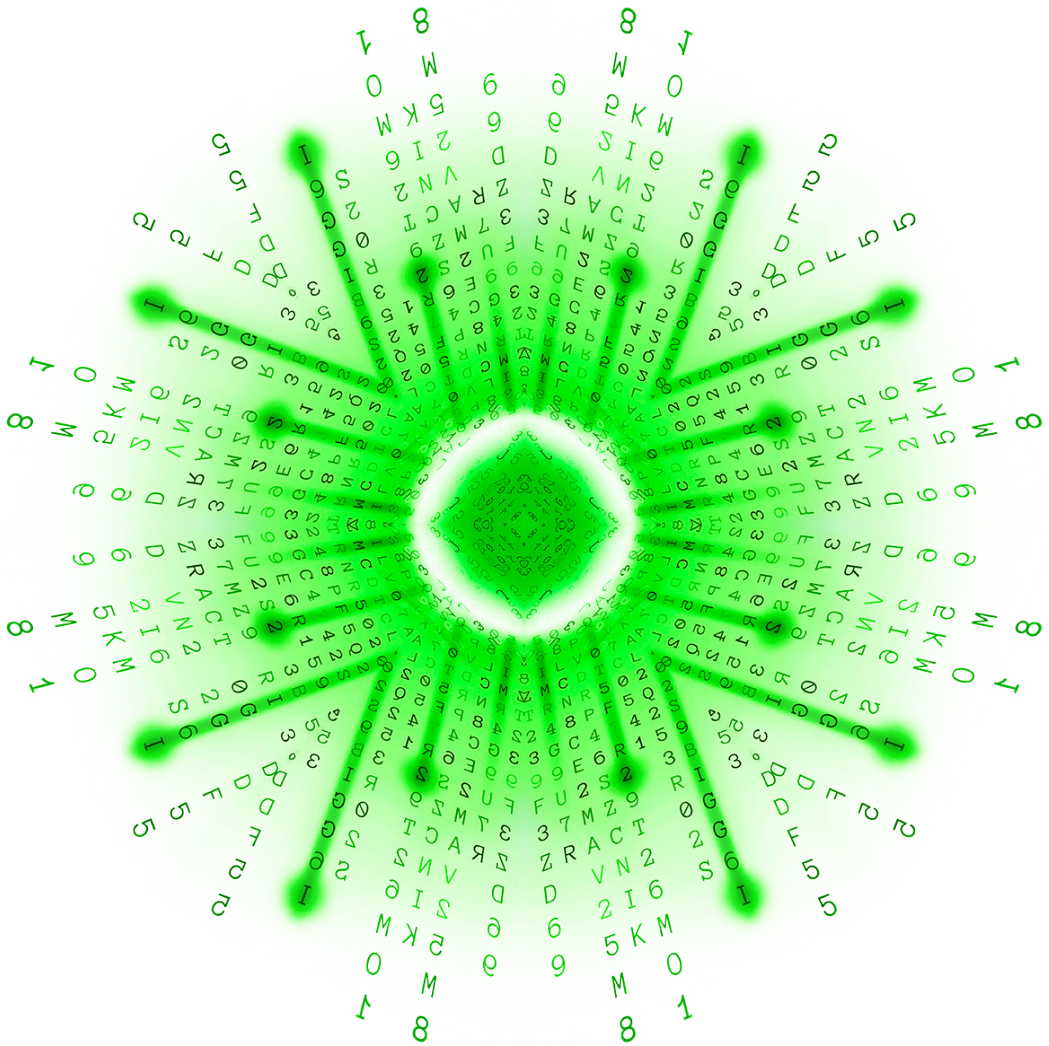
Deloitte.

Deloitte Cyber Security Report Österreich 2020

Eine Studie von Deloitte Österreich in Kooperation mit SORA



MAKING AN IMPACT THAT MATTERS since 1845

Impressum

Herausgegeben von Deloitte Audit Wirtschaftsprüfungs GmbH
StudienautorInnen: Christoph Hofinger und Julia Simon (SORA)
sowie Alexander Ruzicka und Andreas Niederbacher (Deloitte)
unter redaktioneller Mitarbeit von Armin Nowshad und Gina Grassmann (Deloitte)
Grafik und Layout: Claudia Hussovits

Vorwort

Seit Jahren sieht sich die Wirtschaft einer wachsenden Zahl an Cyber-Angriffen ausgesetzt. Die zunehmende Vernetzung und Digitalisierung bietet immer neue Potenziale für kriminelle Umtriebe. Umso wichtiger ist es daher für Unternehmen, sich zu wappnen und entsprechende Maßnahmen im Bereich Cyber Security zu setzen. Aber wie gut sind Österreichs Unternehmen überhaupt bei Cyber Security aufgestellt? Wo liegen die wichtigsten Handlungsfelder?

Um diesen und weiteren Fragen auf den Grund zu gehen, hat das Forschungsinstitut SORA im Jänner 2020 im Auftrag von Deloitte Österreich zum zweiten Mal insgesamt 535 Entscheidungsträgerinnen und Entscheidungsträger im Bereich IT von heimischen Unternehmen zum Thema Daten- und Informations-sicherheit befragt. Dabei zeigt sich: Die Unternehmen fühlen sich sicherer als im Vorjahr. Großen Aufholbedarf gibt es jedoch laut den Ergebnissen vor allem in der Baubranche. Auch in der Prävention und im Umgang mit Cyber-Angriffen sind viele befragte Unter-nehmen noch überfordert und nicht optimal aufgestellt.

Seit Anfang März hat sich die Situation in den heimischen Unternehmen durch die Ausbreitung des Coronavirus drastisch verändert. So arbeiten die Mitarbeiterinnen und Mitarbeiter vieler Organisationen im Home Office – die Sicherheitslage im digitalen Bereich hat sich damit grundlegend verändert. Daher wurde von Deloitte Österreich im Mai 2020 eine zusätzliche Kurzumfrage zum Thema durchgeführt, um der neuen Situation entsprechend Rechnung zu tragen. Die Ergebnisse sind im „Hot Topic"-Teil der vorliegenden Studie zusammengefasst.

Wir wünschen eine spannende Lektüre!

Alexander Ruzicka
Andreas Niederbacher

Alexander Ruzicka
Partner | Risk Advisory

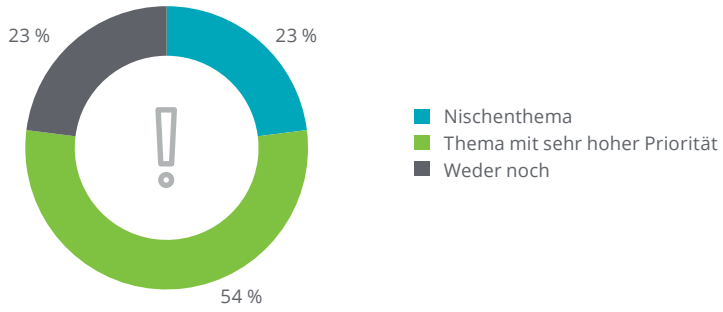
Andreas Niederbacher
Senior Manager | Risk Advisory

Daten- und Informationssicherheit: Ein Thema mit Priorität und (Un-)Sicherheiten

Der diesjährige Cyber Security Report zeigt: Daten- und Informationssicherheit ist für etwas mehr als die Hälfte der befragten Unternehmen ein Thema mit Priorität (54 %). Das sind 10 Prozentpunkte mehr als noch im Vorjahr. Vor allem in Unternehmen der kritischen Infrastruktur (88 %), der unternehmensbezogenen Dienste (72 %) und in Betrieben mit einem Umsatz von über 30 Millionen Euro pro Jahr spielt das Thema überdurchschnittlich häufig eine wesentliche Rolle. Daraus lässt sich schließen: Die Unternehmen haben mehrheitlich die Wichtigkeit von Cyber Security erkannt – die Aufklärungsarbeit der letzten Jahre trägt zunehmend Früchte.

Allerdings: Immerhin für 23 % der Unternehmen ist Daten- und Informationssicherheit nach wie vor nur ein Nischenthema. Das betrifft besonders Unternehmen der Baubranche (43 %) und im Bereich konsumbezogener Dienste (33 %). Hier besteht weiterhin ein großes Risiko für die betroffenen Unternehmen, Opfer von Cyber-Angriffen zu werden.

Was trifft am ehesten auf Ihr Unternehmen zu: Informationssicherheit ist ein Nischenthema oder ein Thema mit sehr hoher Priorität?

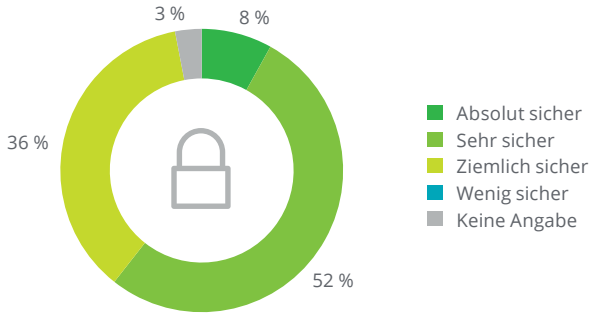


Deloitte View

Jüngste Zahlen der Kriminalstatistik in Österreich zeigen einen Anstieg der Cyberkriminalität. Die höhere Priorität von Daten-Informationssicherheit in Unternehmen kann unter anderem auf diese Entwicklung zurückgeführt werden. Gerade in Zeiten einer zunehmend digitalisierten Welt muss Daten- und Informationssicherheit in allen Unternehmen eine Top-Priorität einnehmen. Das wird den Führungsebenen von immer mehr Unternehmen bewusst.

