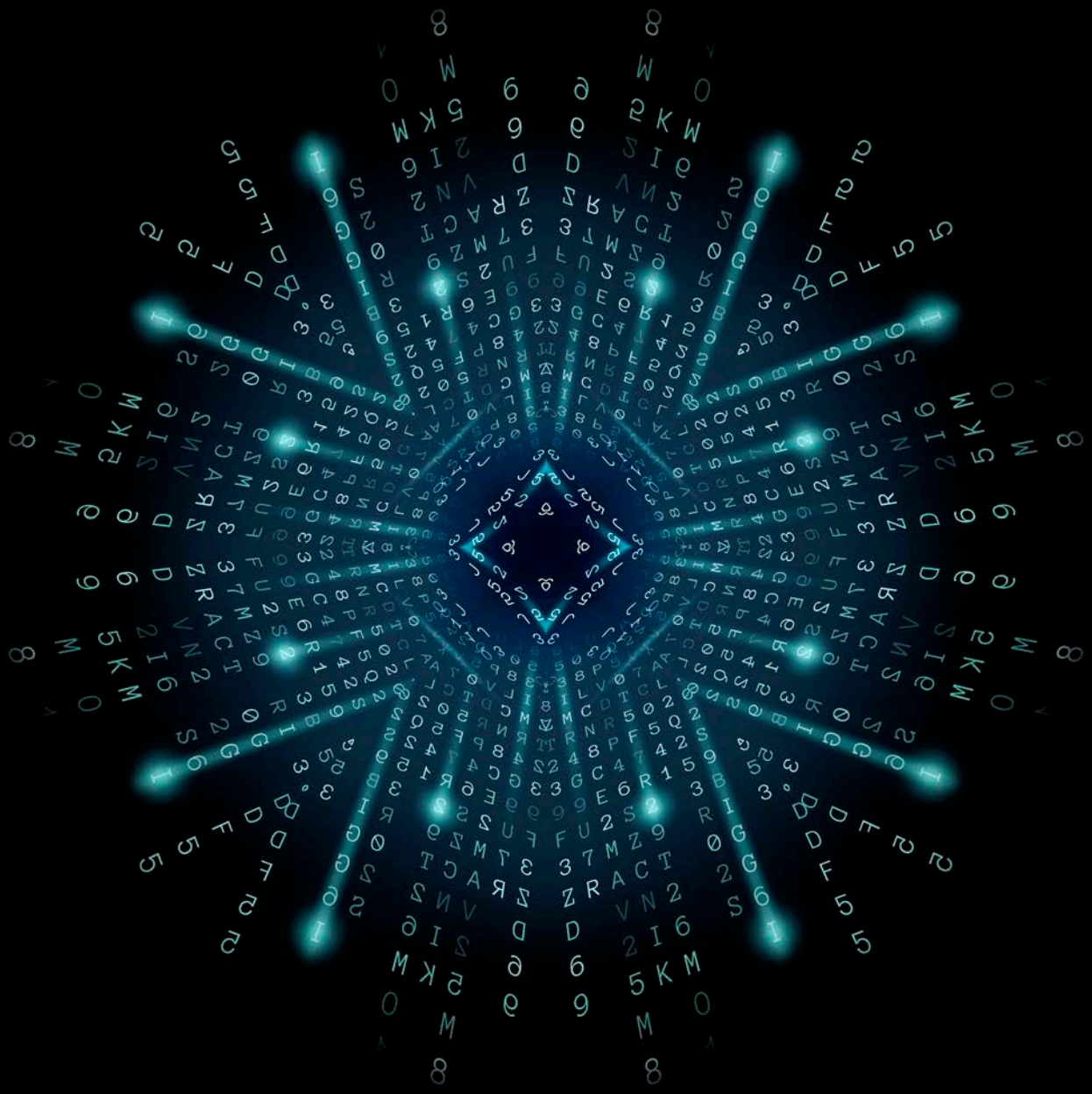
Deloitte.



Deloitte Cyber Security Report 2019

Eine Studie von Deloitte Österreich
in Kooperation mit SORA

Impressum

Herausgegeben von Deloitte Audit Wirtschaftsprüfungs GmbH
Autoren: Alexander Ruzicka und Gilbert Wondracek (Deloitte), Daniel Schönherr und Christoph Hofinger (SORA)
unter redaktioneller Mitarbeit von Armin Nowshad und Gina Grassmann (Deloitte)
Grafik und Layout: Claudia Hussovits

Aus Gründen der einfacheren Lesbarkeit wurde auf die weibliche Form bzw. die Kombination von männlicher und weiblicher Form verzichtet. Es sind selbstverständlich unabhängig von der gewählten Form jeweils beide Geschlechter gleichberechtigt angesprochen.

