie sich stellen:

- Sind wir ausreichend vorbereitet, um gegen die zunehmenden Cyberbedrohungen zu bestehen?
- Ist unsere Cybersicherheitsstrategie zukunftsfähig?
- Sind die persönlichen Daten unserer Kund:innen, aber auch unser Kern-Know-how geschützt?
- Was geht wirklich in unseren Netzwerken vor?
- Wie können wir das Krisenpotenzial von Ereignissen und Entwicklungen schnell erkennen und analysieren?
- Was sind erste Schritte und Maßnahmen für eine rasche Krisenreaktion?
- Wie wird ein systematisches Informationsmanagement betrieben?
- Wie können bei Unsicherheit und hohem Zeit- und Handlungsdruck Entscheidungen getroffen werden?

Die Cybersecurity- und Krisenmanagement-Services von EY im Überblick

- Strategy, Risk & Resilience
- Security Strategy, Design & Roadmap
- Security Transformation
- Cybersecurity Workshops
- Management of Security Campaigns
- Digital Identity & Access
- IAM Strategy, Governance & Roadmap
- Access Controls & Management
- Breached Credential Scans
- Privileged Access Management
- Crisis Management & Communication
- Crisis Risk Assessment
- Pre-Crisis Preparation
- Crisis Management PMO* (*Project Management Office)
- Crisis Communication
- Data Security & Privacy
- Data Protection Strategy & Roadmap
- Secure Development Lifecycle Management
- Encryption (Anonymization, Pseudonymization)
- Application Security Testing
- Endpoint & Infrastructure Protection
- Endpoint & Malware Protection
- Mobile Device & Network Security
- SAP Security
- Container Security

Sicherheit für Ihr digitales Business

Damit das Vertrauen Ihrer Kund:innen, Mitarbeiter:innen und Partner:innen erhalten bleibt, helfen wir Ihnen, sich gegen neue und wiederkehrende Cyberbedrohungen zu schützen. Durch unsere integrierten Lösungen können wir Ihre digitale Transformation maßgeblich unterstützen.

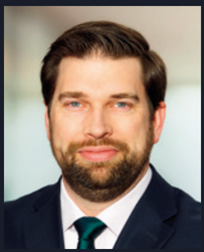
Wir beraten Sie passgenau in allen Fragen zur Cybersicherheit und zum Krisenmanagement – von der Bestandsaufnahme bis hin zur Planung, Umsetzung und Optimierung.

Ansprechpartner

Autoren

Gottfried Tonweber
Leiter Cybersecurity &
Data Privacy EY Österreich

+43 1 21170 1145
gottfried.tonweber@at.ey.com



Bernhard Zacherl
Director Cybersecurity &
Data Privacy EY Österreich

+43 1 21170 1404
bernhard.zacherl@at.ey.com

Birgit Eschinger
Senior Manager Cybersecurity &
Data Privacy EY Österreich

+43 732 790790 5554
birgit.eschinger@at.ey.com

Thomas Steiner
Director Cybersecurity
EY Österreich

+43 1 21170 1120
thomas.steiner@at.ey.com

Ermano Geuer
Leiter Corporate Law
EY Law Österreich

+43 1 26095 2119
ermano.geuer@eylaw.at

Robert Pölzelbauer
Leiter Cyberforensik
EY Österreich

+43 1 21170 1124
robert.poelzelbauer@at.ey.com

Sektorenleiter

Ali Aram
Sector Leader Versicherungen
EY Österreich

+43 1 21170 1149
ali.aram@at.ey.com

Christoph Harreither
Sector Leader Government & Public
EY Österreich

+43 1 21170 1171
christoph.harreither@at.ey.com

Martin Unger
Sector Leader Handel und Konsumgüter EY Österreich, Leiter Strategieberatung Contrast EY Parthenon

+43 1 21170 1845
martin.unger@parthenon.ey.com

Armin Schmitt
Sector Leader Financial Services
EY Österreich

+43 1 21170 1717
armin.schmitt@at.ey.com

Axel Preiss
Sector Leader Advanced Manufacturing & Mobility, Leiter Consulting
EY Österreich

+43 1 21170 1722
axel.preiss@at.ey.com

Christina Khinast
Sector Leader Energy & Resources
EY Österreich

+43 732 790790 5002
christina.khinast@at.ey.com

Impressum:

Eigentümer, Herausgeber und Medieninhaber:
Ernst & Young Wirtschaftsprüfungsgesellschaft
m. b. H. („EY“), 1220 Wien
Inhaltliche Gesamtverantwortung: Gottfried Tonweber, Bernhard Zacherl, Birgit Eschinger und Thomas Steiner
Redaktion: Sarah Mauracher, Nina Eggenberger
Lektorat: Text+Design Jutta Cram
Design: Tanja Maria Schallert, Larissa Jusanovic
Bildmaterial: Gettyimages, Eva Kelety, EY Österreich

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie die Nutzung von Daten und modernsten Technologien bei der Erbringung unserer Dienstleistungen.

Ob Wirtschaftsprüfung (Assurance), Steuerberatung (Tax), Strategie- und Transaktionsberatung (Strategy and Transactions) oder Unternehmensberatung (Consulting): Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

Das internationale Netzwerk von EY Law, in Österreich vertreten durch die Pelzmann Gall Größ Rechtsanwälte GmbH, komplettiert mit umfassender Rechtsberatung das ganzheitliche Service-Portfolio von EY.

„EY“ und „wir“ beziehen sich in dieser Publikation auf alle österreichischen Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Mandanten. Informationen darüber, wie EY personenbezogene Daten sammelt und verwendet, sowie eine Beschreibung der Rechte, die Einzelpersonen gemäß der Datenschutzgesetzgebung haben, sind über ey.com/privacy verfügbar. Weitere Informationen zu unserer Organisation finden Sie unter ey.com.

In Österreich ist EY an vier Standorten präsent.

LJU 2208-000
ED None

ey.com/at