Das Sicherheitsgefühl hat sich im Vergleich zum Vorjahr ebenfalls verbessert: 60 % der heimischen Unternehmen geben an, dass ihre Daten und IT-Systeme absolut bis sehr sicher sind. Das sind um 6 % mehr als 2019. Auch hier fühlen sich Unternehmen der kritischen Infrastruktur (89 %) sowie Großunternehmen ab einem Umsatz von 100 Millionen Euro pro Jahr (74 %) besonders sicher. Im Branchenvergleich sticht die Baubranche negativ hervor: Nahezu die Hälfte der befragten Bauunternehmen bewertet ihre Daten- und IT-Systeme nur als ziemlich sicher (47 %).

Was glauben Sie, wie sicher sind Ihre Daten und IT-Systeme derzeit?



Deloitte View

Unternehmen, die wenig in ihre digitale Sicherheit investieren, erkennen durchaus, dass ihre Systeme Mängel in puncto Sicherheit aufweisen. Gerade in der Baubranche kam es in den vergangenen Monaten vermehrt zu erfolgreichen Cyber-Angriffen. Das hat Auswirkungen auf das subjektive Sicherheitsgefühl der gesamten Branche. Unternehmen, die sich unsicher fühlen, sollten eine professionelle unabhängige Überprüfung durchführen, um den eigenen Status quo zu kennen und entsprechende Schritte zur Erhöhung der Sicherheit setzen zu können.

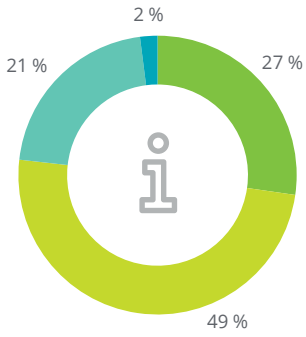
Deloitte View

Das größte Gefahrenpotenzial für Unternehmen liegt darin, keinen klaren Plan für den Ernstfall zu haben. Wenn man nach einem Angriff erst noch überlegen muss, wie man damit umgeht, ist es eindeutig zu spät. Die Prävention muss an erster Stelle stehen – und nicht die Reaktion.

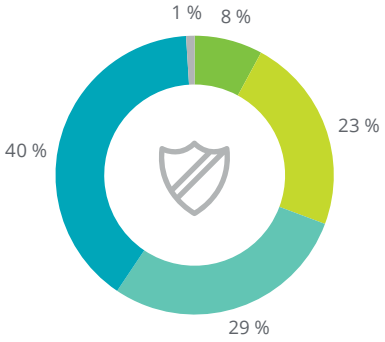
Bei der Einschätzung des eigenen Informationsgrades und der Handlungskompetenz zeigt sich folgendes Bild: Drei Viertel der Unternehmen fühlen sich über Gefahren und Schutzmaßnahmen sehr bis ziemlich gut informiert (76 %). Mit 53 % sind aber etwas mehr als die Hälfte der österreichischen Unternehmen damit überfordert, sich gegen alle möglichen Gefahren abzusichern. 16 % wissen zum Beispiel nicht, was sie bei einem Angriff als erstes tun sollen.

Fast ein Drittel der Befragten (31 %) meint allerdings, dass es ohnehin keinen hundertprozentigen Schutz gibt. Sie befassen sich deshalb erst mit entsprechenden Maßnahmen, wenn es zu Vorfällen kommt (+10 Pp). Insgesamt zeigt sich hier: Jene Unternehmen, bei denen das Thema Daten- und Informationssicherheit eine gewisse Priorität hat, fühlen sich auch besser informiert und sind bei Angriffen seltener überfordert.

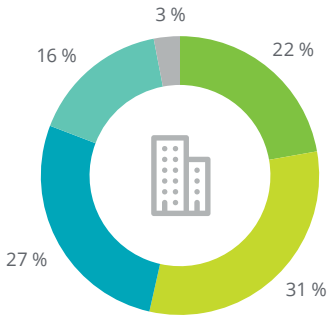
Ich fühle mich gut informiert über alle möglichen Gefahren und Schutzmaßnahmen.



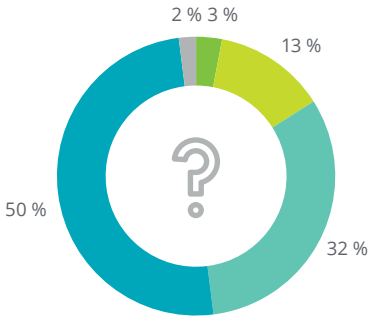
Es gibt ohnehin keinen 100%-igen Schutz, deshalb befassen wir uns erst mit Sicherheitsthemen, wenn es zu Vorfällen kommt.



Sich gegen alle möglichen Gefahren abzusichern, würde das Unternehmen überfordern.



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

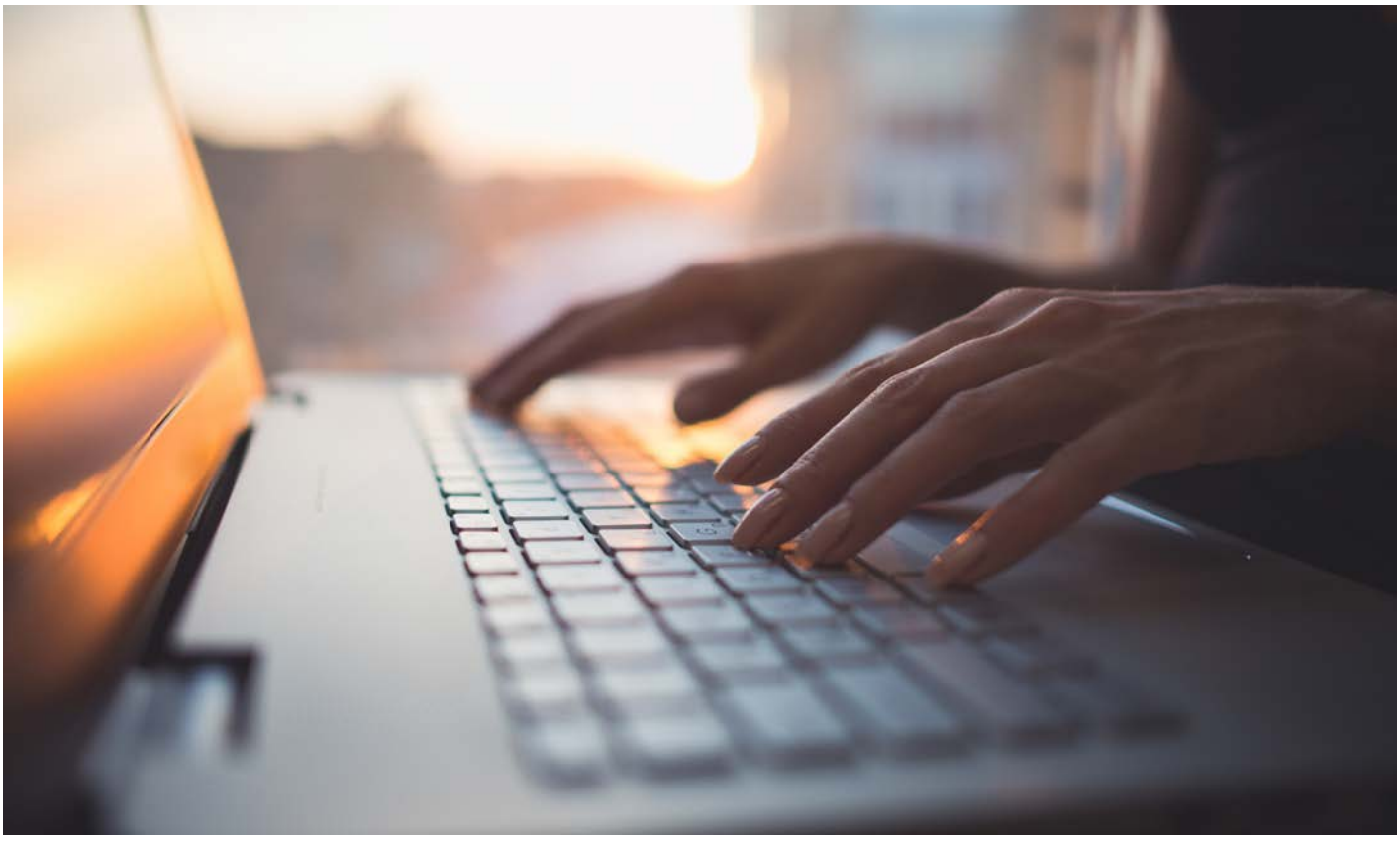


- Stimme sehr zu
- Stimme ziemlich zu
- Stimme wenig zu
- Stimme gar nicht zu
- Keine Angabe

Der Stellenwert von Daten- und Informationssicherheit ist stark vom Umsatz der Unternehmen abhängig. Es lassen sich dabei zwei Ansätze erkennen: Der pragmatische und der präventive Ansatz. In kleineren Unternehmen mit einem Jahresumsatz von bis zu 10 Millionen Euro ist Daten- und Informationssicherheit tendenziell ein Nischenthema. Sie fühlen sich folglich schlechter informiert als mittlere und große Unternehmen. Große Unternehmen mit einem Jahresumsatz von über 40 Millionen Euro sind im Vergleich sicherer sowie seltener überfordert und ergreifen präventive Schutzmaßnahmen. Die kleineren und mittleren Betriebe tendieren eher dazu, erst bei einem konkreten Vorfall zu reagieren. Die Strategie im Umgang mit Daten- und Informationssicherheit steht also in engem Zusammenhang mit den finanziellen und personellen Ressourcen der Unternehmen.