Vorwort

Zwischen Dezember 2018 und Jänner 2019 hat das Forschungsinstitut SORA im Auftrag von Deloitte Österreich insgesamt 517 IT-Entscheider in österreichischen Unternehmen mit 50 oder mehr Mitarbeitern zum Thema Daten- und Informationssicherheit befragt. Das Ergebnis der österreichweiten Befragung lässt eine Sicherheitsschere unter heimischen Unternehmen erkennen: Großunternehmen sind um einiges sicherer und besser auf Gefahren vorbereitet als kleine und mittlere Betriebe. Gerade kleinere Unternehmen sind gefordert mehr für die Sicherheit ihrer IT-Systeme zu tun.

Alexander Ruzicka
Partner | Risk Advisory

Gilbert Wondracek
Senior Manager | Risk Advisory

Auch im Jahr 2019 ist Cyber Security für viele österreichische Unternehmen eine große Herausforderung: Rund ein Viertel der Studienteilnehmer[1] fühlt sich beim Thema Cyber Security überfordert. Genauso viele reagieren auch erst nach einem Vorfall mit entsprechenden Sicherheitsmaßnahmen. Dabei waren bereits knapp 9 von 10 Unternehmen von Störfällen betroffen. Die meisten Unternehmen spüren zwar, dass sie in puncto Informationssicherheit verstärkt Maßnahmen setzen müssten, aber vor allem kleineren und mittleren Unternehmen fehlt es an den notwendigen Strukturen und Strategien in diesem Bereich. Viele von ihnen konzentrieren sich auf Althergebrachtes wie den Einsatz einer Antivirus-Software und hoffen, dass die bestehenden Vorkehrungen ausreichen.

Insgesamt zeigt sich: Das subjektive Sicherheitsgefühl sowie das entsprechende Know-how steigen mit zunehmender Unternehmensgröße und vorhandenen Ressourcen deutlich an. Unternehmen, die beim Thema Cyber Security gut aufgestellt sind, investieren mehr und werden damit noch sicherer. Bei schlecht aufgestellten Unternehmen hat das Thema tendenziell eine niedrigere Priorität und somit nimmt auch das Unsicherheitsgefühl immer mehr zu. Diese negative Entwicklung lässt sich vor allem bei KMU beobachten. Sie laufen damit zunehmend Gefahr, Opfer von Cyberangriffen zu werden. Bei Österreichs Unternehmen tut sich beim Thema Datensicherheit eine Schere auf, die auf Dauer einiges an Risikopotenzial in sich birgt.

1) Befragt wurden je nach Verfügbarkeit die Leiter der IT-Abteilung, IT-Administratoren, Datenschutzbeauftragte, Sicherheitsbeauftragte oder Geschäftsführer.

Das Sicherheitsgefühl in heimischen Unternehmen

Bei der Sicherheit von Daten und IT-Systemen fühlt sich nur jedes zehnte Unternehmen absolut sicher. Weitere 45 % geben an, zumindest sehr sicher zu sein. Dazu zählen vor allem umsatzstarke Großunternehmen. Bei fast der Hälfte der Befragten stellt sich die Situation anders dar: 41 % der Unternehmen haben das Gefühl, dass ihre Daten und IT-Systeme nicht völlig sicher sind. Gerade jene, die Informationssicherheit eher als Nischenthema behandeln, fühlen sich tendenziell weniger sicher.

Dementsprechend ist die Überforderung in österreichischen Unternehmen mit knapp einem Viertel relativ hoch. Vor allem Verantwortliche in kleinen Unternehmen geben an, dass sie sich durch potenzielle Gefahren und Schutzmaßnahmen im IT-Bereich oft überfordert fühlen (30 %). Große Betriebe mit mehr Umsatz haben weniger Schwierigkeiten: Hier hat die Informationssicherheit tendenziell eine höhere Priorität, was der Überforderung entgegenwirkt. Beachtlich ist, dass sich 21 % der Sicherheitsbeauftragten und IT-Administratoren sowie sogar 12 % der IT-Leiter überfordert fühlen.

