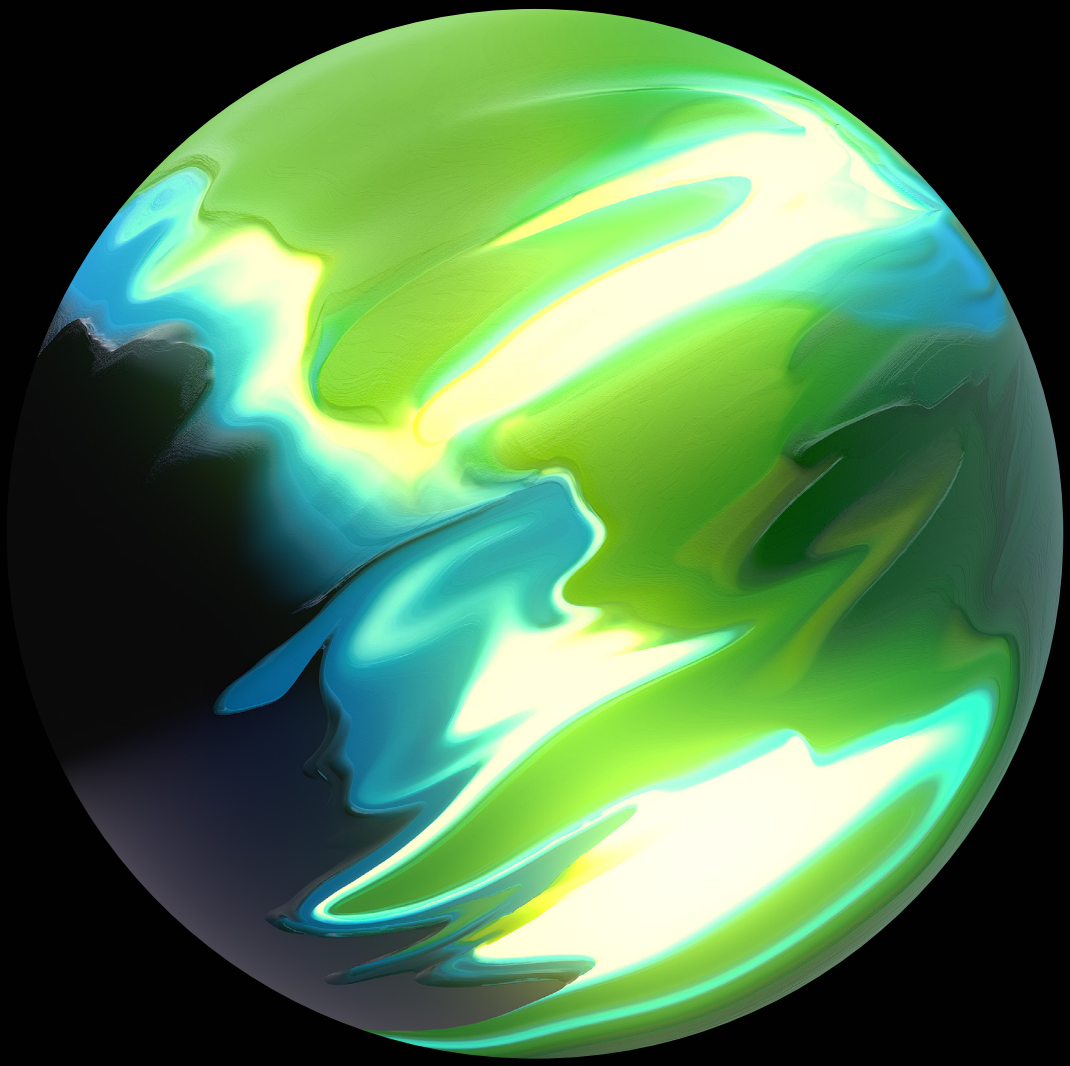
Deloitte.



Deloitte Cyber Security Report 2022

Wie österreichische Unternehmen mit steigenden Cyber-Bedrohungen umgehen

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, Tamara Spiegel und Maria Hofer
Grafik und Layout: Claudia Hussovits

Vorwort

Viele Unternehmen mussten sich aufgrund der COVID-19-Pandemie völlig neu aufstellen und haben einen Digitalisierungs-Boost erlebt. Alle Beschäftigten in Österreich haben viele Veränderungen mitgetragen, zentrale Stichworte im Arbeitskontext sind hier Remote und Hybrid Working.

