techconsult
The IT Market Analysts

Studie:
New Work, aber sicher

Die Zukunft mobiler Arbeitsumgebungen

Unterstützt durch

DriveLock

Inhalt

Einleitung

Das Jahr 2020 und große Teile des Jahres 2021 standen im Zeichen der Pandemie. Dabei wurden nicht nur viele Einschränkungen und Veränderungen von Privatpersonen verlangt, auch Unternehmen mussten sich an die neuen Gegebenheiten anpassen und in gewisser Weise eine Vorbildfunktion bei der Pandemiebekämpfung einnehmen.

Viele Unternehmen entsandten Mitarbeiter und Mitarbeiterinnen innerhalb kürzester Zeit ins Homeoffice. Damit wurde der Trend der vergangenen Jahre zu Mobile Work und Working from Home massiv beschleunigt.

Doch Mitarbeiter und Mitarbeiterinnen ins Homeoffice zu senden, birgt auch Gefahren.

Denn Cyberkriminelle machen sich den Umstand zu Nutze, dass in den eigenen vier Wänden, die Sicherheitsstandards nicht auf dem Niveau sind, wie innerhalb der geschützten Unternehmenswände – und selbst dort brechen Cyberkriminelle immer wieder durch die Sicherheitsbarrieren durch. Auch Homeoffice-Arbeitsplätze müssen größtmögliche Sicherheit bieten, um Cyberkriminellen nicht Tür und Tor zu öffnen. Lasche Sicherheitsvorkehrungen, der Einsatz von ungesicherten privaten Geräten oder das Fehlen der Kommunikation auf dem „kurzen Dienstweg", um sich von der Legitimität einer scheinbar seriösen E-Mail eines „Kollegen" zu überzeugen, führen zu einer Vervielfältigung möglicher Einfallstore für Cyberkriminelle. Denn eins ist sicher: Die Anzahl von Cyberangriffen steigt weiter an.

- Was ist der Status quo von Homeoffice aktuell?
- Wie werden die Unternehmen in Zukunft mit Büroarbeitsplätzen verfahren?
- Gab es im vergangenen Jahr relevante Sicherheitsvorfälle in Bezug auf mobile Arbeit?
- Wie versuchen Unternehmen gegen die Cyberkriminellen vorzugehen?

Um diese und weitere Fragen zu beantworten, wurden im Rahmen dieser Studie 201 Unternehmen aller Branchen im Juni 2021 zu ihrer Arbeitsgestaltung, ihren Sicherheitsvorkehrungen, aber auch ihren Erkenntnissen im Rahmen der Pandemie untersucht. Im Fokus standen Unternehmen ab 250 Mitarbeitern.

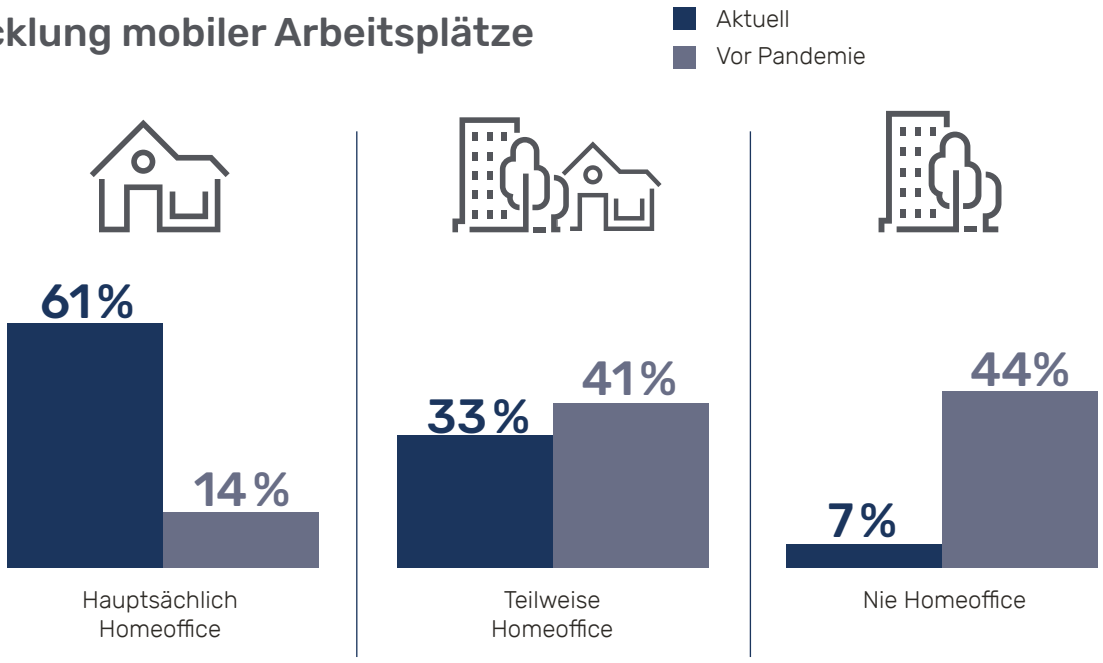
The New Normal – Mobile Work auf dem Vormarsch

In den vergangenen Monaten hatte die COVID-19-Pandemie die Welt fest im Griff. Sowohl im privaten Bereich als auch in Unternehmen waren Veränderungen an der Tagesordnung. Beispielsweise mussten innerhalb kürzester Zeit Kontakte auf ein Minimum reduziert werden. Für Unternehmen hieß dies, klassische Büroarbeitsplätze vorübergehend zu schließen und die eigenen Mitarbeiter ins Homeoffice zu schicken. Für den überwiegenden Teil der Unternehmen war dies eine große Veränderung.

In einigen Unternehmen gab es zwar schon früher die Möglichkeiten zur Arbeit aus dem Homeoffice, doch insgesamt überwog der Anteil von Präsenzarbeitsplätzen. Knapp 44 Prozent der befragten Unternehmen gaben an, vor der Krise ausschließlich Büroarbeitsplätze angeboten zu haben. Bei weiteren 41 Prozent waren sowohl Büroarbeitsplätze als auch Homeoffice-Arbeitsplätze in einem hybriden Arbeitsmodell vorhanden.

Der Rest bot sogar die Möglichkeit, nahezu ausschließlich aus dem Homeoffice zu arbeiten. Im Zuge der Krise hat sich die Arbeitsplatzwahl jedoch drastisch verändert. Auch mit der sogenannten „Homeoffice-Pflicht" seitens der Gesetzgeber waren Unternehmen mehr oder weniger dazu gezwungen ihren Mitarbeitern zumindest die Möglichkeit zu bieten, aus dem Homeoffice arbeiten zu können. Mehr als 60 Prozent der Unternehmen lebte im Juni 2021 ein Modell mit nahezu 100 Prozent Homeoffice. Während ein weiteres Drittel immerhin ein Hybrid-Modell anbot. Nur die wenigsten Unternehmen gaben ihren Mitarbeitern keine Möglichkeiten von zu Hause aus zu arbeiten. Hauptsächlich betrifft das Industrieunternehmen, Finanzdienstleister sowie öffentliche Verwaltungen.