Die Großunternehmen sind im Schnitt auch besser auf potenzielle Vorfälle vorbereitet. Während sich rund ein Viertel der heimischen KMU erst nach einem erfolgten Vorfall mit Sicherheitsthemen auseinandersetzt, agieren 92 % der befragten Unternehmen mit 250 Mitarbeitern und mehr um einiges vorausschauender.

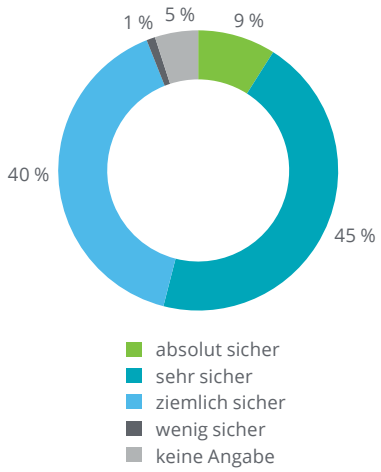
Insgesamt gibt jedoch ein Drittel aller Unternehmen an, dass die Sicherheitsmaßnahmen für die IT deren Arbeit erschwert. Das scheint vor allem die umsatzschwächeren Unternehmen daran zu hindern, sich intensiver mit dem Thema auseinanderzusetzen.

Generell gilt: Die Risiken verschwinden nicht. Im Falle einer Überforderung sollten die Unternehmen externe Unterstützung in Betracht ziehen. Auch geringe Investitionen können außerdem einen großen Beitrag zur Unternehmenssicherheit leisten.

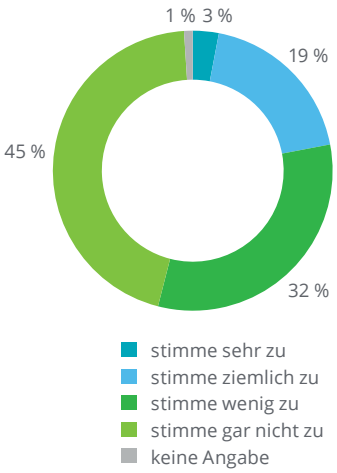
„Der Großteil der befragten Unternehmen will in den nächsten drei Jahren zwischen 10.000,- und 50.000,- Euro in Sicherheitsmaßnahmen investieren. Generell gilt jedoch: Es kommt nicht darauf an, wieviel man ausgibt. Viel wichtiger ist, dass das Thema überhaupt angegangen wird und die Mittel für die richtigen Dinge eingesetzt werden."

Alexander Ruzicka | Partner | Risk Advisory

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



Wenn ich an alle möglichen Gefahren und Schutzmaßnahmen denke, fühle ich mich überfordert



Private und berufliche Nutzung von Endgeräten und Diensten

Zu einem hohen Risiko führt aktuell die Nutzung privater Apps oder Endgeräte für berufliche Belange. Laut Studie nutzt jedoch ein Viertel (26 %) der befragten Unternehmen WhatsApp für Geschäftliches. Im Branchenvergleich liegt der unternehmensbezogene Dienstleistungsbereich besonders weit vorne.

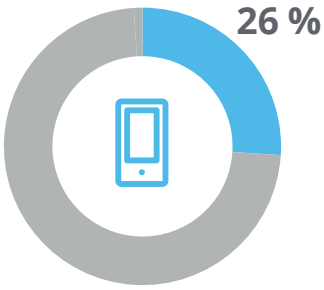
Aus Expertensicht ist von WhatsApp und Co. im beruflichen Kontext jedenfalls eher abzuraten. Der Einsatz von Instant-Messaging-Diensten im Unternehmensumfeld wirft eine Vielzahl an Datenschutzbedenken auf. So ist etwa die Einwilligung aller Mitarbeiter vor der Nutzung notwendig, es braucht einen Vertrag zur Auftragsdatenverarbeitung mit dem Anbieter und die Synchronisation von auf dem Handy gespeicherten Kontakten mit der App ist nur schwer regulierbar. Die meisten Anbieter arbeiten aber derzeit daran, ihre Dienste DSGVO-konform auszugestalten.

In einem Drittel der Unternehmen (31 %) greifen Mitarbeiter für berufliche Zwecke auch auf private Handys, Laptops oder Tablets zurück. Tendenziell ist dies vor allem in kleineren und mittleren Unternehmen verbreitet. Die Vermischung von beruflichem und privatem Gebrauch erleichtert allerdings den Identitätsdiebstahl sowie das Einschleppen von Schadsoftware enorm. Zusätzlich gewöhnt man sich daran, leichtfertig mit sensiblen Informationen umzugehen – wie etwa beim Speichern von Dokumenten am Handy oder am PC zu Hause.