Corona hat generell die Arbeits- und Lebensumstände der Menschen verändert. Durch den Angriffskrieg Russlands gegen die Ukraine wurde unfassbares menschliches Leid ausgelöst, gleichzeitig haben die ohnehin schon hohen Cyber-Angriffe gegen Unternehmen an Intensität gewonnen.

All diese Entwicklungen und Krisen haben eines gemein: Sie bringen auch neue Bedrohungen für die Cyber-Sicherheit mit sich.

Unsere Studie zeigt: Es gab noch nie so viele Cyber-Attacken wie heute.

Doch wie gut sind Österreichs Unternehmen für diese zunehmenden Cyber-Bedrohungen gewappnet? Wie sehr sind sie bereits jetzt von konkreten Attacken betroffen? Und welche Schutz-maßnahmen planen sie für die Zukunft?

Diese und weitere Fragen beantworten wir mittlerweile zum dritten Mal im Rahmen unseres jährlichen Cyber Security Reports, für den das Forschungsinstitut SORA im Jänner 2022 insgesamt 450 Mittel- und Großunternehmen in Österreich telefonisch befragt hat.

So viel vorweg: Ransomware-Angriffe gehören inzwischen in der Wirtschaft zum Alltag. Bei jedem fünften befragten Unternehmen kam es bereits zu einer Verschlüsselung von Daten. Die dadurch entstehenden Kosten sind substanziell. Neben den finanziellen Schäden verzeichnen die Unternehmen auch Reputations- und Imageschäden.

Erfahren Sie in unserer Studie mehr darüber, warum ein gewachsenes Bewusstsein für das Thema Cyber Security nicht ausreichend ist, um sich vor Cyber-Angriffen und damit verbundenen Schäden zu schützen.

Wir wünschen eine spannende Lektüre und freuen uns über eine persönliche Kontaktaufnahme!

Karin Mair und Georg Schwondra

Karin Mair
Managing Partner | Financial Advisory & Risk Advisory

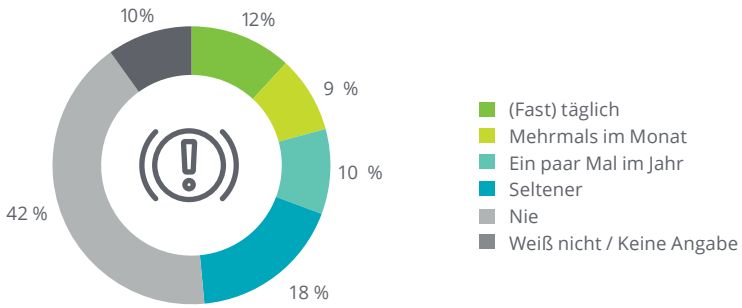
Georg Schwondra
Partner | Risk Advisory

Die Hälfte der Unternehmen erlebt Ransomware-Attacken

Jedes achte Unternehmen wird (fast) täglich angegriffen

12 % der Unternehmen in Österreich mit über 50 Beschäftigten geben an, dass (fast) täglich Angreifer*innen versuchen, von außen in das Unternehmens-Netzwerk einzudringen – mit dem Ziel, Daten zu verschlüsseln. Bei 9 % geschieht dies mehrmals im Monat, bei 10 % mindestens mehrmals im Jahr, bei 18 % seltener. Bei jedem zweiten Unternehmen (52 %) kommt es entweder nie zu Angriffsversuchen, oder die Befragten haben dazu keine Angaben gemacht.

Häufigkeit von Angriffsversuchen



Deloitte View

In den letzten Jahren konnte ein rasanter Anstieg der Cyber-Kriminalität festgestellt werden. Laut Studie hat fast die Hälfte der befragten Unternehmen (49 %) erkannt, dass mindestens einmal ein Cyber-Angriff auf sie unternommen wurde. Jedes achte Unternehmen in Österreich muss sich beinahe täglich mit Cyber-Angriffen auseinandersetzen. Um sich vor Attacken nachhaltig zu schützen, muss Daten- und Informationssicherheit als Top-Priorität auf die Agenden der heimischen Unternehmen gesetzt werden.

Bei fast jedem fünften Unternehmen ab 50 Beschäftigten kam es schon einmal zu einer Verschlüsselung von Daten

18 % der Unternehmen berichten, dass ihre Daten bereits einmal von Angreifer*innen verschlüsselt wurden. Die meisten der betroffenen Unternehmen (86 %) konnten die Daten über eine Sicherung (Backup) wiederherstellen. In zwei von drei Fällen (65 %) konnten die Daten außerdem zumindest zum Großteil wieder entschlüsselt werden.