Entwicklung mobiler Arbeitsplätze



Basis: 201 Unternehmen

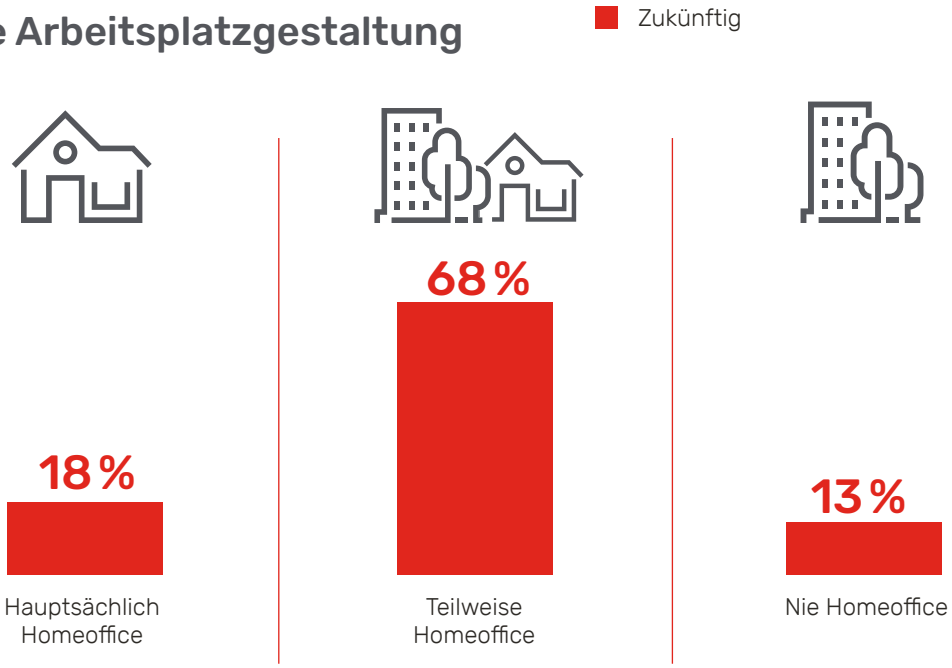
Die Zukunft von Remote Arbeit

Obwohl während der Krise ein Großteil der Unternehmen eine Homeoffice-Strategie gefahren hat, stellt sich natürlich auch die Frage: „Wie wird sich das in Zukunft gestalten?". Sicherlich ist nicht jedes Unternehmen mit der „Homeoffice-Pflicht" zufrieden gewesen und hat dies vielleicht nur zähneknirschend umgesetzt. Für manche Unternehmen kann eine Rückkehr zu Präsenz auch für eine verbesserte Produktivität sorgen. Man denke beispielsweise an interdisziplinäre Teams, die vielleicht an Flipcharts besser kollaborativ zusammenarbeiten können als über Videokonferenzen.

Tatsächlich soll die Arbeit in vollständiger Präsenz aber für viele nur noch eine Randerscheinung sein.

Die überwiegende Mehrheit, mehr als zwei Drittel der Unternehmen, setzt in Zukunft auf ein hybrides Modell, bei dem Mitarbeiter bei Bedarf am Arbeitsplatz sind, aber auch einen gewissen Anteil pro Woche von zu Hause aus arbeiten können. Damit verbinden die Unternehmen die positiven Aspekte der Homeoffice- und der Präsenzwelt und bieten ihren Mitarbeitern die Möglichkeit ihre Arbeitsplatzwahl flexibel an die persönlichen Umstände, Präferenzen und den tatsächlichen betrieblichen Bedarf anzupassen. Wichtige Meetings oder kollaborative Produktentwicklung können vor Ort durchgeführt werden und ortsunabhängige Arbeiten werden aus dem Homeoffice erledigt.

Zukünftige Arbeitsplatzgestaltung



Basis: 201 Unternehmen

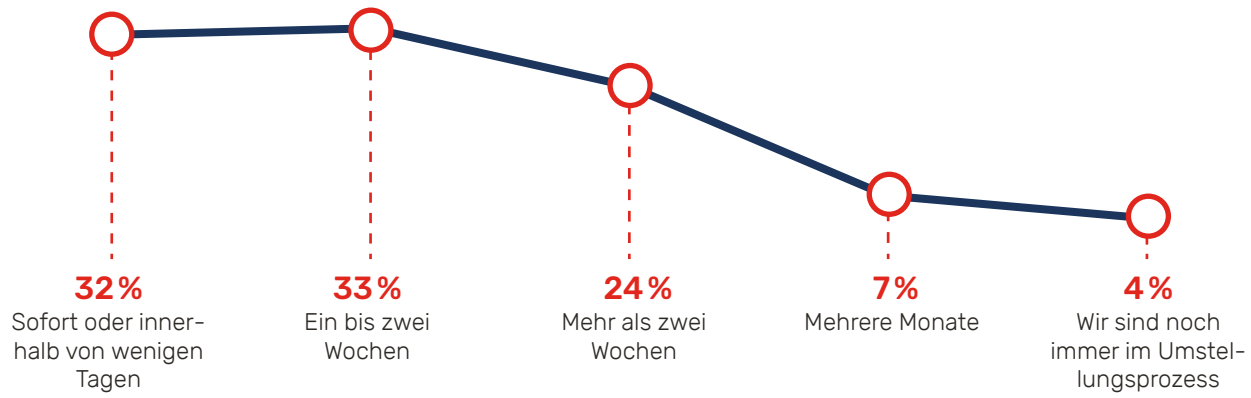
Homeoffice schnell umgesetzt

Jetzt da wir wissen, dass die überwiegende Mehrheit der Unternehmen in irgendeiner Form die Möglichkeiten zum Homeoffice angeboten hat, ist es interessant zu erfahren, wie schnell das Ganze umgesetzt werden konnte. Immerhin wird Deutschland auch mal als „Digitales Neuland" bezeichnet, in dem die Mühlen der Digitalisierung nur sehr langsam mahlen.

Knapp ein Drittel der Unternehmen hatte bereits die technischen Voraussetzungen für das Angebot von Homeoffice Arbeitsplätzen im gesamten Betrieb. Anders lässt sich schwer erklären, wie ein Drittel der Unternehmen bereits binnen weniger Tage die Arbeitsabläufe auf Remote Work umstellen konnte. Das spricht dafür, dass diese Unternehmen bereits weit fortgeschritten in Sachen Digitalisierung waren.

Zukünftige Arbeitsplatzgestaltung

Dauer der Umsetzung



Basis: 201 Unternehmen

Besonders schnell in der Bereitstellung von Homeoffice-Arbeitsplätzen waren sowohl Handelsunternehmen als auch Banken und Versicherungen. 45 Prozent der Befragten aus diesen Branchen gaben an in weniger als zwei Wochen die Arbeitsplätze ins Homeoffice migriert zu haben. Interessanterweise konnten Banken und Versicherungen zwar schnell auf Homeoffice umstellen, haben allerdings vorher nur selten die Möglichkeit für Homeoffice angeboten. Die technischen Voraussetzungen waren also gegeben, doch man verzichtete auf das Angebot mobiler Arbeitsplätze.