Deloitte View

Nur, weil Unternehmen kleiner sind, heißt das nicht, dass sie nicht genauso potenzielle Ziele von Cyber-Angriffen werden können. Für sie sind Investitionen in eine erfolgreiche Daten- und Informationssicherheit allerdings oftmals herausfordernder als für große Unternehmen. So haben KMU meist keine Mitarbeiterinnen und Mitarbeiter, die sich dezidiert mit dem Thema Cyber Security beschäftigen. Zudem sind die notwendigen Mittel, um die Infrastruktur ausreichend zu schützen, im Verhältnis zum Umsatz auch bedeutend höher. Schlussendlich lohnen sich Investitionen jedoch – denn der Schaden eines erfolgreichen Angriffs kann wesentlich höher sein als sinnvolle Investitionen in die Cyber Security.



Information und Präventionsmaßnahmen geben Sicherheit

Praktiken der Unternehmen, welche die Daten- und Informationssicherheit potenziell gefährden können, haben sich im Vergleich zum Vorjahr kaum verändert. Die externe Speicherung (41 %) sowie der externe Zugriff auf Daten (37 %) sind 2020 gleichermaßen üblich wie 2019. Die Nutzung von privaten Geräten für berufliche Zwecke (20 %) war jedoch Anfang des Jahres unüblicher (-10 Pp) als in der Vorgängerstudie. Das legt den Schluss nahe, dass das Sicherheitsbewusstsein gestiegen ist.

Betrachtet man die Ergebnisse im Detail, so ist in den Branchen Industrie und Gewerbe (47 %) sowie unternehmensbezogene Dienste (46 %) der externe Zugriff auf Daten oder Programme etwa im Home Office besonders üblich. Private Handys, Laptops und Tablets werden vor allem in Bauunternehmen für berufliche Zwecke genutzt (30 %). In großen Unternehmen mit einem Umsatz von über 100 Millionen Euro pro Jahr ist das hingegen bei 91 % eher unüblich.

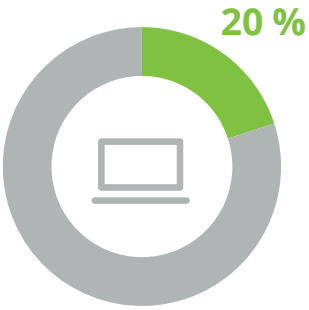
Deloitte View

Private Geräte stellen generell ein hohes Sicherheitsrisiko für Unternehmen dar. Da deren berufliche Nutzung gerade in jenen Unternehmen üblich ist, die wenig Budget für Datensicherheit haben, wird das potenzielle Risiko für diese Betriebe noch mehr erhöht.

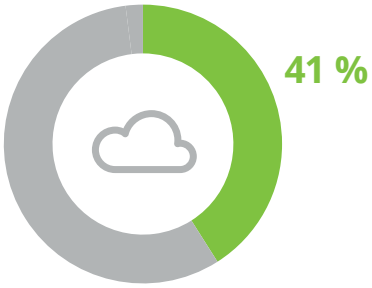
Doch auch bei privaten Geräten können Unternehmen ein gewisses Maß an Sicherheit erzielen. Dafür bedarf es strikten Vorgaben sowie gesonderten Prozessen und Systemen wie zum Beispiel Remote-Desktop-Infrastrukturen. Aktuell müssen Mitarbeiterinnen und Mitarbeiter bei der Nutzung ihrer Privatgeräte oftmals noch eine schlechtere Usability in Kauf nehmen, wobei sich diese in den vergangenen Jahren stark verbessert hat.

Sind die folgenden Dinge in Ihrem Unternehmen eher üblich oder eher unüblich?

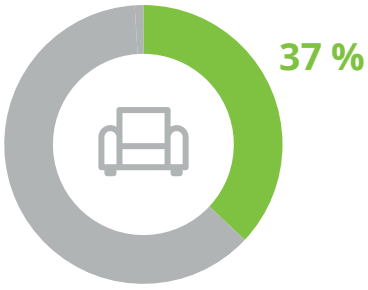
Nutzung von privaten Handys, Laptops oder Tablets für berufliche Zwecke



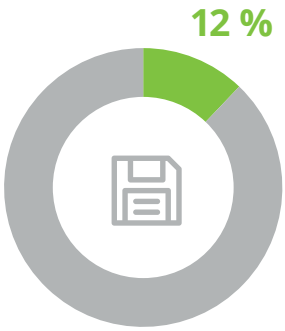
Speicherung von Daten in externen Cloud Services



MitarbeiterInnen können auf Daten oder Programme von außerhalb des Unternehmens zugreifen
(z.B. Home Office)



MitarbeiterInnen nehmen Daten für berufliche Zwecke mit nach Hause
(z.B. USB Stick)