Deloitte View

Zunehmend geht ein erfolgreicher Ransomware-Angriff mit einer Datenverschlüsselung einher. Durch konkrete und zeitgemäße Sicherheitsmaßnahmen wie Backups können Daten zwar meist wieder erfolgreich hergestellt werden, doch deren Entschlüsselung kostet Zeit sowie Geld und ist häufig nicht vollständig möglich.

Lösegeld wird selten bezahlt - Dunkelziffer ist deutlich höher

In 5 % der Fälle von Datenverschlüsselungen bezahlte nach eigenen Angaben das betroffene Unternehmen den Angreifer*innen Lösegeld.

Deloitte View

Ein Ziel von Cyber-Kriminellen ist das Erpressen von Lösegeld. Nur 5 % der von Datenverschlüsselungen betroffenen Unternehmen geben an, sich auf die finanziellen Forderungen der Cyber-Kriminellen eingelassen und Lösegeld bezahlt zu haben, um wieder an ihre sensiblen Daten zu gelangen. Die Praxis zeigt aber, dass deutlich mehr Unternehmen davon betroffen sein müssen. Ferner äußern sich die meisten Unternehmen grundsätzlich nicht öffentlich zu Cyber-Angriffe und deren Folgen.

Entscheidend ist, dass sich die Unternehmen im Vorfeld bestmöglich vorbereiten, um rasch und effektiv auf einen Ransomware-Angriff reagieren zu können, damit die Forderung nach Lösegeld gar nicht erst aufkommt.

Gestiegenes Bewusstsein beim Thema Cyber Security

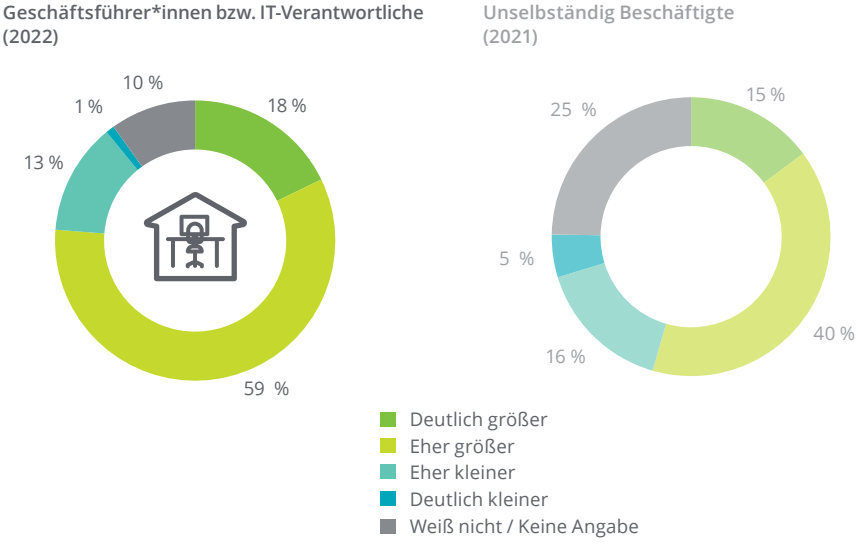
Aufgrund der hohen Zahl an Angriffen sowie durch veränderte Arbeitsbedingungen während der Corona-Pandemie kann in den österreichischen Unternehmen ein gestiegenes Bewusstsein für Cyber Security beobachtet werden.

Höhere Cyber-Risiken durch Home Office

Drei von vier Führungspersonen (77 %) in Unternehmen mit mehr als 50 Beschäftigten gehen davon aus, dass die Bedrohung durch Cyber-Risiken im Home Office deutlich oder eher größer als bei der Arbeit im Büro ist.