Nachzügler sind wenig überraschend die öffentlichen Verwaltungen. Hier gab ein Viertel der Befragten an, mehrere Monate für die Bereitstellung gebraucht zu haben. In öffentlichen Verwaltungen mahlen die Mühlen in der Regel sehr langsam, Prozesse sind komplex und Budgets sehr knapp.

Die Präsenzkultur wird in der Verwaltung noch großgeschrieben. Die Gründe hierfür können vielfältig sein. Vorstellbar wären komplexe Prozesse, niedrige Budgets, eine etablierte Präsenzkultur oder auch starke Reglementierungen. Trotzdem sollten auch öffentliche Verwaltungen versuchen, vor allem im Hinblick auf zukünftige Generationen von Mitarbeitern, durch flexible Arbeitsmöglichkeiten eine attraktive Alternative zu Unternehmen in der freien Wirtschaft darzustellen.

Insgesamt lässt sich für die kommerziellen Bereiche jedoch sagen: Die Digitalisierung war bereits auf einem guten Stand und so konnten mehr als zwei Drittel der Unternehmen binnen 14 Tagen aus dem Homeoffice arbeiten. Es brauchte nur einen Grund um den Mitarbeitern verstärkt mobile Arbeit anzubieten. Die Grundvoraussetzungen waren bereits vorhanden, anscheinend fehlte nur der Wille.

Remote Work: Ja, aber sicher.

Remote Work hat sich also in den vergangenen Monaten etabliert und wird auch in Zukunft bleiben. Doch mobile Arbeitsplätze dauerhaft bereitzustellen ist nur dann sinnvoll, wenn diese auch sicher benutzt werden können und für Unternehmen keine signifikanten Risiken entstehen. Cyberkriminelle haben ihre Angriffsstrategien an die Remote-Worker angepasst und fokussieren diese verstärkt. Gezielte Cyberattacken auf ungeschützte Systeme, ausgeklügelte Phishing-Angriffe oder die Verschlüsselung wertvoller Daten mit gleichzeitiger Lösegeldforderung - die Möglichkeiten für Cyberkriminelle, um Schaden anzurichten sind vielfältig.

Mit der Zunahme von mobilen Arbeitsplätzen, steigt auch die Anzahl an potenziellen Angriffsvektoren. Beispielsweise gab es Unternehmen, bei denen auf private Geräte zurückgegriffen werden musste – mit unterschiedlichen Sicherheitsstandards oder sogar überhaupt keinen.

Möglich ist auch, dass sich Mitarbeiter zu Hause deutlich sicher fühlen und nicht stringent auf die Sicherheitsanweisungen der IT achten.

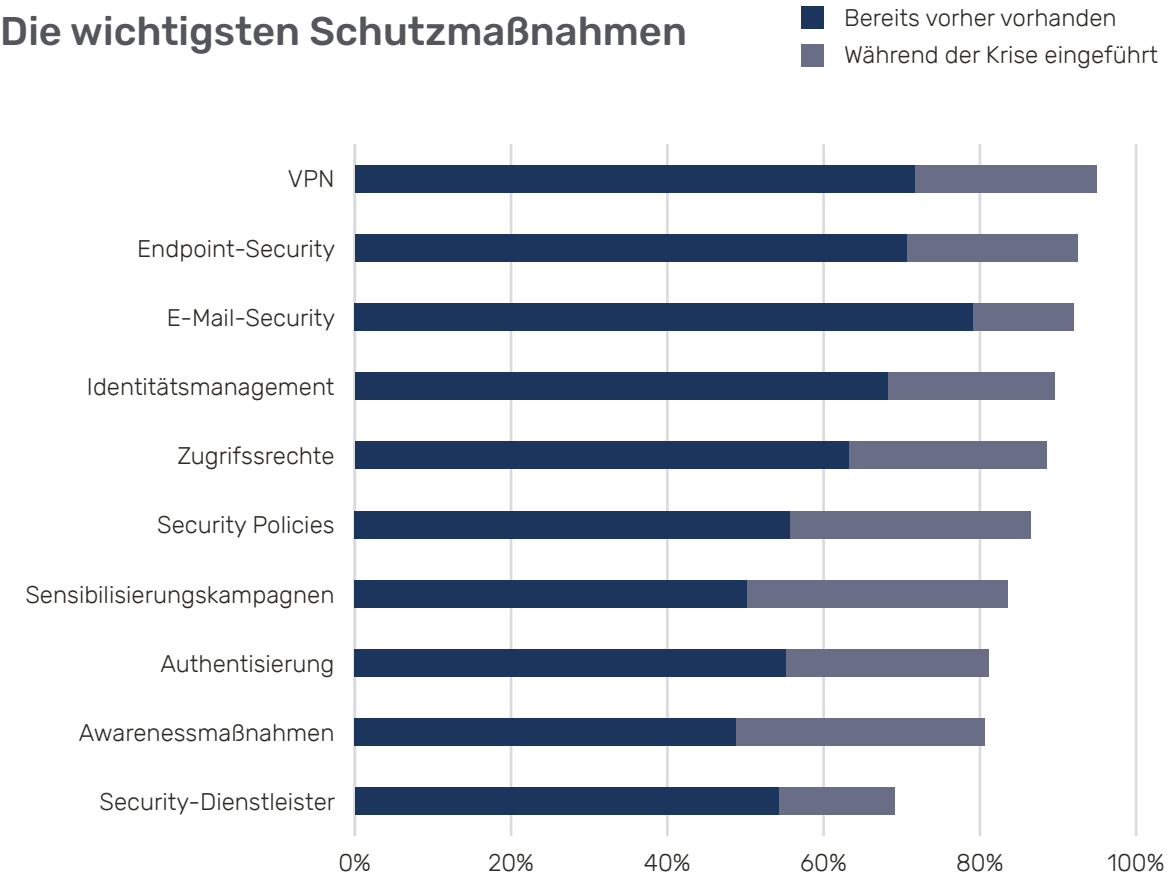
Um die Arbeit von zu Hause sicher zu gestalten, stehen Unternehmen verschiedene Methoden zur Verfügung. Die meisten davon sollten Unternehmen bereits vorher verwendet haben, da es sich um allgemeine IT-Sicherheitsmaßnahmen handelt, die auch für stationäre Arbeitsplätze wichtig sind.

Einige der wichtigsten Maßnahmen waren bereits vor der Krise in den Unternehmen zu großen Teilen vorhanden. Beispiele für Maßnahmen, die schon früher einen großen Einsatzgrad hatten, wären beispielsweise E-Mail-Security (79 Prozent), VPN-Dienste (72 Prozent) oder auch Endpunktsicherheit (71 Prozent). Während der Krise stieg die Verbreitung dieser Lösungen nochmals an und alle drei Maßnahmen sind bei weit über 90 Prozent der Unternehmen im Einsatz.