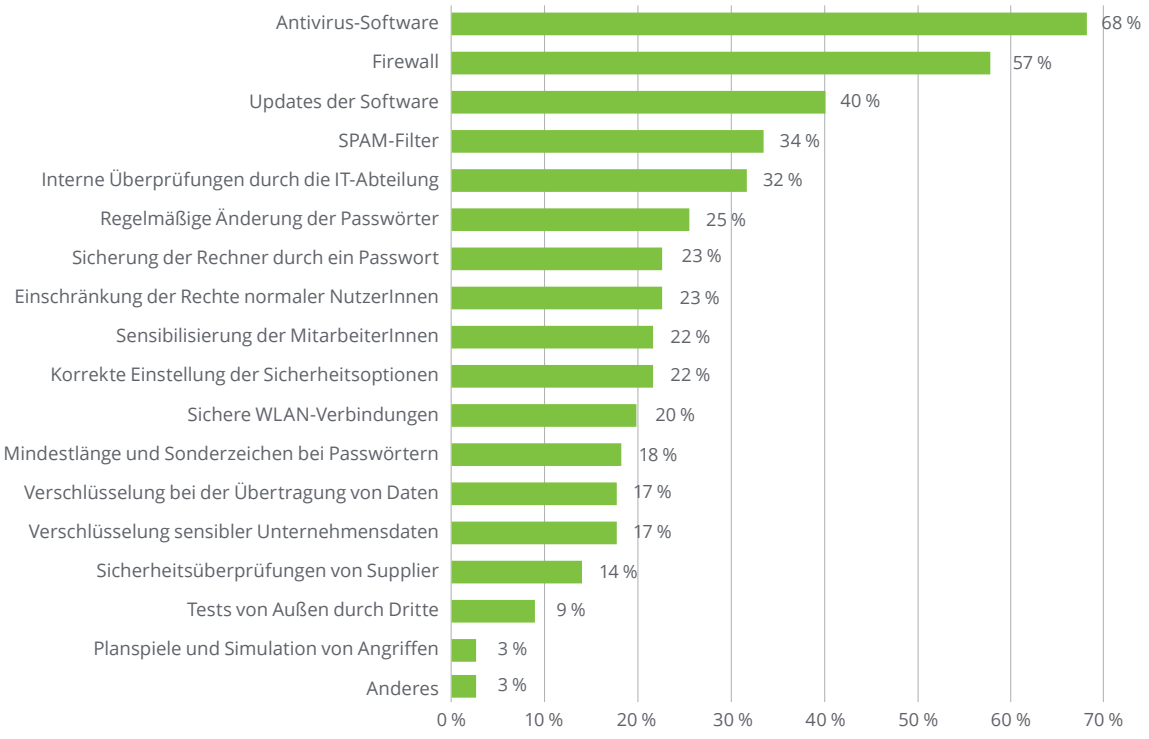


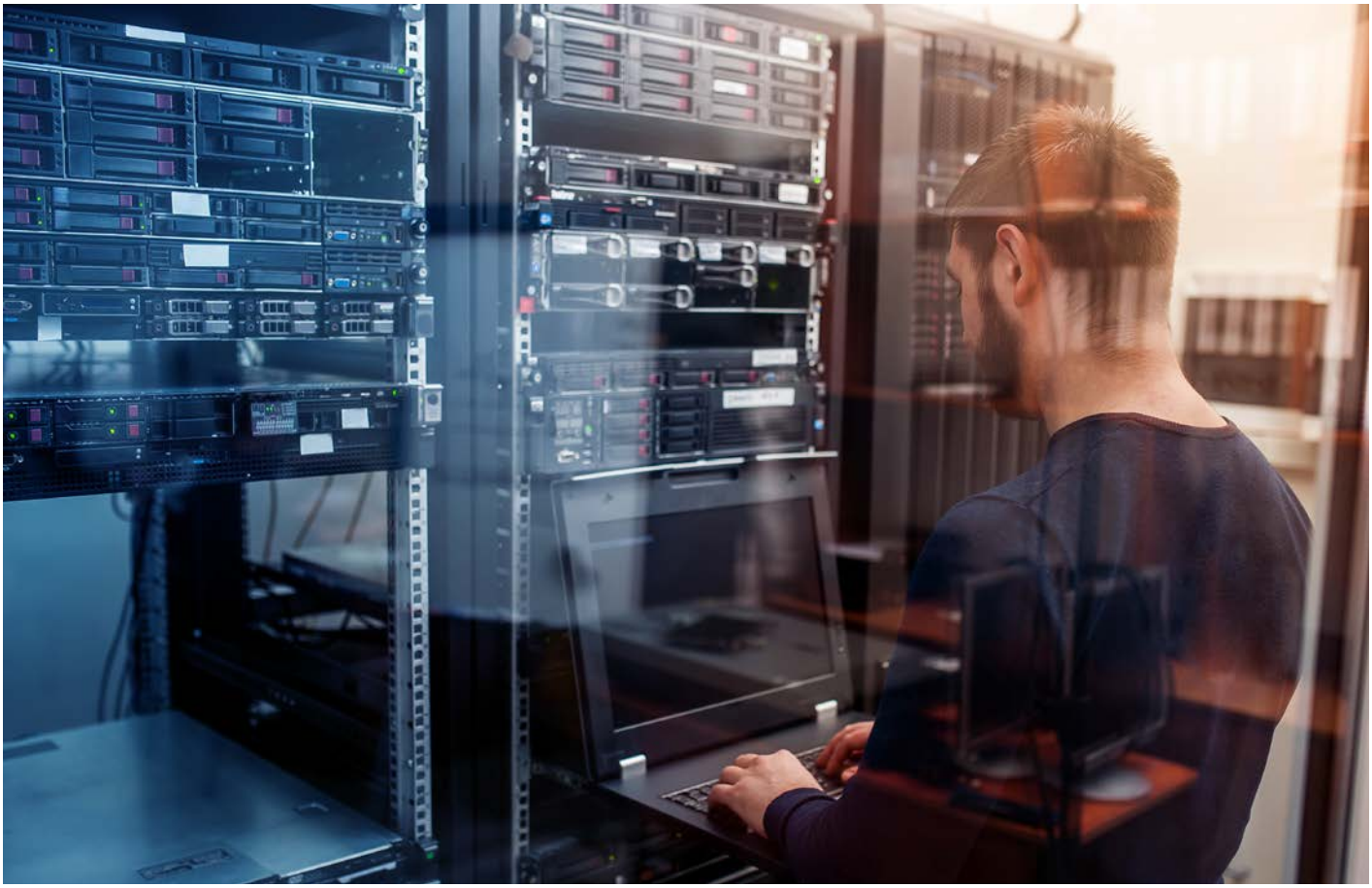
Eher üblich

Die Unternehmen setzen beim Schutz von Daten- und Informationssystemen vorrangig auf den Einsatz von Antivirus-Software (68 %), Firewalls (57 %) und regelmäßige Updates (40 %). Gründe für die Umsetzung dieser Maßnahmen sind vor allem die Prävention und Anliegen der Unternehmen zur Schadensbegrenzung (52 %). 48 % geben auch an, dass der Einsatz von Maßnahmen mittlerweile State of the Art und damit einfach üblich ist. Laut 33 % herrscht außerdem ein Standard in der Branche vor, dem sie gerecht werden müssen. Weitere 23 % berufen sich auf gesetzliche Richtlinien.

Im Gesamten scheint es den Befragten bei den Maßnahmen oftmals darum zu gehen, sich selbst ein Sicherheitsgefühl zu geben. Vorbereitung und Routine scheinen Zuversicht zu schaffen. Unternehmen, die vor allem deswegen Maßnahmen umsetzen, weil es üblich ist, fühlen sich bei einem Angriff dennoch überdurchschnittlich häufig überfordert (61 %). Präventionsmaßnahmen werden aber auch oft in jenen Unternehmen umgesetzt, in denen Daten- und Informationssicherheit ein Nischenthema (61 %) ist.

Welche Maßnahmen zum Schutz von Daten und Informationssystemen gibt es in Ihrem Unternehmen?

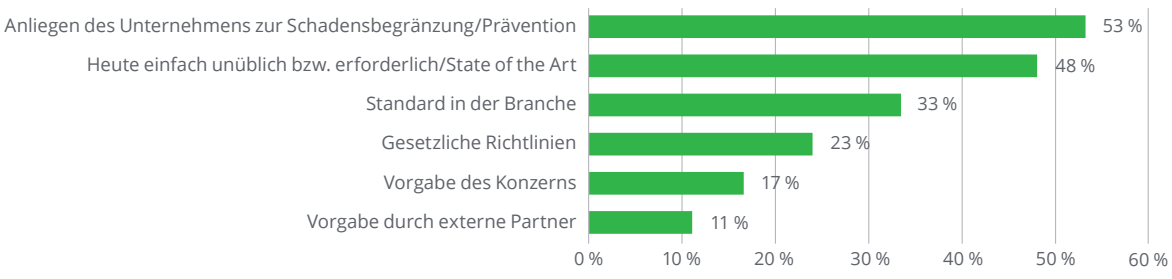




Deloitte View

Maßnahmen sollten immer auch auf ihre Wirksamkeit hin überprüft werden. Placebo-Effekte wirken immer nur so lange, bis wirklich etwas passiert. Generell besteht außerdem die Gefahr, dass Unternehmen sich nur auf Standard-maßnahmen fokussieren, die mittlerweile im besten Fall eine Grundlage bilden, aber sicher nicht die Komplexität der neuen Bedrohungsszenarien entsprechend berücksichtigen. Es empfiehlt sich, auf innovativere Lösungen zu setzen – wie zum Beispiel automatisierte Monitorings der Infrastruktur.

Aus welchen Gründen werden diese Maßnahmen in Ihrem Unternehmen umgesetzt?



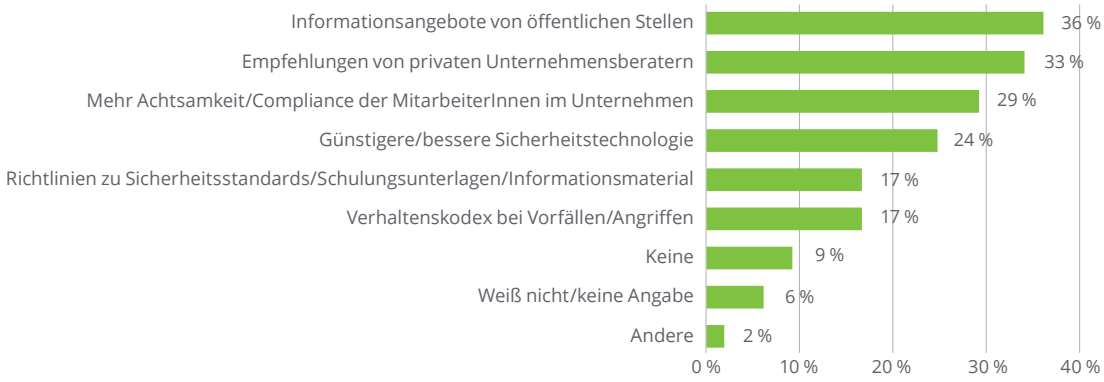
Deloitte View

Große Unternehmen haben häufig Abteilungen oder Service Center implementiert, die sich prioritär mit dem Thema Cyber Security befassen und sich als Dienstleister im eigenen Betrieb verstehen. Insbesondere bei kleineren Unternehmen kann ein Hinzuziehen externer Anbieter eine sinnvolle Option sein, um ein vergleichbares Sicherheitsniveau zu realisieren.

Unternehmen wünschen sich unterstützende Angebote und Maßnahmen zur Verbesserung ihrer Daten- und Informationssicherheit. Informationsangebote von öffentlichen Stellen werden von 36 % der Befragten eingefordert und sind besonders für Unternehmen interessant, in denen Daten- und Informationssicherheit ein Nischenthema ist oder die sich schlecht informiert und überfordert fühlen. Fast die Hälfte der befragten Bauunternehmen (45 %) zählt hier dazu.

Empfehlungen von privaten Unternehmensberatungen würde ein Drittel der Befragten in Anspruch nehmen. Daran interessiert sind vorrangig kleinere und mittlere Unternehmen mit einem Umsatz unter 30 Millionen Euro pro Jahr. 29 % wollen außerdem mehr Achtsamkeit und Compliance bei den Mitarbeiterinnen und Mitarbeitern schaffen. Das ist besonders relevant für Unternehmen, die sich bereits informiert und kompetent fühlen – etwa aus der Branche der unternehmensbezogenen Dienste (39 %) sowie größere Unternehmen mit mehr als 100 Millionen Umsatz pro Jahr (41 %). Sie haben ihre technischen Grenzen oftmals erreicht und wollen in einem nächsten Schritt bei der potenziellen „Schwachstelle Mensch" ansetzen. Eine günstigere und bessere Sicherheitstechnologie wünschen sich wiederum 24 % der Befragten.

Welche Angebote und Maßnahmen würden Sie dabei unterstützen, Ihre Daten und Informationssysteme besser zu sichern?



Schadsoftware und Hacker-Angriffe sind die häufigsten Gründe für Security Breaches

Im Vergleich zu 2019 hat die Summe der registrierten Security Breaches in heimischen Unternehmen abgenommen (- 16 Pp): Schließt man bei der Befragung vom Vorjahr allgemeine technische Probleme und Identitätsdiebstahl aus, berichteten damals 66 % der Unternehmen von Vorfällen. 29 % sprachen von einem Security Breach, 20 % von zwei und 17 % von drei oder mehr.

2020 berichtet nur mehr die Hälfte der Unternehmen von Security Breaches: In einem Viertel der Unternehmen gab es lediglich einen Security Breach (24 %, - 5 Pp), 17 % identifizierten zwei (- 3 Pp) und 9 % drei oder mehr (- 8 Pp). Außerdem kam es seltener zu Datenverlust aufgrund unzureichender Backups (- 15 Pp) oder durch den leichtfertigen Umgang seitens der Mitarbeiterinnen und Mitarbeiter (- 5 Pp).