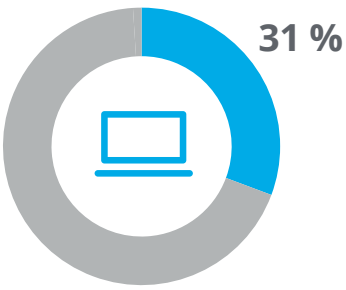
Die Speicherung von Daten in externen Cloud Services ist in 54 % der heimischen Unternehmen noch eher unüblich. Größere Unternehmen nutzen dieser Dienste aber bereits mehrheitlich. In 38 % der Unternehmen können Mitarbeiter zudem von außerhalb auf Unternehmensdaten und -programme zugreifen. Möglich ist das am ehesten bei Großunternehmen, in denen Mitarbeitern auch flexible Arbeitsmodelle wie Home-Office angeboten werden.

Auch in Zukunft geht der Trend in Richtung agilere Arbeitsmodelle. Die Sicherheitsmaßnahmen wachsen jedoch nicht schnell genug mit der Nutzung mit. Hier besteht daher dringender Handlungsbedarf.

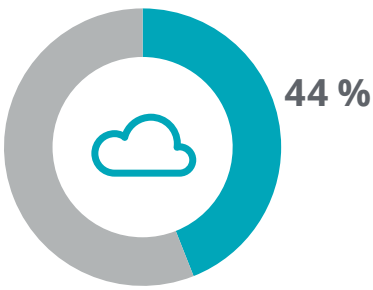
Nutzung von WhatsApp für berufliche Zwecke



Nutzung von privaten Handys, Laptops oder Tablets für berufliche Zwecke



Speicherung von Daten in externen Cloud Services



Bekannte Störfälle und potenzielle Angriffsszenarien

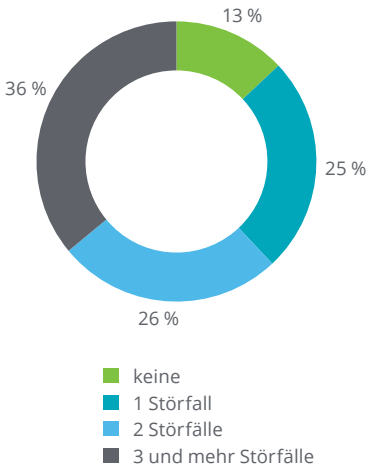
Nur 13 % der Befragten hatten bisher noch keinen Störfall im Unternehmen. Jedes vierte Unternehmen hat einen Störfall erlebt. Weitere 26 % berichten von zwei, 36 % von drei oder mehr Störfällen. Laut Telefonumfrage handelt es sich bei den Störfällen am häufigsten um allgemeine technische Probleme. Davon berichten ganze 77 % der befragten Unternehmen. Einen Befall durch Schadsoftware hat bereits ein Drittel der heimischen Unternehmen erlebt. Bei 16 % der befragten Unternehmen kam es zu Störfällen aufgrund eines leichtfertigen Umgangs mit Daten durch die Mitarbeiter, bei 14 % zu Onlinebetrug und bei ebenfalls 14 % zu Hacker-Angriffen.

In den letzten 12 Monaten waren außerdem 4 % der befragten Betriebe Opfer von Angriffen, die nicht automatisch abgefangen wurden. Als Motivation hinter den Angriffen vermuten die meisten das Lahmlegen von Systemen und Servern sowie Datendiebstahl. In den meisten Fällen hatten diese Angriffe spürbare finanzielle Folgen für die betroffenen Unternehmen.

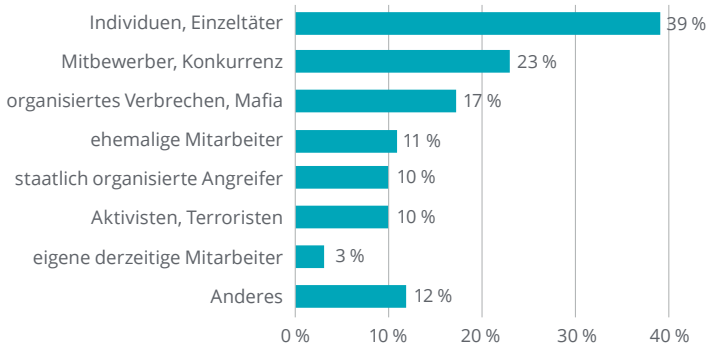
Mit 39 % fürchten sich die meisten Unternehmen vor Angriffen durch individuelle Einzeltäter. 23 % trauen auch dem Mitbewerb gezielte Angriffe zu. Lediglich 11 % haben ehemalige Mitarbeiter im Verdacht. Derzeitige Mitarbeiter stellen nur für 3 % der befragten Unternehmen eine Gefahrenquelle dar.