Im Kontrast dazu waren nicht technische Maßnahmen vor der Krise bei rund der Hälfte der Unternehmen im Einsatz. Dazu zählen beispielsweise Sensibilisierungskampagnen, Awareness-Schulungen oder auch das Aufstellen von Security-Policies für Homeoffice-Arbeitsplätze. Zwar haben auch viele Unternehmen während der Krise schnell organisatorische Maßnahmen ergriffen, doch auch hier gibt es noch Optimierungsbedarf.

Immerhin verzichtet jedes fünfte Unternehmen auf Awareness-Schulungen, um die Mitarbeiter für die Gefahren im Cyberspace zu wappnen. Der Faktor Mensch ist und bleibt aber das schwächste Glied im Bezug auf die Cybersicherheit und lässt sich im Gegensatz zur Technologie, leichter von Cyberkriminellen austricksen.

Die wichtigsten Schutzmaßnahmen



Basis: 201 Unternehmen | Mehrfachnennungen

Den mit Abstand niedrigsten Einsatzgrad erreicht die Zusammenarbeit mit einem Security-Dienstleister. Knapp die Hälfte der Unternehmen hatte vor der Krise bereits einen Dienstleister für die IT-Sicherheit mit an Bord. Doch während der Krise sind nur weitere 15 Prozent dazugekommen. Ein knappes Drittel verzichtet gänzlich auf den Einsatz eines Security-Dienstleisters. Dabei kann dieser insbesondere bei jenen Unternehmen ein wichtiges Instrument darstellen, bei denen die IT-Sicherheit nicht mit dem internen Personal aufrechterhalten oder gar verbessert werden kann.

Die einflussreichsten Maßnahmen

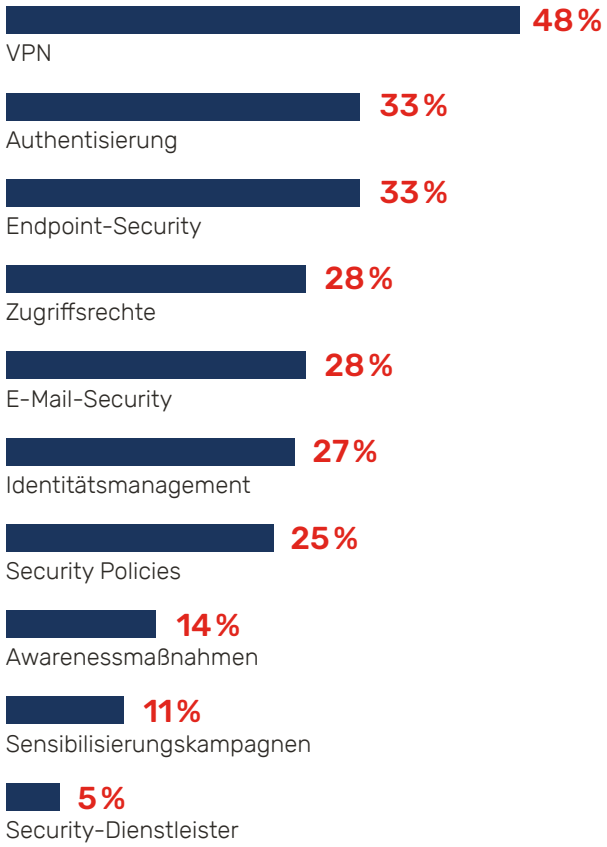
Einen besonders positiven Einfluss auf die Sicherheit an mobilen Arbeitsplätzen hat laut Studienteilnehmern insbesondere der Einsatz von VPN-Diensten gebracht. Knapp die Hälfte der Befragten, hat dieser Maßnahme eine besonders hohe Bedeutung bei der Absicherung von mobiler Arbeit zugesprochen. Mit dem Einsatz von VPN-Diensten können Unternehmen sichere Tunnel vom Heim-Arbeitsplatz zum Betriebsnetzwerk aufbauen.

Dahinter folgen die Einführung von Zwei- bzw. Multi-Faktor-Authentifizierung (MFA) und der Einsatz von Lösungen für die Endpunktsicherheit. Ein knappes Drittel der Befragten spricht diesen Maßnahmen eine hohe Relevanz für die sichere mobile Arbeit zu. Authentisierungsmaßnahmen können einen wichtigen Schutz bieten, beispielsweise wenn ein Passwort in die Hände eines Dritten gelangt. Ohne die Authentisierungsmaßnahmen würde ein gestohlenes Passwort einem Cyberkriminellen direkt Zugang zum Unternehmensnetzwerk bescheren. Mit Authentisierung müsste der Cyberkriminelle noch an weitere Dinge gelangen um sich ins Unternehmensnetzwerk einzuloggen. Das könnte ein Code auf dem Smartphone des Mitarbeiters sein oder ein Hardware-Dongle oder ein Fingerabdruck. Für Unternehmen gibt es eine große Bandbreite an verschiedenen Authentisierungsmaßnahmen, die auch beliebig miteinander kombiniert werden können, um noch größere Schutzwirkung zu erzielen.

Der Einsatz einer Lösung für die Endpunktsicherheit ist ein weiterer Punkt, der von Unternehmen nicht nur hochgeschätzt wird, sondern auch in jedem Unternehmen eingesetzt werden sollte. Heutzutage gibt es sehr viele Endpunkte mit denen Mitarbeiter sich mit dem Unternehmensnetzwerk verbinden können. Rechner, Laptops, Smartphones oder Tablets, all diese Geräte sind in Unternehmen verbreitet. Mit jedem Gerät steigt auch die Anzahl potenzieller Angriffsvektoren für Cyberkriminelle.

Daher ist der Einsatz einer Lösung zum Schutz aller Endpunkte im Unternehmen unerlässlich, um das Gefahrenpotenzial zu minimieren.

Maßnahmen mit den größten Effekten



Basis: 201 Unternehmen | Mehrfachnennungen

Man sollte sich jedoch nicht nur auf eine einzige Maßnahme konzentrieren. Denn erst die Kombination und das Zusammenspiel verschiedener technischer und organisatorischer Maßnahmen sorgen für ein ausreichendes Schutzniveau. Wer beispielsweise nur E-Mail-Eingänge sichert, aber die Endgeräte und die Mitarbeiter außer Acht lässt, wird nicht für eine Verbesserung der Sicherheit sorgen können.

Sicherheitsvorfälle in der Pandemie gestiegen

Während der Pandemie hielten Cyberkriminelle die Füße nicht still. Eher nutzten sie die Chancen und die neue Vulnerabilität der Unternehmen und Mitarbeiter, um sich Zugang zu Unternehmensnetzwerken zu verschaffen. Um das zu bewerkstelligen, kamen Angriffsszenarien, die sich schon in der Vergangenheit für Cyberkriminelle als äußerst lukrativ erwiesen haben, noch stärker zum Einsatz.