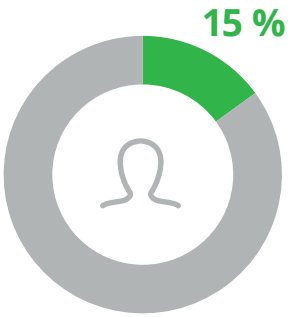
Am häufigsten erleben die befragten Unternehmen Security Breaches in Form von Befall durch Schadsoftware aus dem Internet (27 %), wobei hier die unternehmensbezogenen Dienste (37 %) überdurchschnittlich betroffen sind. Hacker-Angriffe fanden in 15 % der befragten Unternehmen statt – davon besonders selten in Bauunternehmen (1 %) und häufiger in Unternehmen mit einem Umsatz über 100 Millionen Euro (28 %). Onlinebetrug oder auch Phishing (12 %) tritt häufig in der Branche der unternehmensbezogenen Dienste und in umsatzstärkeren Unternehmen (21 %) sowie in der kritischen Infrastruktur (26 %) auf. Mit Denial of Service haben bereits 12 % der Befragten Erfahrungen gemacht. Hier sind die konsumbezogenen Dienste sowie Unternehmen der kritischen Infrastruktur besonders betroffen (30 %).

Deloitte View

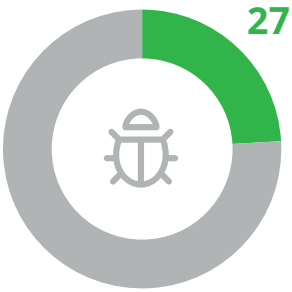
Die EU-DSGVO und damit verbundene Investitionen im Bereich Datenschutz und Infrastruktur lassen auch eine Erhöhung der allgemeinen Informationssicherheit erkennen. Grund hierfür sind Synergie-Effekte beider Bereiche.

Sind diese Szenarien bei Ihnen im Unternehmen bereits aufgetreten?

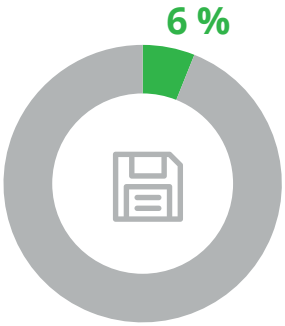
Hacker-Angriffe



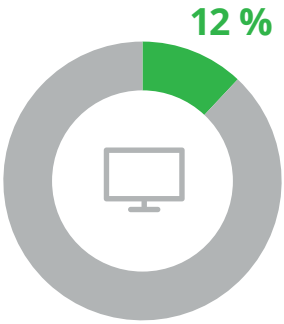
Befall durch Schadsoftware aus dem Internet (wie z.B. Viren, Trojaner oder Ransomware)



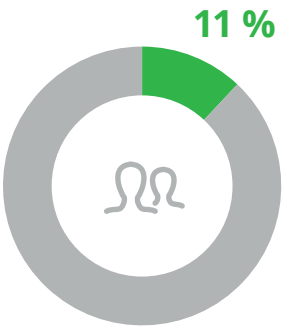
Datenverlust (z.B. aufgrund unzureichender Backups oder fehlender Updates)



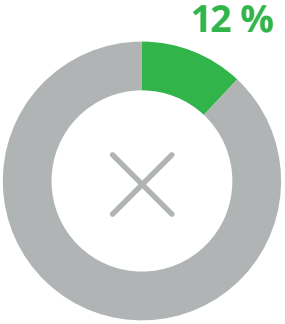
Onlinebetrug (z.B. mittels gefälschter Websites oder E-Mails bzw. Phishing)



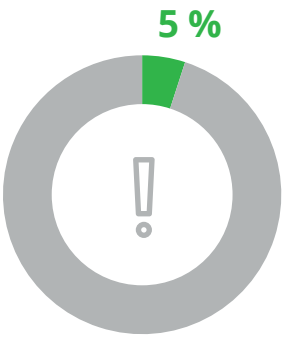
Datenverlust durch MitarbeiterInnen aufgrund leichtfertigen Umgangs



Blockieren oder Stören von Webseiten oder Systemen (Denial of Service)



Vorsätzlicher Datenmissbrauch
(z.B. unerlaubte Datenweitergabe)



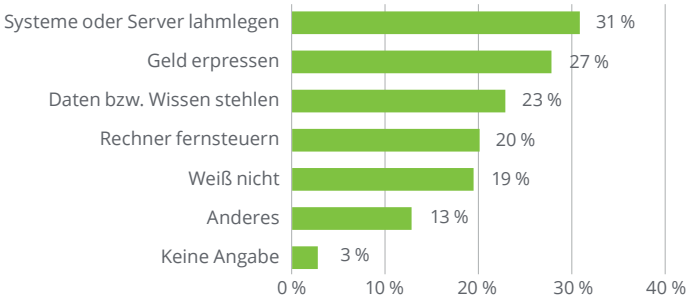
Bereits aufgetreten

Die Gründe und Absichten der Angreiferinnen und Angreifer schätzen die befragten Unternehmen 2020 vielfältiger ein als noch im Vorjahr. Jeder der vier abgefragten Gründe – Lahmlegen des Systems oder Servers, Diebstahl von Daten und Wissen, Fernsteuerung des Rechners und Erpressung von Geld – erscheint zwei von zehn Befragten naheliegend. Seltener als 2019 wird jedoch vermutet, dass Angreiferinnen und Angreifer das System oder den Server lahmlegen wollen (- 21 Pp). Das Erpressen von Geld (+ 22 Pp) wird hingegen häufiger angenommen. Je größer das Unternehmen, desto eher gilt die Vermutung, dass es die Angreiferinnen und Angreifer auf Daten, Wissen oder Geld abgesehen haben.

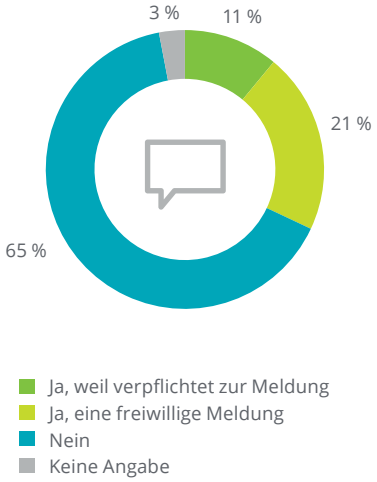
Deloitte View

Diese Ergebnisse decken sich auch mit den Erfahrungen aus der Beratungspraxis. Vor allem digitale, anonyme Zahlungsmöglichkeiten haben den Anstieg von Gelderpressungen stark gefördert.

Was vermuten Sie, worauf hatten es die AngreiferInnen abgesehen?

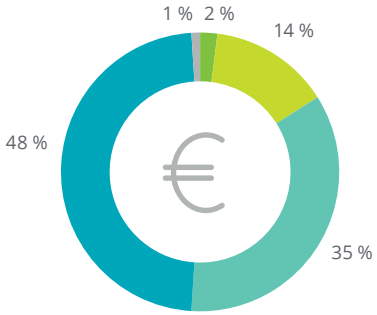


Haben Sie den Vorfall der Polizei oder anderen öffentlichen Stellen gemeldet?

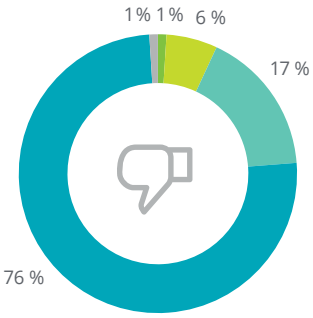


Wie hoch waren die Folgen der Angriffe für Ihr Unternehmen?