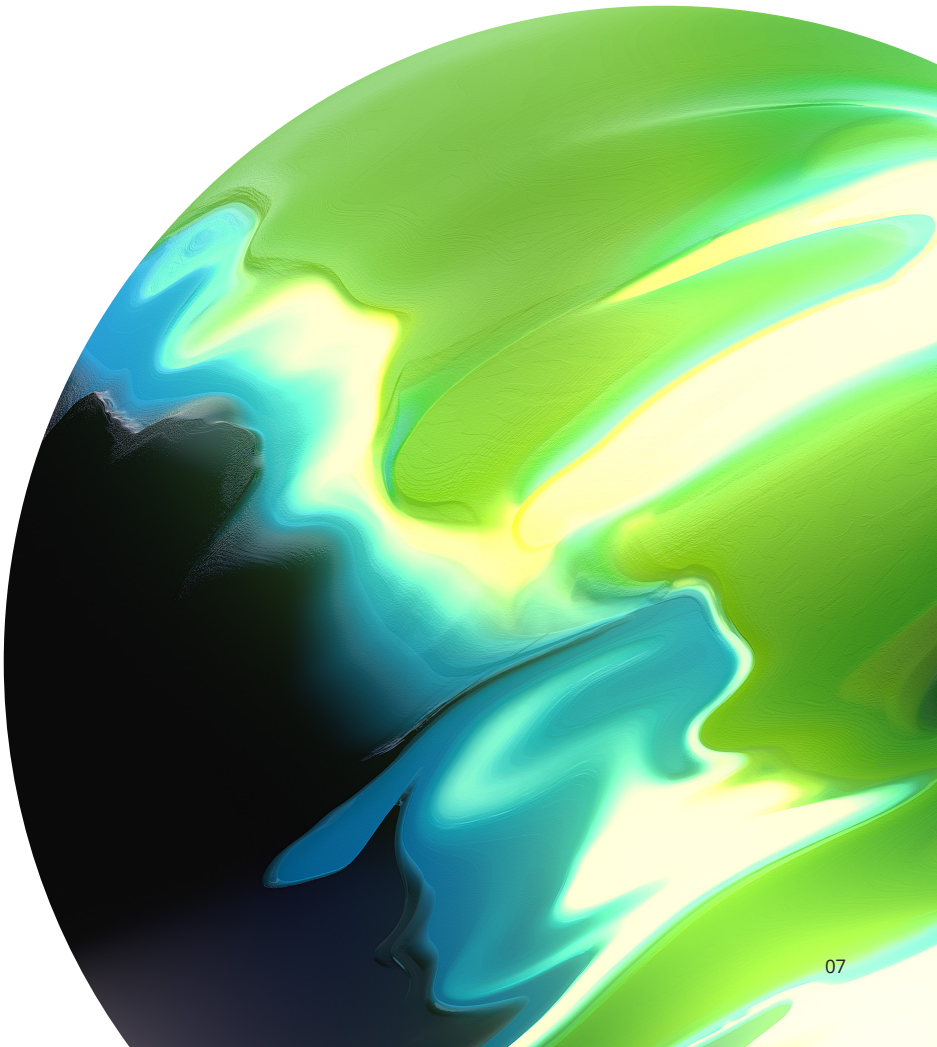
Das liegt über der Einschätzung der Cyber-Risiken im Home Office durch die Beschäftigten selbst. Im Rahmen der letztjährigen Studie gaben rund 55 % der unselbständig Beschäftigten an, dass die Bedrohung durch Cyber-Risiken im Home Office deutlich oder eher größer sei als im Büro. Das deutet darauf hin, dass das Bewusstsein für die potenzielle Bedrohung zwar auf der Führungsebene vorhanden ist, aber in der Belegschaft noch Nachholbedarf besteht.

Einschätzung der Cyber-Risiken im Home Office



Deloitte View

Das allgemeine Bewusstsein für das Thema Cyber Security ist bei den heimischen Unternehmen in den letzten Jahren gestiegen. Grund dafür sind erfolgreiche Awareness-Kampagnen, die unter anderem durch die pandemiebedingte Zunahme an Home Office und der damit verbundenen erhöhten Risiken durchgeführt wurden. Cyber-Security-Awareness allein reicht nicht aus, um Unternehmensdaten zu schützen. Die erhöhte Personalfluktuation führt beispielsweise zu Sicherheitslücken, die es mit effektiven Maßnahmen wie dem Einsatz von XDR-Lösungen, gehärteter Infrastruktur und verbesserten Angriffsdetektionslösungen (z.B. Honeypots) nachhaltig zu schließen gilt.



Höhere subjektive Informiertheit über Cyber-Risiken

Neun von zehn Unternehmen (92 %) fühlen sich sehr oder ziemlich gut über alle möglichen Gefahren und Schutzmaßnahmen informiert. Während sich dieser Anteil unter Befragten in Führungspositionen in IT-Abteilungen kaum verändert hat (96 % in 2020 gegenüber 93 % in 2022), zeigt sich unter Entscheidungsträger*innen, die nicht in der IT-Abteilung arbeiten, eine merkliche Verbesserung. 2020 fühlten sich aus dieser Gruppe zwei Drittel (66 %) sehr oder ziemlich gut informiert, im Jahr 2022 sind es bereits 82 %.