Das steht in Widerspruch zu dem, was sich bei der Beratung von Unternehmen in der Realität beobachten lässt. Hier kommt es deutlich häufiger zur Informationsmitnahme durch Mitarbeiter oder Racheaktionen von Ex-Kollegen. Diese Diskrepanz legt den Schluss nahe, dass diese Gefahrenquelle vom Großteil der Unternehmen massiv unterschätzt wird. Die Dunkelziffer ist höher, als das Studienergebnis vermuten lässt. Eine diskrete Vorgehensweise bei Sicherheitsüberprüfungen kann hier Schwachstellen aufzeigen, ohne Unruhe im Unternehmen zu verursachen.

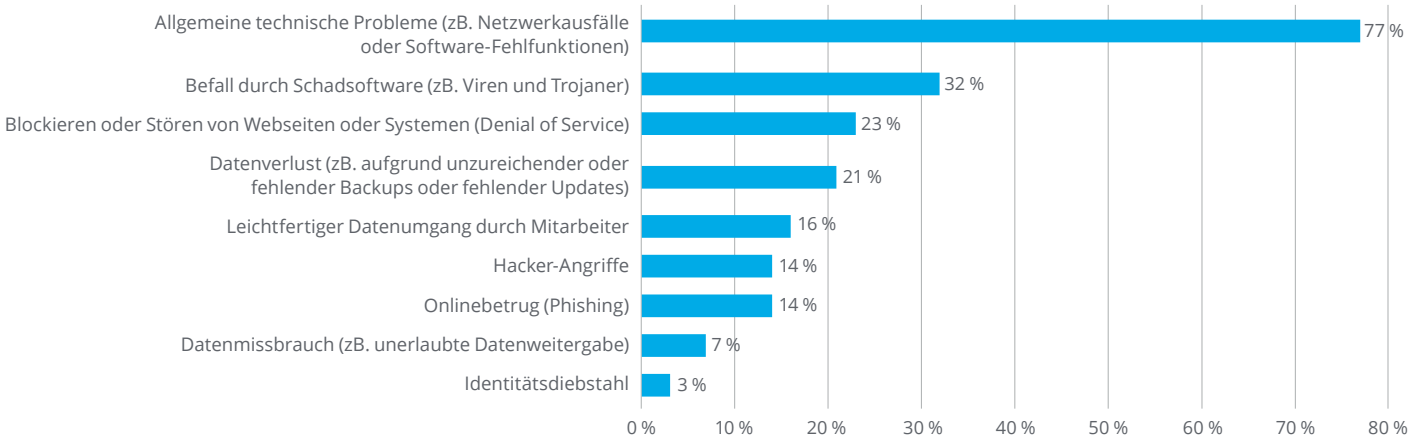
Wie viele Störfälle gab es im Unternehmen in der Vergangenheit?



Von wem befürchten Sie am ehesten Angriffe auf Ihr Unternehmen?