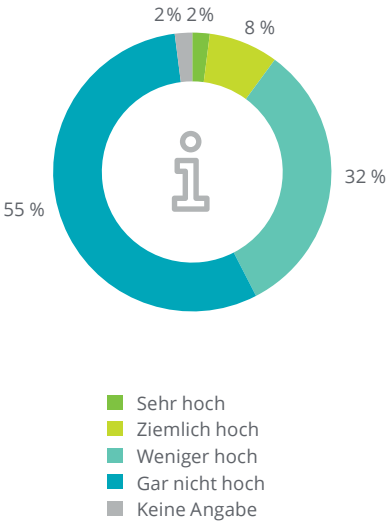
Die finanziellen Folgen



Die Image-Folgen



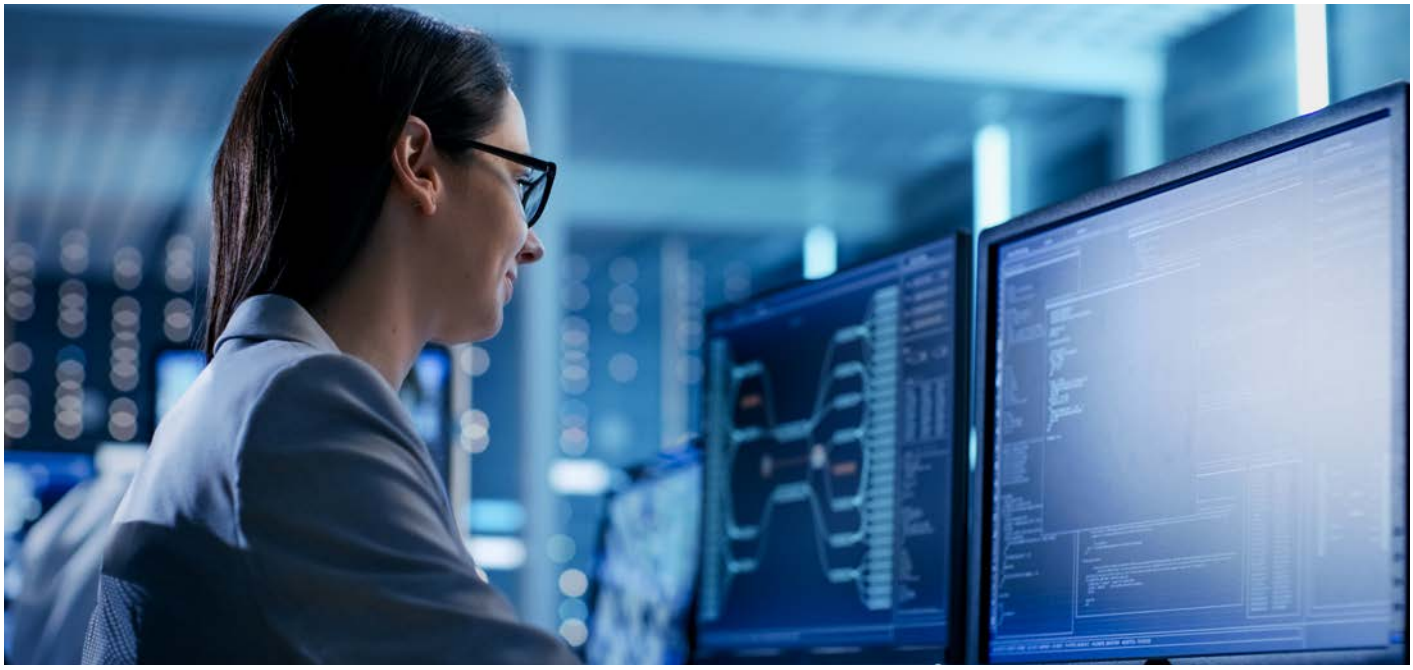
Die Verluste an wichtigen Informationen



Eine Meldung bei der Polizei oder einer anderen öffentlichen Behörde haben rund 32 % der Unternehmen gemacht, die einen oder mehrere Security Breaches verzeichnet hatten. Dabei waren rund 11 % dazu verpflichtet, die restlichen 21 % haben die Meldung freiwillig gemacht. Eine Meldung wird laut Umfrage generell häufiger vorgenommen, wenn es mehrere Security Breaches gab und wenn das Unternehmen der kritischen Infrastruktur angehört. Keine Meldung (65 %) haben überdurchschnittlich oft Unternehmen vorgenommen, in denen IT-Sicherheit ein Nischenthema ist (89 %), die Teil der Baubranche sind (80 %) oder deren subjektives Sicherheitsgefühl gering ist (79 %).

Die Folgen der Angriffe in den Unternehmen mit einem oder mehreren Security Breaches sind laut den Befragten verhältnismäßig gering. Sehr bis ziemlich hohe finanzielle Folgen melden lediglich 16 % der Unternehmen – und hier vor allem jene, die IT-Sicherheit als Nischenthema sehen, sich schlecht informiert fühlen und bei Angriffen überfordert sind. Auch Unternehmen der Baubranche (21 %) sind dabei besonders betroffen.

Die Folgen durch den Verlust von Daten oder wichtigen Informationen waren nur für 10 % der Befragten sehr bis ziemlich hoch: Auch hier fallen neben kleinen Unternehmen (14 %) wieder die Bauunternehmen (21 %) negativ auf. Mit sehr bis ziemlich hohen Imageschäden waren bislang nur 7 % der Betriebe konfrontiert – hier vor allem jene der kritischen Infrastruktur (13 %). Generell steigen die finanziellen Folgen sowie die Folgen für das Image mit der Anzahl der Security Breaches.



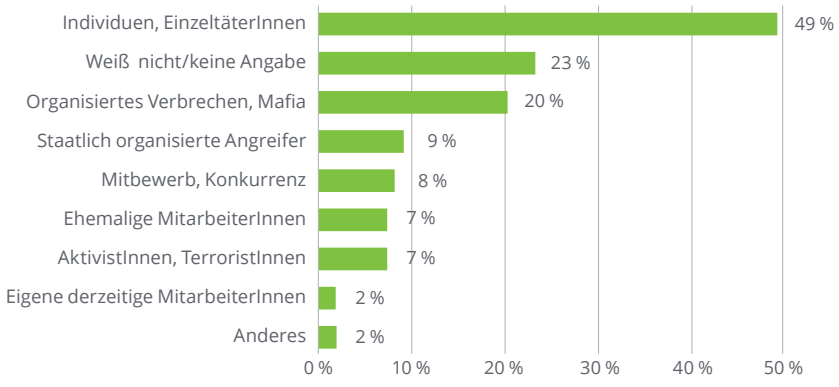
Deloitte View

Auch, wenn die finanziellen Folgen sich für die Unternehmen oft in Grenzen halten, darf nicht bei Investitionen in die Cyber Security gespart werden. Denn wie die Umfrageergebnisse zeigen, trifft es vor allem die Unternehmen, die sich nicht ausreichend mit dem Thema beschäftigen.

Ferner sind die finanziellen Folgen aufgrund von Imageschäden oder durch fehlende Verfügbarkeiten oftmals sehr schlecht kalkulierbar. Die Auswirkungen solcher Schäden können auch noch nach Jahren für Unternehmen spürbar sein.

Laut Studie befürchten mittlerweile rund 49 % der Unternehmen Angriffe von Individuen (+ 10 Pp). 20 % der Unternehmen rechnen mit Angriffen durch das organisierte Verbrechen oder die Mafia. Angriffe von Mitbewerbern werden nur mehr von 8 % der Befragten vermutet (- 15 Pp).

Von wem befürchten Sie am ehesten Angriffe auf Ihr Unternehmen?



HOT TOPIC: Cyber Security in Zeiten von COVID-19

Durch die Ausbreitung von COVID-19 musste der Großteil der österreichischen Unternehmen komplett oder teilweise auf Home Office umsatteln. Welche Herausforderungen hat dieser Umstand für die heimischen IT-Abteilungen sowie für Datenschutzexpertinnen und -experten mit sich gebracht? Welche Auswirkungen hat die Corona-Krise auf die Cyber Security der Unternehmen? Mit einer Kurzumfrage unter 114 Entscheidungsträgerinnen und Entscheidungsträgern aus österreichischen Betrieben ging Deloitte Österreich diesen Fragen Anfang Mai 2020 auf den Grund.

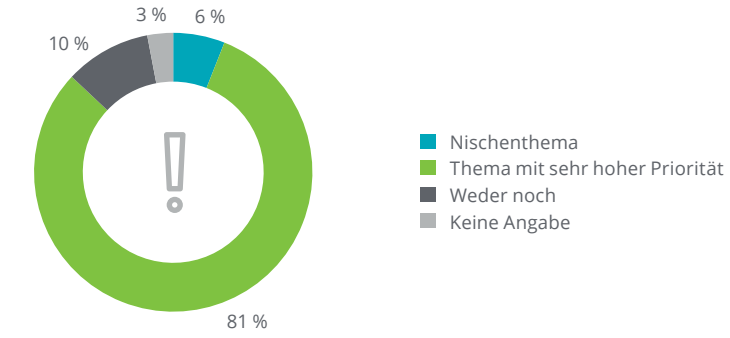
Sicherheitsgefühl in der Corona-Krise

Für 81 % der Befragten ist Informationssicherheit auch in Zeiten von Corona ein Thema mit hoher Priorität. Dementsprechend fühlt sich auch der Großteil sicher: Ganze 60 % bewerten ihre Daten und IT-Systeme als absolut bis sehr sicher, 31 % beschreiben diese aktuell zumindest als ziemlich sicher. Aber dennoch steigt das Unsicherheitsgefühl: So beobachteten 22 % in den letzten Wochen eine leichte bis starke Abnahme ihrer Daten- und IT-Sicherheit.

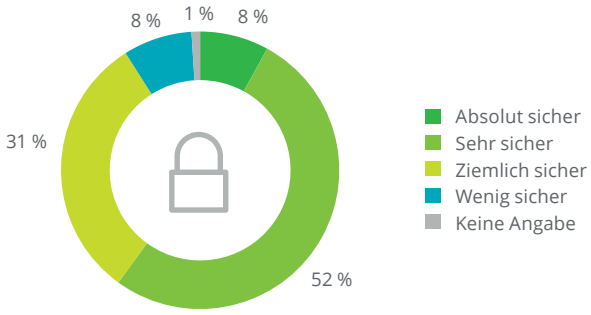
Deloitte View

Neben den offensichtlichen IT-Herausforderungen des dezentralen Arbeitens ist das Thema der Informationssicherheit in den letzten Wochen wieder in den Vordergrund gerückt. Die österreichischen Unternehmen sind zwar relativ selbstbewusst, was die Sicherheit ihrer Daten- und IT-Systeme anbelangt. Dennoch bringt die neue Situation rund um COVID-19 mehr Unsicherheit mit sich.