Dementsprechend ist auch der Anteil der Unternehmen zurückgegangen, die folgender Aussage zustimmen: „Es gibt keinen 100 %igen Schutz. Wir befassen uns daher erst mit Sicherheitsthemen, wenn es zu Vorfällen kommt." 2020 stimmte dieser Aussage noch jede*r dritte Befragte (31 %) sehr oder ziemlich zu, 2022 sind es nur mehr 18 %. Anders als beim Wissen über Gefahren und Schutzmaßnahmen tritt dieser Rückgang gleichermaßen bei Befragten aus IT- und anderen Abteilungen auf.

Außerdem wüssten rund neun von zehn Unternehmen (89 %) bei einem Angriff auf das IT-System ziemlich oder sehr sicher, was als erstes zu tun wäre. Gegenüber 2020 (82 %) ist das ein Anstieg um sieben Prozentpunkte.

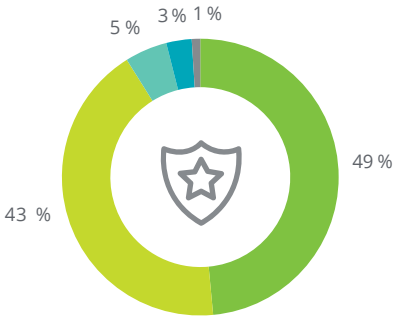
Einschätzung der Sicherheit der eigenen Daten und IT-Systeme im Vergleich zur Zeit vor der Pandemie unverändert

Der Anteil der Unternehmen, die ihre Daten und IT-Systeme insgesamt absolut oder sehr sicher einschätzen, liegt im Vergleich zur Erhebung von 2020 unverändert bei 61 %. Besonders hoch wird die IT-Sicherheit eingeschätzt, wenn die Mitarbeiter*innen durch regelmäßige Schulungen für die Bedrohung von Ransomware-Attacken sensibilisiert werden (69 % „absolut oder sehr sicher"). Unternehmen, die ihre Mitarbeiter*innen nicht regelmäßig schulen, schätzen ihre IT-Sicherheit nur zu 58 % als sehr oder eher sicher ein. Daraus kann man den Schluss ziehen, dass die IT-Sicherheit in Unternehmen durch Schulungen der Mitarbeiter*innen auf jeden Fall erhöht wird.

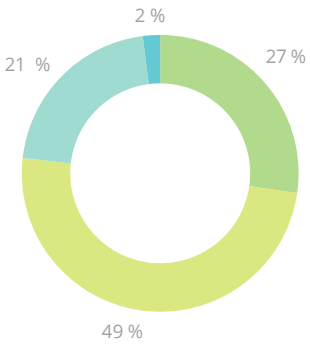
Cyber-Security-Awareness im Zeitvergleich

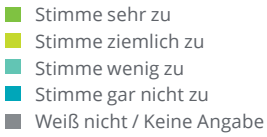
„Fühle mich gut informiert über alle möglichen Gefahren und Schutzmaßnahmen“

(2022)



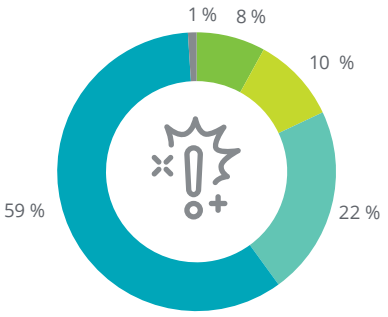
(2020)



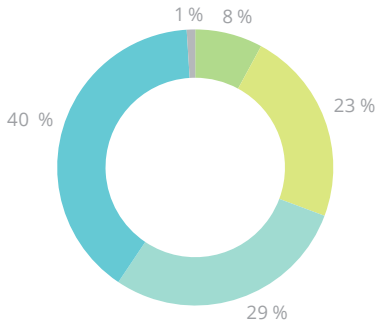


„Es gibt keinen 100%igen Schutz. Wir befassen uns daher erst mit Sicherheitsthemen, wenn es zu Vorfällen kommt“

(2022)

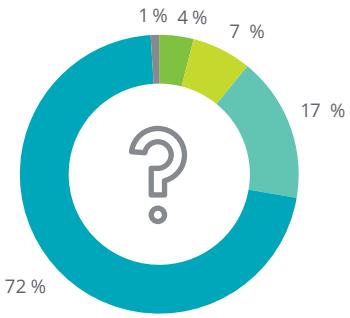


(2020)