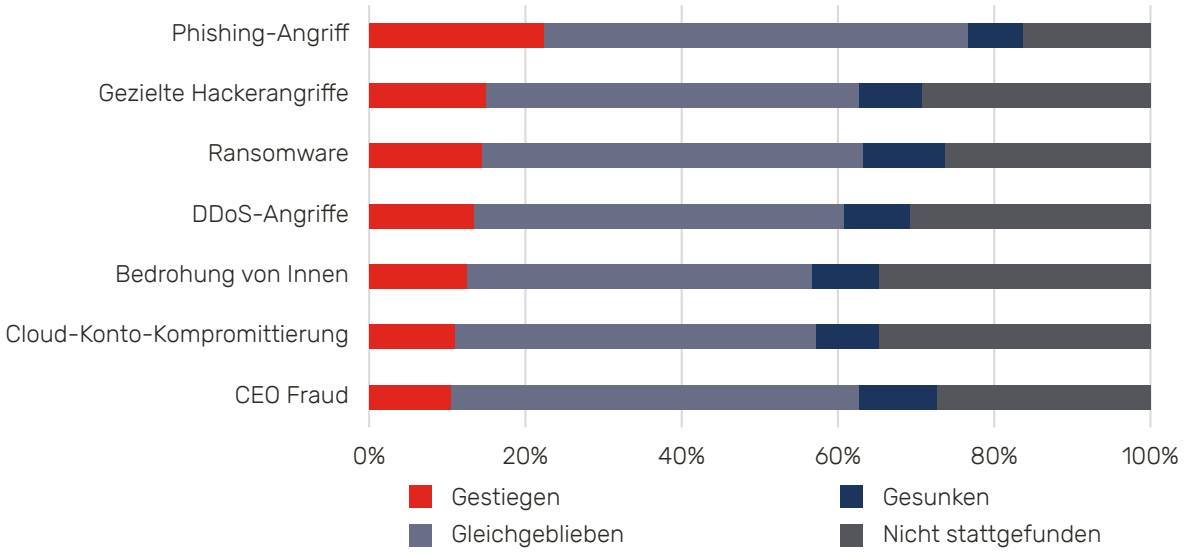
Ein Beispiel für so ein verstärktes Angriffsszenario findet sich im Bereich der Phishing-Angriffe. Ein Fünftel der Unternehmen konnte hier einen klaren Anstieg zu Vor-Corona-Zeiten feststellen. Darüber hinaus berichten weitere 54 Prozent davon, dass die Rate von Phishing-Versuchen auf einem konstanten Niveau geblieben ist. Im Vergleich zu anderen abgefragten sicherheitsrelevanten Vorfällen, haben Phishing-Angriffe die höchste Quote an gestiegenen sowie gleich gebliebenen Angriffen. Öffentliche Verwaltungen standen dabei ganz besonders im Fokus von Phishing-Angriffen.

Hier gab knapp ein Drittel der Befragten an, verstärkt durch Phishing-Angriffe bedroht gewesen zu sein – keine Branche weist auch nur annähernd eine so hohe Steigerungsrate aus.

Der Grund dafür liegt auch auf der Hand. Riesige Mengen sensibler persönlicher Daten von Bürgern sind ein lukratives Ziel für jeden Cyberkriminellen. Darüber hinaus müssen öffentliche Einrichtungen insbesondere in Krisenzeiten handlungsfähig sein.

Hier sollte ein jedes Unternehmen besonderes Augenmerk darauflegen und die Sicherheitsmaßnahmen entsprechend anpassen. Wichtige Mittel, um Phishing-Versuche abzublocken, sind der Einsatz von technischen Sicherheitslösungen wie beispielsweise Endpoint Protection oder E-Mail-Sicherheit, um im Falle eines Phishing-Versuchs automatisch einzugreifen. Aber auch organisatorische Maßnahmen, wie Awareness-Kampagnen oder Sicherheitsschulungen sind von höchster Bedeutung, um bereits im Vorfeld Phishing-Versuche zu unterbinden. Denn wenn Mitarbeiter einen Phishing-Versuch direkt als solchen erkennen können, sinkt die Gefahr für einen Sicherheitsvorfall immens. Die Aussage, dass keine Angriffe stattgefunden haben, muss mit Bedacht betrachtet werden. Vor allem, wenn Unternehmen über keinen hohen IT-Sicherheitsreifegrad verfügen, wird es ihnen schwerfallen, eine verlässliche Bewertung abzugeben, ob ein Angriff stattgefunden hat oder verhindert wurde.

Entwicklung der Cyberangriffe in den vergangenen 12 Monaten



Basis: 201 Unternehmen | Mehrfachnennungen

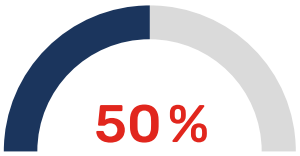
Cyberabwehr – das Maß aller Dinge

Um diese Gefahren nicht nur heute sondern auch in Zukunft abzuwehren, stehen Unternehmen verschiedene Mittel zur Auswahl. Beispielsweise kann neue Sicherheitstechnologie bezogen werden, es kann internes Know-how für die IT-Sicherheit aufgebaut werden, die Mitarbeiter können sensibilisiert werden oder gleich die gesamte IT-Sicherheit ausgelagert werden, sollte man sich nicht in der Lage sehen, den wachsenden Anforderungen gerecht zu werden. Jede Maßnahme erfüllt ihren Zweck und sorgt für eine Verbesserung der IT-Sicherheit.

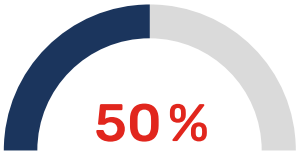
Die Hauptmittel, um sich vor neuen Gefahren zu schützen, sind zum einen der Aufbau von Know-how bei IT-Mitarbeitern und zum anderen die Einführung neuer verpflichtender Regelungen wie beispielsweise der Einsatz von sicheren Passwörtern. Der Aufbau von Know-how ist ein äußerst wichtiges Instrument, vor allem wenn man zukunftsgerichtet agieren möchte. Mit der Verlagerung ins Homeoffice sind in vielen Unternehmen auch die Anzahl und die Komplexität der Aufgaben signifikant gestiegen. Seien es neue Geräte oder auch die Vielzahl von unterschiedlichen kollaborativen Tools. Externe Fachkräfte sind aufgrund ihrer Nachfrage über alle Branchen hinweg oftmals schwierig zu bekommen. Die Bedarfe der Unternehmen können dadurch in vielen Fällen nicht gedeckt werden. Daher ist es ratsam, die vorhandenen Kompetenzen der eigenen IT-Mitarbeiter noch weiter auszubauen, um auch in Zukunft proaktiv Maßnahmen zum Schutz vor IT-Gefahren zu gestalten.

Die Einführung neuer, verbindlicher Regelungen stellt hingegen eine Maßnahme dar, die man als niedrigschwellig bezeichnen kann. Richtlinien für sichere Passwörter, eine Pflicht zur Nutzung von VPN oder die Einführung von Authentisierungsmaßnahmen, die man auch bequem über das Smartphone nutzen kann, stellen Sicherheitsmaßnahmen dar, die keine großen Investitionen benötigen und dadurch schnell und relativ unkompliziert implementiert werden können. Aber auch mitarbeiterzentrierte Maßnahmen wie die gezielte Sensibilisierung für die neuen Angriffsvektoren, beispielsweise über praxisnahe Schulungen und der Erwerb neuer, moderner Sicherheitstechnologie stehen bei Unternehmen hoch im Kurs.