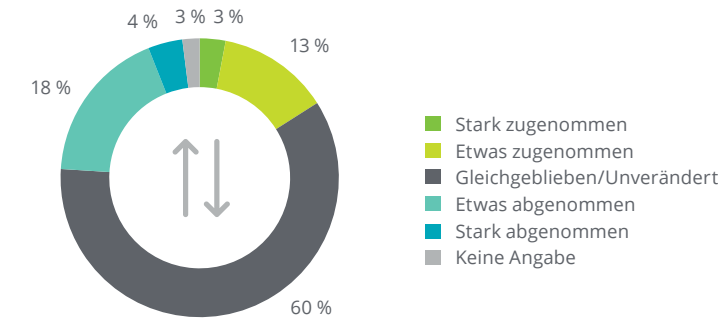
Was trifft am ehesten auf Ihr Unternehmen zu: Ist Informationssicherheit ein Nischenthema oder ein Thema mit sehr hoher Priorität?



Was glauben Sie, wie sicher sind Ihre Daten und IT-Systeme derzeit?



Hat die Sicherheit Ihrer Daten- und IT Systeme durch COVID-19 zugenommen,abgenommen oder ist sie gleichgeblieben?



Cyber Security im Home Office

Derzeit befindet sich laut Umfrage die Mehrheit der Mitarbeiterinnen und Mitarbeiter heimischer Unternehmen im Home Office: So arbeiten bei 42 % der Befragten rund drei Viertel der Mitarbeiterinnen und Mitarbeiter von zu Hause aus, bei 21 % tut dies sogar die gesamte Belegschaft. Nur 8 % geben an, dass in ihrem Unternehmen niemand im Home Office tätig ist.

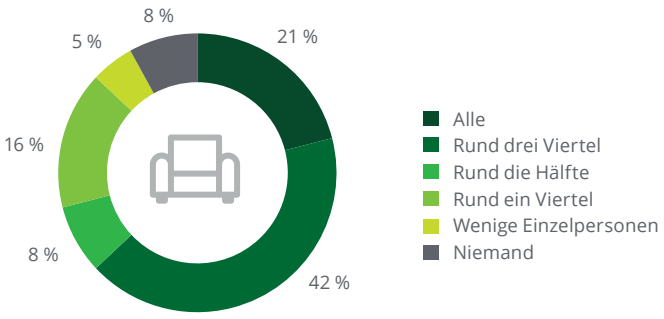
Grund zur Sorge gibt es offenbar nicht: Ganze 91 % sind der Meinung, dass die unternehmenseigenen Informationssicherheitssysteme gut für Home Office aufgestellt sind. Abstriche in puncto Cyber Security aufgrund des externen Zugriffs auf Programme und Daten mussten die wenigsten machen. Auch ein verstärktes Auftreten von Sicherheitslücken wurde bisher eher selten beobachtet. In Bezug auf den Umgang mit personenbezogenen Daten im Zusammenhang mit an COVID-19 Erkrankten hält sich der Aufwand laut Umfrage ebenfalls in Grenzen.

Allerdings hat sich der Wartungsaufwand bei rund einem Drittel der Unternehmen erhöht. Auch die Nutzung privater Geräte für berufliche Zwecke hat immerhin bei 41 % eher zugenommen. Dementsprechend geben 61 % an, dass der Risikofaktor „Mensch" in der derzeitigen Situation noch kritischer geworden ist.

Deloitte View

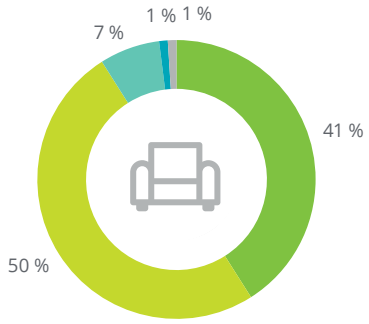
Viele Unternehmen haben Home Office bereits in der Vergangenheit praktiziert und dadurch Erfahrungswerte gesammelt. Doch die Skalierbarkeit auf einen Großteil der Belegschaft stellt eine große Herausforderung dar. Unternehmen, die auf durchdachte und nicht unter Druck der kurzfristigen COVID-19 bedingten Umstellung entstandene Sicherheitskonzepte zugreifen können, sind hier klar im Vorteil.

Wie viele Ihrer MitarbeiterInnen befinden sich derzeit im Home Office?

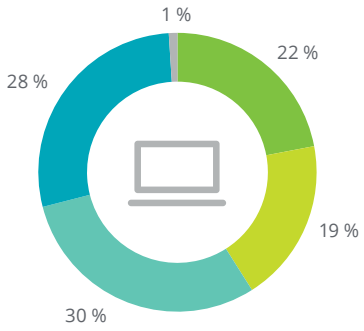


Treffen die folgenden Aussagen auf Ihr Unternehmen zu?

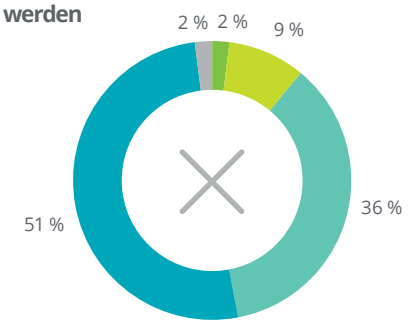
Unser Informationssicherheits-system ist für Home Office gut aufgestellt



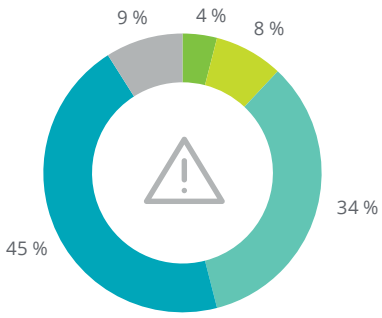
Die Nutzung von privaten Geräten für berufliche Zwecke hat durch die aktuelle Situation zugenommen



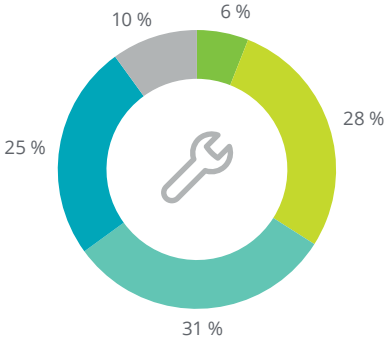
Um MitarbeiterInnen externen Zugriff auf Programme/Daten zu ermöglichen, müssen Abstriche in puncto Cyber Security gemacht werden



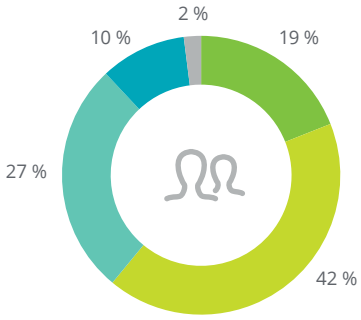
Das Aufkommen von Sicherheits-lücken hat durch die aktuelle Situation zugenommen



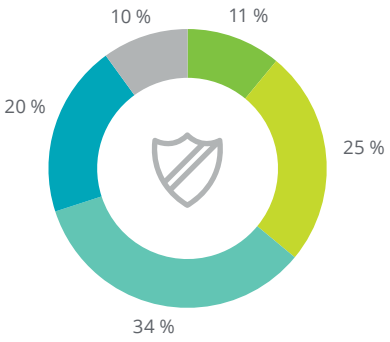
Der Wartungsaufwand für das Firmennetzwerk hat sich erhöht

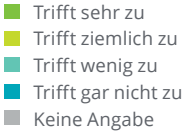


Der Risikofaktor "Mensch" ist in der derzeitigen Situation noch kritischer geworden



Der Umgang mit personenbezogenen Daten im Zusammenhang mit COVID-19-Erkrankungen erfordert zusätzliche Prozesse oder Sicherheitsmaßnahmen





Aufkommen von Cyber-Angriffen

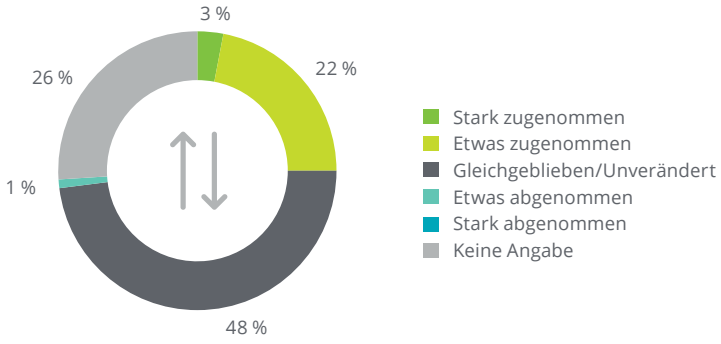
Die Umfrage zeigt: Nur wenige Unternehmen haben seit dem Ausbruch von COVID-19 Angriffe auf ihre Daten- und IT-Systeme festgestellt. Aber: Viele Angriffe bleiben lange unentdeckt. So konnte etwa kein einziges der befragten Unternehmen bisher einen erfolgreichen Hacker-Angriff verzeichnen, gleichzeitig sind sich aber 17 % nicht sicher, ob nicht doch ein Angriff stattgefunden hat. Am vergleichsweise häufigsten berichten die Befragten von Onlinebetrug mittels gefälschter Websites und E-Mails. 12 % sind diesem Angriff auch bereits zum Opfer gefallen.

Laut den meisten Unternehmen hat sich die Häufigkeit von Angriffen durch die Verbreitung von COVID-19 nicht verändert. 25 % nehmen jedoch einen Anstieg im Vergleich zu vorher wahr.