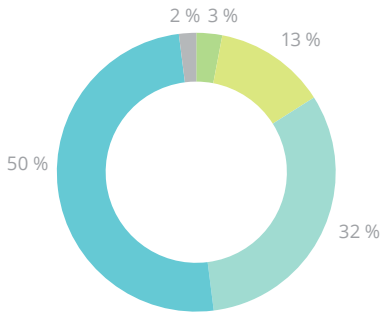


„Bei einem Angriff auf unsere IT-Systeme wüsste ich nicht, was ich als erstes tun soll“

(2022)



(2020)



Unzureichende Präventionsmaßnahmen

Der Großteil der Unternehmen hat keinen Krisen- bzw. Notfallplan

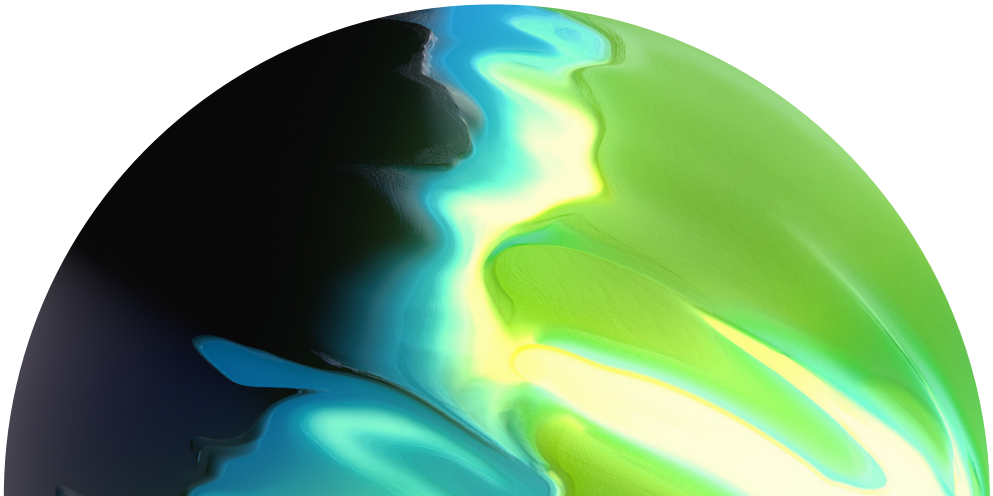
Trotz eines gestiegenen Bewusstseins gibt nur jedes fünfte Unternehmen mit mindestens 50 Mitarbeiter*innen (20 %) an, einen Krisen- bzw. Notfallplan im Unternehmen zu haben, um gegen Ransomware-Angriffe geschützt zu sein.[1] Stattdessen setzen die Unternehmen beim Schutz von Daten und Informationssystemen ähnlich wie 2020 hauptsächlich auf:

- Antivirus Software/Firewalls (72 %)
- Sensibilisierung der Mitarbeiter*innen durch regelmäßige Schulungen (25 %)
- Überprüfungen durch die IT-Abteilung oder Security-Expert*innen (22 %)
- Regelmäßige Updates (21 %)

Deloitte View

Aus der Umfrage geht hervor, dass heimische Unternehmen im Ernstfall nicht ausreichend vorbereitet sind. Nur jedes fünfte Unternehmen kann im Anlassfall auf einen vorher entwickelten Krisen- bzw. Notfallplan zurückgreifen. Dabei stellt sich nicht die Frage, ob ein Unternehmen einen Ransomware-Angriff erlebt, sondern wann – und wie hoch der daraus resultierende Schaden für den Betrieb sein wird. Unternehmen sollten daher wesentlich umfassendere Vorbereitungsmaßnahmen entwickeln und diese regelmäßig auf deren Wirksamkeit testen. Ein aktuelles, robustes IT-Sicherheitskonzept sollte neben einem Krisen- und Notfallplan jedenfalls auch Werkzeuge wie Netzwerksegmentierung und Detektionsmaßnahmen für Cyber-Angriffe umfassen.