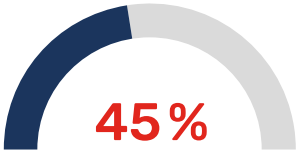
Mit welchen Mitteln werden Cyberangriffe verhindert



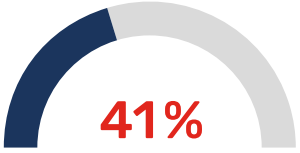
Einführung neuer Regeln und Pflichten (bspw. Sichere Passwörter)



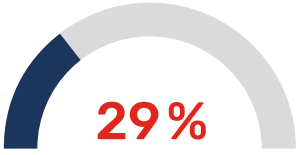
Aufbau von Know-how bei IT-Mitarbeitern



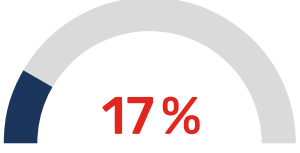
Gezielte Sensibilisierung auf neue Angriffsvektoren



Erwerb neuer Security-Technologie



Überarbeitung bestehender Regeln



Auslagerung der IT-Sicherheit an einen Dienstleister

Basis: 201 Unternehmen | Mehrfachnennungen

Bedrohungslage verschärft sich nochmals

Da auch in Zukunft permanent an der IT-Sicherheit gefeilt werden muss und man sich nicht auf den vergangenen Erfolgen ausruhen darf, sollte die IT-Sicherheit weiter ganz oben auf der Prioritätsliste stehen. Insbesondere vor dem Hintergrund, dass nicht mit einer Abflachung der Bedrohungslage zu rechnen ist. Eher wird sich die Bedrohungslage noch verschärfen.

Das sehen fast 40 Prozent der befragten Unternehmen auch so. Sie gehen davon aus, dass in Zukunft noch mehr und noch verheerendere Cyberangriffe erfolgen werden. Knapp 54 Prozent gehen davon aus, dass die Bedrohungslage auf einem stabilen hohen Niveau verbleiben wird. Und nur die wenigsten gehen von einer Entspannung aus.

Bedrohungslage für Unternehmen

Wir erwarten in Zukunft eine Verschärfung der Bedrohungslage

Wir glauben, die Bedrohungslage bleibt in etwa gleich

Wir glauben, dass sich die Bedrohungslage entspannen wird

Basis: 201 Unternehmen

Dass die Erwartung der steigenden Cyberangriffe real ist, zeigt ein Beispiel aus der näheren Vergangenheit. Erst vor kurzem wurden tausende Kunden, darunter auch deutsche Unternehmen, Opfer eines Hackerangriffs auf den von ihnen eingesetzten US-amerikanischen Dienstleister. Laut Aussage der Hackergruppe konnte sie mehr als eine Million Computer infizieren. In Schweden wurden bei diesem Angriff beispielsweise die Kassensysteme einer der größten Supermarktketten des Landes blockiert.

Dadurch war das Unternehmen gezwungen alle 800 Filialen zu schließen. Die Cyberkriminellen forderten nebenbei knapp 70 Millionen „Lösegeld", um die infizierten Computer wieder freizugeben.

Das zeigt einmal mehr die globale Reichweite der Cyberkriminellen und wie einfach es ihnen teilweise gemacht wird, sich in Unternehmensnetzwerke einzuschleusen. Deswegen sollte jedes Unternehmen allerhöchste Vorsicht walten lassen und jede Möglichkeit in Anspruch nehmen, das eigene Unternehmen vor den großen Gefahren zu schützen.

Hindernisse der IT-Security-Umsetzung

Doch woran liegt es, dass viele Unternehmen trotz des Bewusstseins für das Gefahrenpotenzial weiterhin so anfällig sind für erfolgreiche Cyberattacken? Für die teils nicht optimale Umsetzung von IT-Sicherheitsmaßnahmen gibt es eine Vielzahl von Gründen. Diese können organisatorischer oder monetärer Natur sein oder auch technisch bedingt, beispielsweise durch unzureichende Infrastruktur.

Positiv kann man sehen, dass nur wenige Unternehmen keinen Nutzen für umfassende Security-Konzepte erkennen. Das Bewusstsein, dass die ganzheitlichen Methoden oder Bereitstellungsformen von IT-Security ihnen auf Dauer helfen würden, ist definitiv vorhanden. Doch warum es nicht umgesetzt wird, steht auf einem anderen Blatt.

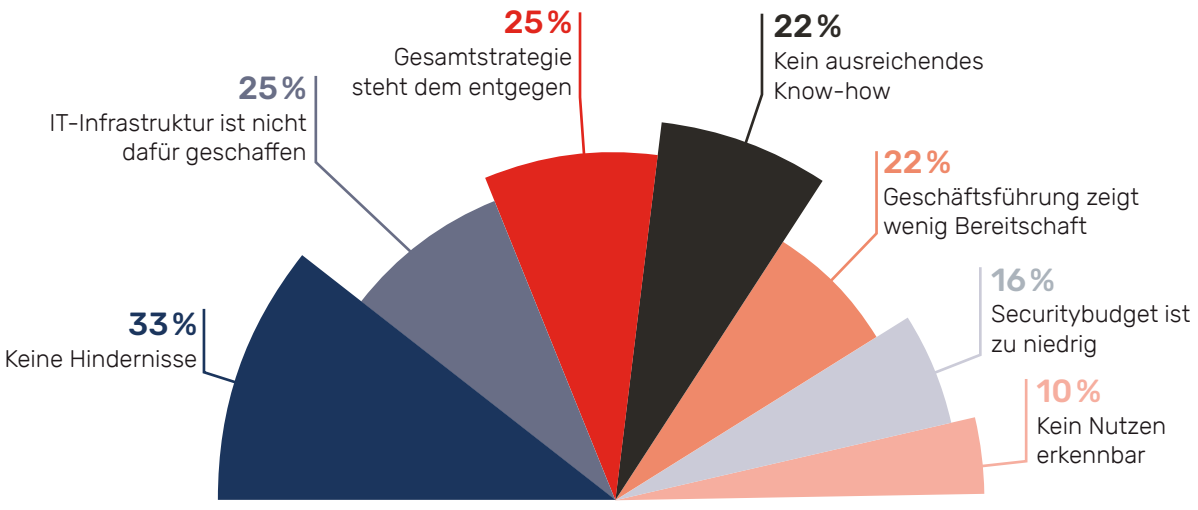
Eine der häufigsten Ursachen, warum es bei der Umsetzung von IT-Sicherheitskonzepten hapert, ist die Tatsache, dass in vielen Unternehmen eine IT-Infrastruktur vorherrscht, die das Implementieren von IT-Security-Konzepten und -Lösungen nicht oder nur schwer ermöglicht. Das gab knapp ein Viertel der Unternehmen zu Protokoll.

Besonders bei historisch gewachsenen IT-Systemen mit vielen Legacy-Anwendungen, vielen Insellösungen und wenig Standardisierung kann die Implementierung von komplexen IT-Security-Lösungen die Unternehmen vor erhebliche Probleme stellen.