Deloitte View

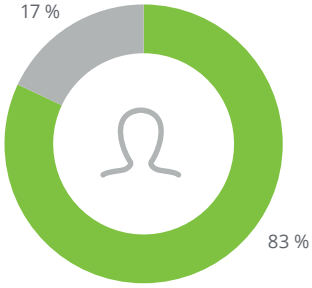
Es stellt ein großes Risiko dar, dass viele Cyber-Angriffe unentdeckt bleiben. Hier lohnt es sich für Unternehmen in entsprechende Programme und Tools zu investieren, um dieses Risiko gering zu halten. Zu berücksichtigen ist: Bei gleichbleibendem Aufkommen von Cyber-Angriffen besteht jedenfalls ein erhöhtes Risiko, dass diese erfolgreich sind. Denn durch die Umstellung der Arbeitsweise auf Home Office und die Nutzung von nicht routinemäßig genutzter Software können Mitarbeiterinnen und Mitarbeiter leichter Opfer von Angriffen werden. Awareness-Bildung und die Kommunikation von Angriffsmustern ist deshalb wichtiger denn je.

Haben Angriffe auf Ihre Daten und Systeme seit der COVID-19-Situation zugenommen, abgenommen oder sind gleichgeblieben?

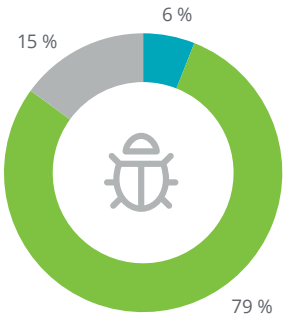


Sind seit dem Ausbruch von COVID-19 in Österreich (März 2020) folgende Szenarien in Ihrem Unternehmen aufgetreten?

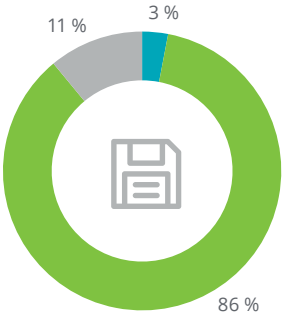
Hacker-Angriff



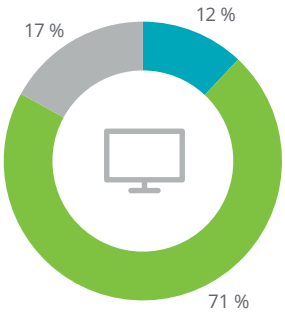
Befall durch Schadsoftware aus dem Internet (wie z.B. Viren, Trojaner oder Ransomware)



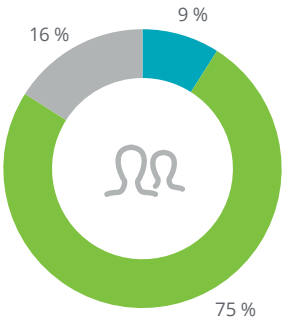
Datenverlust (z.B. aufgrund unzureichender Backups oder fehlender Updates)



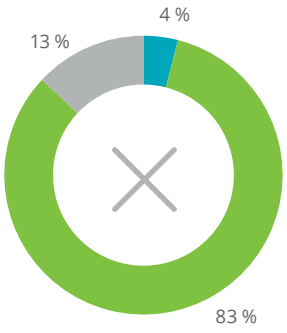
Onlinebetrug (z.B. mittels gefälschter Websites oder E-Mails bzw. Phishing)



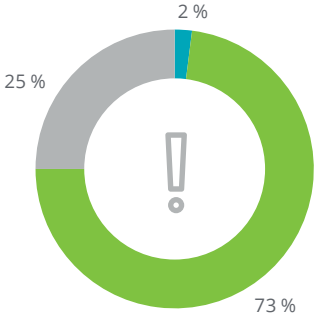
Datenverlust durch MitarbeiterInnen aufgrund leichtfertigen Umgangs

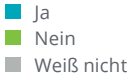


Blockieren oder Stören von Webseiten oder Systemen (Denial of Service)



Vorsätzlicher Datenmissbrauch (z.B. unerlaubte Datenweitergabe)





Aktuelle und geplante Maßnahmen

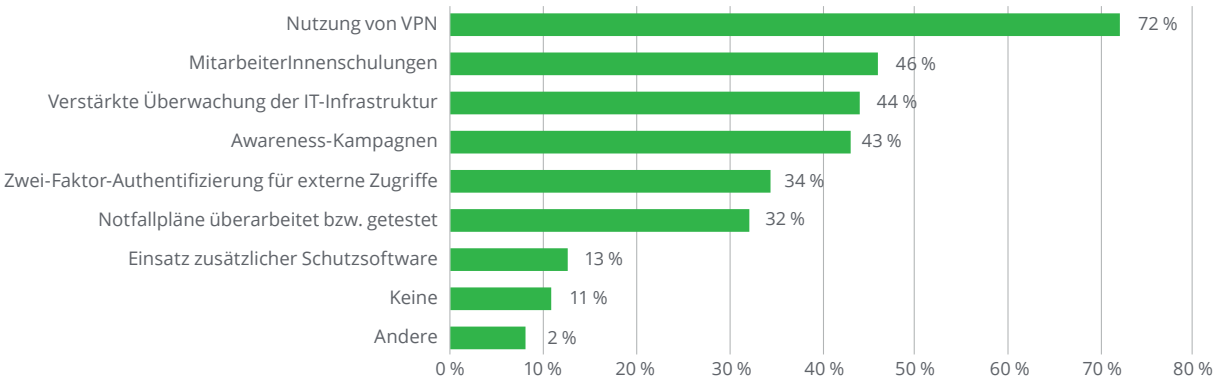
Die meisten Unternehmen setzen zur Bewältigung der neuen Arbeitsbedingungen auf die Nutzung von VPN (72 %), Schulungen der Mitarbeiterinnen und Mitarbeiter (46 %) sowie entsprechende Awareness-Kampagnen (43 %) und eine verstärkte Überwachung der IT-Infrastruktur (44 %). Zusätzliche Schutzsoftware kommt nur bei 13 % der befragten Unternehmen zum Einsatz.

Vor dem Hintergrund von COVID-19 wollen 40 % der Befragten in Zukunft verstärkt auf die Erhöhung der Sicherheitsbestimmungen und -vorkehrungen für mobile Endgeräte fokussieren. Auch die Überarbeitung bestehender Sicherheitsrichtlinien steht bei 38 % auf dem Plan. Zusätzliche Investitionen in den Bereich Cyber Security werden hingegen nur von 21 % in Betracht gezogen.

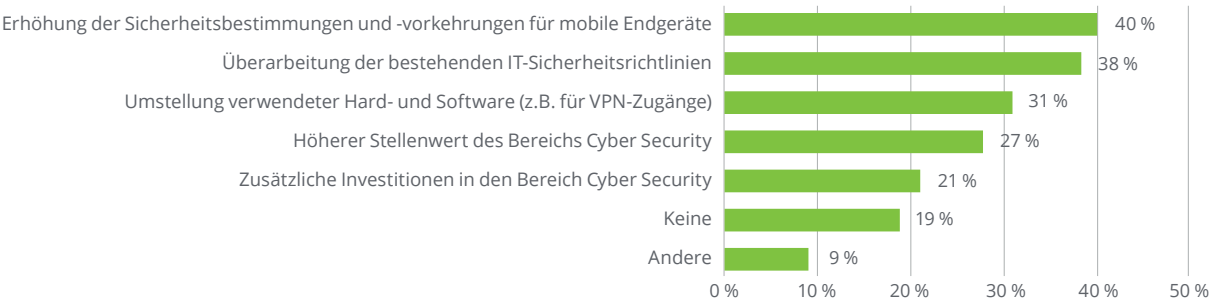
Deloitte View

Auch in den turbulenten Zeiten von COVID-19 setzt man auf bewährte Maßnahmen und auf das Funktionieren des bestehenden Sicherheitskonzeptes. Frei nach dem Motto „More of the same" wurde Home Office in der IT-Architektur vieler Unternehmen bereits berücksichtigt. Es gilt nun sicherzustellen, dass Mitarbeiterinnen und Mitarbeiter, die dies erst kürzlich nutzen, in Bezug auf die Gefahren sensibilisiert werden.

Welche zusätzlichen Maßnahmen im Bereich der Daten- und Informationssicherheit haben Sie zur Bewältigung der neuen Arbeitsbedingungen aufgrund von COVID-19 – gerade in Hinblick auf Home Office – getroffen?



Auf welche Maßnahmen im Bereich der Daten- und Informationssicherheit werden Sie vor dem Hintergrund von COVID-19 in Zukunft fokussieren?



Sample & Methode der Umfrage von Deloitte und SORA zu Cyber Security

Zielpopulation: Unternehmen in Österreich ab 50 Beschäftigte
Erhebungsmethode: Standardisierte Telefonbefragung (CATI) durch SORA
Befragungszeitraum: Jänner 2020
Stichprobe: 535 Unternehmen
Gewichtung: Nach Anzahl der Mitarbeiterinnen und Mitarbeiter sowie nach Bundesland

Sample & Methode der Kurzumfrage von Deloitte zu Cyber Security in Zeiten von COVID-19

Erhebungsmethode: Online-Umfrage
Befragungszeitraum: Mai 2020
Umfrageteilnahme: 114 Unternehmen

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

Kontakt

Alexander Ruzicka
Partner | Risk Advisory
Tel.: +43 1 537 00-7950
aruzicka@deloitte.at

Andreas Niederbacher
Senior Manager | Risk Advisory
Tel.: +43 732 675 290 250
aniederbacher@deloitte.at

Deloitte Audit
Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien

www.deloitte.at

Deloitte.