Folgende Szenarien sind im Unternehmen bereits aufgetreten



Sicherheitsmaß-nahmen im Fokus

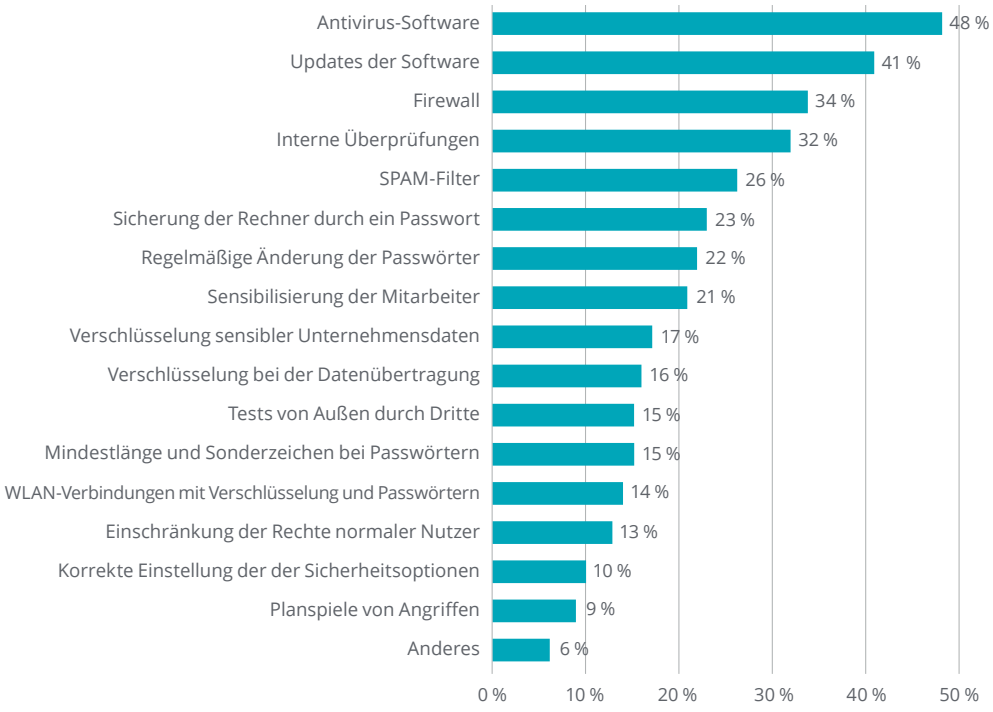
Der Großteil jener Sicherheitsmaß-nahmen, auf die sich die befragten Unternehmen in Zukunft konzentrieren wollen, sollten laut Einschätzung der Deloitte Experten bereits Standard sein. So stehen bei 48 % der Einsatz einer Antivirus-Software und bei 41 % Softwareupdates im Fokus. Wichtige Maßnahmen wie die korrekte Einstellung der Sicherheitsoptionen, Planspiele von Angriffen sowie Tests von außen durch Dritte werden in erster Linie von jenen Unternehmen durchgeführt, bei denen Informationssicherheit einen hohen Stellenwert hat und die sich ohnehin sicher fühlen. Je größer der Betrieb, desto öfter wird außerdem auch auf die Sensibilisierung der Mitarbeiter gesetzt – dabei würden besonders kleinere Unternehmen von besser geschulten Mitarbeiter profitieren.

Als Konsequenz der EU-DSGVO wurden außerdem nur von 53 % der Unternehmen zusätzliche Maß-nahmen eingeführt. Hierbei handelte es sich laut Umfrage häufig um große Unternehmen mit mehr Umsatz.

„Viele Unternehmen stecken beim Thema Cyber Security den Kopf in den Sand. Das ist ein großer Fehler. Wer vor dem Hintergrund wachsender Bedrohungen keine Maßnahmen setzt, wird früher oder später zur Zielscheibe. Das sollte auch kleinen Unternehmen bewusst sein."

Gilbert Wondracek | Senior Manager | Risk Advisory

Auf welche Sicherheitsmaßnahmen legen Sie in nächster Zeit Ihren Schwerpunkt?



Fazit

In Österreichs Unternehmen herrscht in puncto Cyber Security noch einiger Aufholbedarf. Vor allem die kleineren Betriebe müssen ihre passive Haltung ablegen und das Thema aktiv angehen. Die Angst vor hohen Kosten ist dabei weitgehend unbegründet. Vor allem, wenn man bedenkt, dass ein etwaiger Schaden oder Datendiebstahl zu weit höheren Kosten führen kann, rentiert sich die Investition in Cyber Security einmal mehr. Mit den richtigen fokussierten Maßnahmen lässt sich die Unternehmenssicherheit bereits mit relativ wenig finanziellem, personellem und zeitlichem Aufwand erhöhen.

Größere Unternehmen sind zwar tendenziell sicherer und haben mehr Budget für Cyber Security zur Verfügung. Doch auch sie sollten sich fragen, ob sie ihre Ressourcen effektiv und für die richtigen Dinge einsetzen.

Unabhängig von der Unternehmensgröße sind die heimischen Betriebe angehalten, sich mit dem Thema Cyber Security intensiv auseinanderzusetzen und ihre bestehenden Sicherheitsmaßnahmen kritisch zu hinterfragen. Denn der Großteil ist der steigenden Zahl an potenziellen Risiken nach aktuellem Stand noch nicht gewachsen. Eine gewisse Grundhygiene und eine klare Strategie sind beim Thema Cyber Security unbedingt notwendig.

Deloitte.