Budgetprobleme hingegen sind insgesamt gar nicht der ausschlaggebende Grund. Hauptsächlich die öffentlichen Verwaltungen sehen dies als Kernproblem bei der Einführung von IT-Sicherheitsmaßnahmen. Hier gibt ein Drittel der Befragten an, aus Budgetgründen keine weiteren IT-Security-Maßnahmen durchführen zu können.

Unternehmen, die Probleme bei der notwendigen Modernisierung und Verbesserung ihrer IT-Sicherheit haben, sollten genau überlegen, ob sie ihr Unternehmen weiterhin den Gefahren aussetzen wollen, oder ob sie beispielsweise auf cloudbasierte Lösungen setzen möchten. Wenn die Infrastruktur nicht geeignet ist oder es an monetären Mitteln für die Neuanschaffung von Security-Infrastruktur fehlt, können schnell einsatzfähige Cloudlösungen Abhilfe schaffen.

Hindernisse bei der Einführung von IT-Security



Basis: 201 Unternehmen

Strategien und Konzepte für die IT-Sicherheit

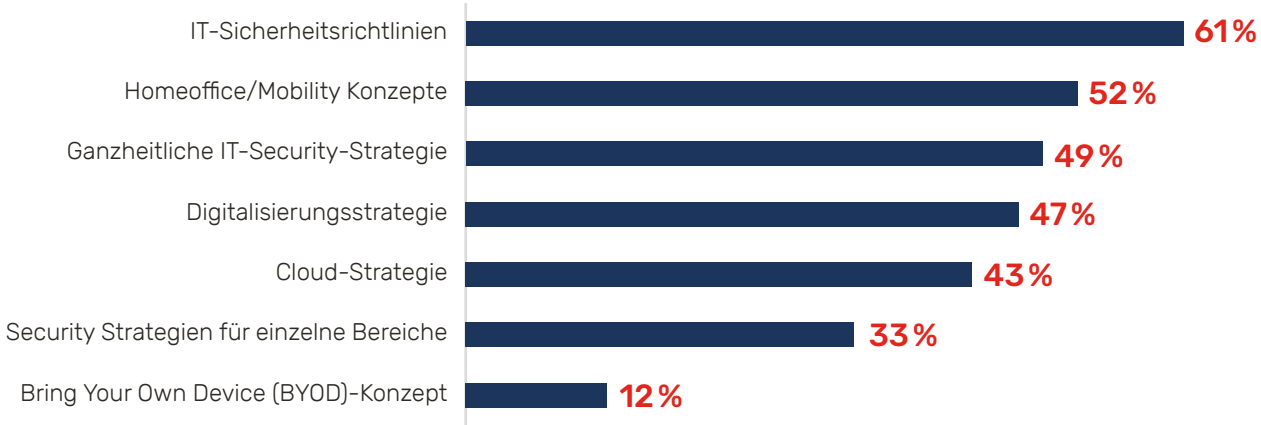
Betrachtet man die verschiedenen Strategien, Konzepte und Einzelmaßnahmen, die Unternehmen umsetzen, so fällt auf, dass IT-Sicherheit in den meisten Unternehmen einen hohen Stellenwert genießt. Gleichzeitig sind die Zahlen teilweise aber auch ernüchternd. Insgesamt scheint es, als würde eine große Zahl der Unternehmen ohne ausgefeilte Konzepte und Strategien arbeiten und Entscheidungen über IT-Sicherheit oder Mobilität eher ad-hoc treffen.

Die Mehrheit der Unternehmen verwendet Einzelmaßnahmen statt ganzheitlicher IT-Security-Strategien. Beispielsweise haben drei von fünf Unternehmen IT-Sicherheitsrichtlinien in ihren Unternehmen implementiert. Dazu zählen unter anderem Passwortrichtlinien oder auch Regelungen zum Umgang mit vertraulichen Daten. Besonders stark setzen Banken und Versicherungen auf solche Richtlinien. Hier geben mehr als drei Viertel der Finanzdienstleister an, Sicherheitsrichtlinien für die IT aufgestellt zu haben. Bei einer Branche, die stark reguliert ist und mit hochsensiblen Daten arbeitet, nicht wenig verwunderlich. Die Einführung von einzelnen Richtlinien ist mit vergleichsweise wenig Aufwand verbunden. Die Kosten und die Personalressourcen sind überschaubar und Richtlinien können sehr einfach rausgegeben werden.

An zweiter Stelle folgen bereits Konzepte für den sicheren Betrieb von Homeoffice-Arbeitsplätzen. Knapp die Hälfte der Unternehmen hat einen durchdachten Plan, wie Homeoffice umgesetzt wird und wie ein sicherer und effizienter Betrieb gewährleistet wird. Bedeutet allerdings auch im Umkehrschluss, dass auch die Hälfte der Unternehmen auf Sicht fährt und überhaupt keinen definierten Plan hat, wie Mobilität in ihren Unternehmen umgesetzt werden soll. Hier herrscht dringender Nachholbedarf, vor allem wenn man bedenkt, dass Homeoffice nicht mehr verschwinden wird und Cyberattacken nicht weniger werden.

Eine ganzheitliche IT-Security-Strategie ist immerhin bei knapp der Hälfte der Unternehmen ein wichtiger Bestandteil der Cyberabwehr. Unternehmen, die über eine solche Strategie verfügen, geben sich nicht mit Insellösungen zufrieden. Sie sehen IT-Sicherheit als das „große Ganze" und sind bestrebt, eine ganzheitliche Cybersecurity im Unternehmen einzuführen. Weg von kleinteiligen Einzelschritten, die unter Umständen nicht einmal im Einklang miteinander funktionieren, hin zu unternehmensweiten IT-Sicherheitsmaßnahmen, die alle denselben hohen Anforderungen und Standards gerecht werden.