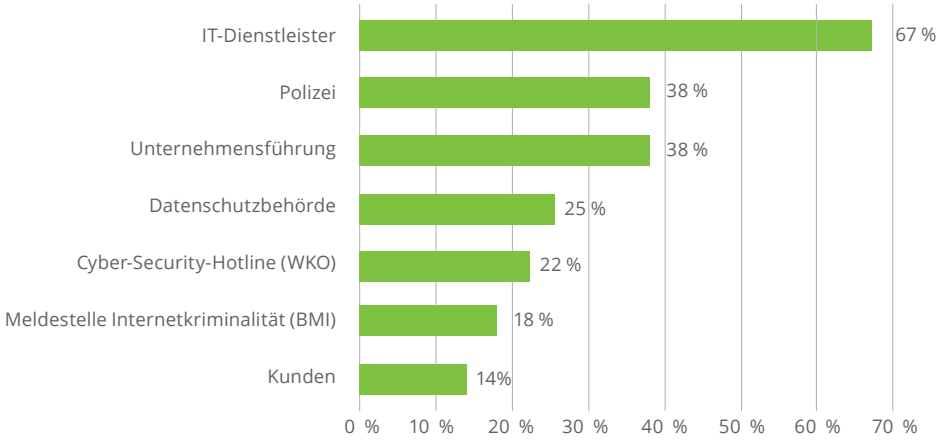
1) Spontane Mehrfach-Nennungen mit Feldvercodung durch die Interviewer*innen auf die Frage „Welche Maßnahmen treffen Sie in Ihrem Unternehmen, um vor Ransomware-Angriffen geschützt zu sein?“



Die Mehrheit würde nicht die Polizei verständigen

Kommt es zu einem Cyber-Angriff, würden sich zwei Drittel der Befragten (67 %) an einen IT-Dienstleister wenden. Die behördlichen Stellen Polizei (38 %), Datenschutzbehörde (25 %) und Meldestelle des BMI (18 %) würden jeweils nur von einer Minderheit kontaktiert werden.[1]

Anlaufstellen im Schadensfall



Deloitte View

Der Großteil der befragten Unternehmen würde sich bei einem Cyber-Angriff an keine behördliche Stelle wenden. Einerseits fehlt den Unternehmen in vielen Fällen das Wissen, wer im Notfall kontaktiert werden soll. Entsprechende Präventionsmaßnahmen sowie Krisen- und Notfallpläne sind hier essenziell, um dem potenziellen Schaden so gering wie möglich zu halten.

Andererseits gibt es Unternehmen, die das geforderte Lösegeld zahlen und den Vorfall nicht an offizielle Stellen melden.

Unternehmen müssen bei einer Cyber-Attacke Zugriff auf ihre Krisen- und Notfallpläne haben. Die Pläne dürfen nicht nur auf einem Server gespeichert sein, denn im Falle einer Verschlüsselung wären diese dann ebenfalls nicht zugänglich.

Hohe finanzielle Schäden durch IT-Ausfall

Cyber-Angriffe bleiben oft nicht ohne Konsequenzen: Die Image-Folgen, die Verluste an wichtigen Informationen bzw. die finanziellen Folgen des Ransomware-Angriffs sind jeweils für jedes zehnte betroffene Unternehmen sehr oder ziemlich belastend.

Mittel- und Großunternehmen schätzen den finanziellen Schaden bei einem einwöchigen Ausfall des IT-Systems durchschnittlich auf 1,2 Mio. Euro

Konfrontiert mit der theoretischen Situation, dass aufgrund eines Cyber-Angriffs das Computersystem des Unternehmens eine Woche stillstehen würde, wird der geschätzte finanzielle Schaden durchschnittlich mit 1,2 Mio. Euro beziffert. Bei Unternehmen mit 50 bis 99 Mitarbeiter*innen wird er auf durchschnittlich 750.000 Euro, bei Unternehmen mit 100 bis 249 Beschäftigten auf durchschnittlich 1,1 Mio. Euro und bei Großunternehmen mit mindestens 250 Beschäftigten auf durchschnittlich 2,6 Mio. Euro geschätzt. Im Verhältnis zur Finanzkraft der Unternehmen beträgt der Median der Verlustschätzungen etwa 1,2 % des gesamten Jahresumsatzes.

Dabei macht es keinen Unterschied, ob man die Unternehmen nach Größe, subjektiver IT-Sicherheit, Erfahrung mit Verschlüsselungen oder Betroffenheit von Ransomware-Angriffen unterscheidet.

Deloitte View

In Österreich nimmt die Anzahl an Ransomware-Angriffen seit den frühen 2010er-Jahren stark zu. Bei 18 % der Unternehmen wurden Daten schon einmal verschlüsselt.

Bei einem einwöchigen Ausfall des IT-Systems rechnen heimische Mittel- und Großunternehmen mit einem finanziellen Schaden von 1,2 Mio. Euro.

Da in der Regel neben den Umsatzausfällen auch beträchtliche Ausgaben für die Wiederherstellung und -beschaffung der verschlüsselten bzw. gestohlenen Daten anfallen, gehen Deloitte und SORA davon aus, dass die tatsächlichen Kosten für einen einwöchigen Stillstand des Computersystems deutlich höher sind als die genannten 1,2 % des Jahresumsatzes. Neben den Umsatzausfällen können die Unternehmen außerdem Reputationsschäden und Schadenersatzforderungen treffen.

Methode und Sample

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

Erhebungsmethode:
Standardisierte Telefonbefragung (CATI)

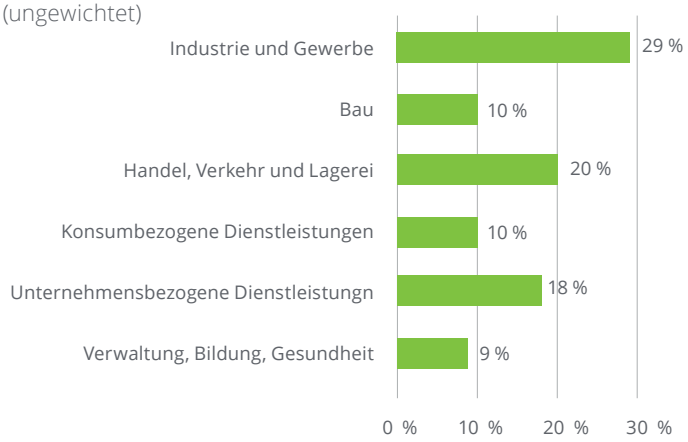
Befragungszeitraum:
Jänner 2022

Stichprobe:
450 Unternehmen

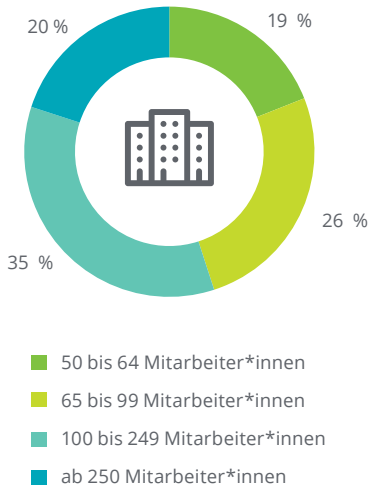
Gewichtung:
Anzahl der Mitarbeiter*innen und Region

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

Branche
(ungewichtet)



Unternehmensgröße
(ungewichtet)



Fazit

Die vorliegende Studie bestätigt: Die meisten heimischen Unternehmen setzen sich mittlerweile mit dem Thema Cyber Security auseinander. Die Gefahr ist real: Die Hälfte der Befragten erlebt regelmäßig Ransomware-Angriffe. Bei fast einem Fünftel konnten Cyber-Kriminelle sogar sensible Unternehmensdaten verschlüsseln. Dennoch gibt nur ein kleiner Prozentsatz an, Lösegeld bezahlt zu haben, was eine viel höhere Dunkelziffer vermuten lässt. Der Großteil der befragten Unternehmen würde sich bei einem Cyber-Angriff außerdem an keine behördliche Stelle wenden.

Trotz steigender Cyber-Security-Awareness bieten Österreichs Unternehmen noch immer eine zu große Angriffsfläche. Durch häufiges Home Office und eine hohe Fluktuationsquote entstehen Sicherheitslücken, die es zu schließen gilt.

Um bei einer Cyber-Attacke rasch und effizient handeln zu können, müssen Unternehmen über ein vorher entwickeltes IT-Sicherheitskonzept verfügen. Ein solches Konzept muss einen zeitgemäßen Krisen- und Notfallplan enthalten und darf nicht nur auf einem Server abgelegt sein. Zudem ist es geboten, die IT-Sicherheitsmaßnahmen eines Unternehmens stets weiterzuentwickeln und in regelmäßigen Abständen zu testen, um eine wirksame technische Barriere gegen Ransomware aufzubauen. Laufende Schulungen und Sensibilisierung der Mitarbeiter*innen sind integraler Bestandteil eines Cyber-Sicherheitskonzepts.

Das Resümee ist klar: Cyber Security muss heute in die DNA jedes Unternehmens integriert werden.

Kontakt

Karin Mair
Managing Partner | Financial Advisory & Risk Advisory

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

Georg Schwondra
Partner | Risk Advisory

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

Deloitte.