Sicherheitsstrategien und -konzepte

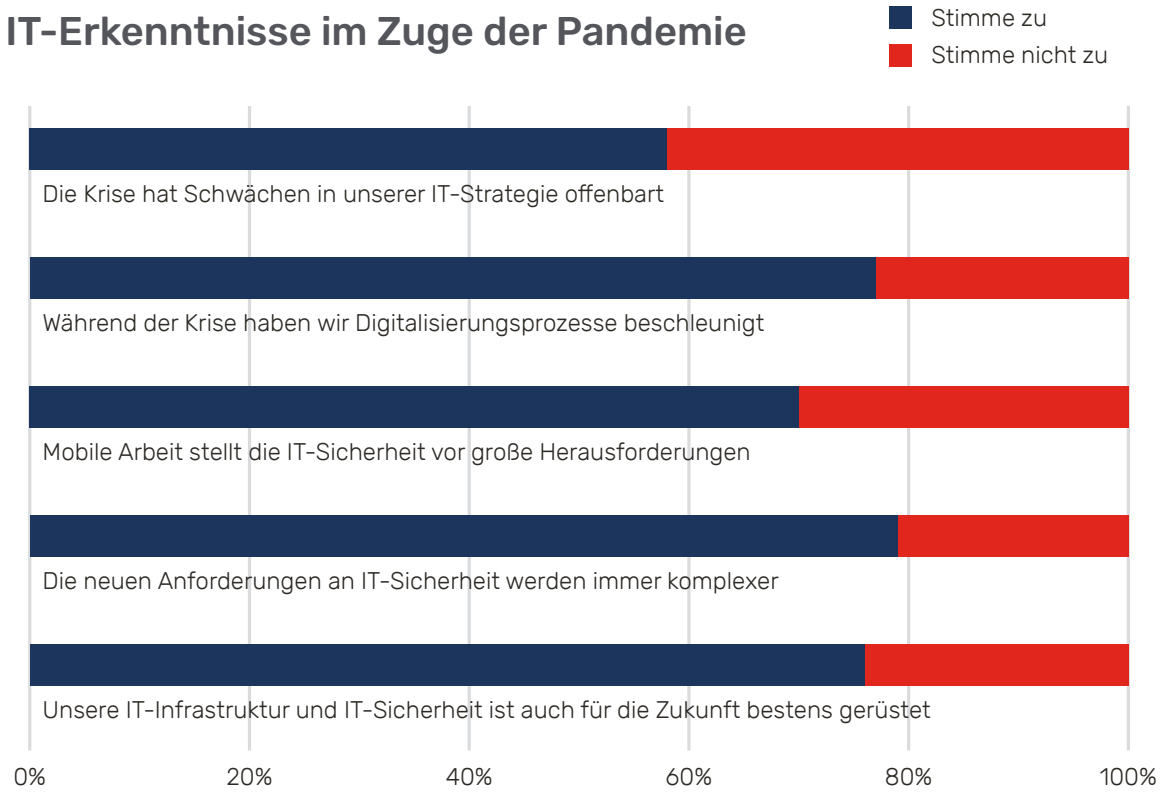


Basis: 201 Unternehmen | Mehrfachnennungen

Zu guter Letzt: Was wurde gelernt?

Die Krise wirkte in vielen Unternehmen als Ventil, um Versäumnisse der Vergangenheit zu erkennen und aufzuzeigen, dass viele Herausforderungen nicht einfach zu lösen sind und auch in Zukunft schwierig bleiben. Beispielsweise sagen knapp 80 Prozent der Unternehmen, dass die Anforderungen an IT-Sicherheit immer komplexer werden.

Vor allem öffentliche Verwaltungen (86 Prozent) stimmen dieser Aussage vollends zu. Besonders dann, wenn im eigenen Unternehmen, das nötige Know-how und die nötigen finanziellen Mittel fehlen, um Technologie zu erwerben und Wissen aufzubauen, steht Cyberkriminellen in Zukunft Tür und Tor offen.



Basis: 201 Unternehmen | Mehrfachnennungen

Unternehmen, die selbst erkennen, dass sie den Anforderungen an IT-Sicherheit bald nicht mehr gerecht werden können, sollten die Problemfelder schleunigst angehen. Wenn es nicht für den Aufbau von internem Know-how reicht, sollte das Hinzuziehen eines IT-Security-Dienstleisters nicht ausgeschlossen werden.

Gleiches gilt für den verstärkten Einsatz von Homeoffice-Arbeitsplätzen. Knapp 70 Prozent der Unternehmen sehen in mobiler Arbeit einen Gefahrenherd, der ihnen zunehmend Kopfschmerzen bereitet. Denn die Absicherung der mobilen Arbeitsplätze stellt die IT vor Herausforderungen.

Im Homeoffice kann das Schutzniveau der eigenen vier Betriebswände nicht aufrechterhalten werden. Daher braucht es vor allem nicht nur technische Schutzkonzepte, sondern auch allgemeingültige Regeln und ergänzende mitarbeiterbezogene Maßnahmen, um das höchstmögliche Sicherheitsniveau zu gewährleisten.

Fazit

Die Krise hat die Art und Weise wie wir arbeiten nachhaltig verändert. Weg von starren Büroarbeitsplätzen hin zu mobilen Arbeitsplätzen. Diese neuen Arbeitsplätze werden auch in Zukunft nicht verschwinden, sondern ein Teil der Arbeitswelt werden. Für Unternehmen und Mitarbeiter bedeutet ein hybrides Modell, bestehend aus Homeoffice und Präsenzarbeit, viele Vorteile.

Dabei ist das „New Normal" gar nicht so neu wie es scheint. Denn bereits vor der Pandemie waren die Voraussetzungen zur mobilen Arbeit in vielen Bereichen bereits gegeben. Es fehlte lediglich der Anstoß, um das Ganze auch tatsächlich in der Breite umzusetzen. Deshalb konnten viele Unternehmen auch in sehr kurzer Zeit Homeoffice für ihre Mitarbeiter bereitstellen.

Doch trotz der raschen Etablierung von Homeoffice-Arbeitsplätzen darf die IT-Sicherheit nicht vernachlässigt werden. Denn Cyberkriminelle wissen um die Anfälligkeit von mobilen Arbeitsplätzen. Sei es die technische Security-Ausstattung, die zu Hause nicht mit der im Büro mithalten kann, als auch der Mitarbeiter selbst, der das schwächste Glied in der IT-Security-Kette ist und von Cyberkriminellen gerne gezielt angegriffen und ausgetrickst wird.

Unternehmen und öffentliche Verwaltungen sollten daher stets die Veränderungen der Angriffsszenarien im Blick haben und ihre IT-Sicherheit stetig anpassen und verbessern. Nur so kann ein sicherer Betrieb gewährleistet werden. Denn die Cyberangriffe werden auch in Zukunft nicht abnehmen, sie werden sowohl in Anzahl als auch ihrer Schwere immer stärker werden. Das zeigen Beispiele aus jüngerer Vergangenheit bei denen immer wieder erfolgreich Cyberangriffe weltweit durchgeführt wurden.

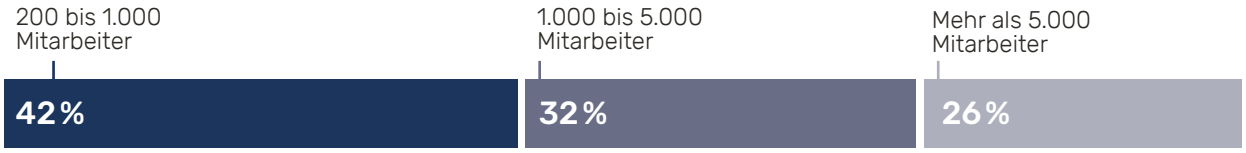
Die Veränderungen werden zu einem großen Teil bleiben. Homeoffice wird weiterhin in vielen Unternehmen seinen Platz finden und von einer Abschwächung der Cyberangriffe kann nicht ausgegangen werden, eher noch werden diese auf hohem Niveau weiter bestehen oder gar noch aggressiver werden. Daher ist es für Unternehmen unabdingbar zu handeln, um sichere Bedingungen für eine hybride Arbeitswelt zu schaffen.

Unternehmen, die von der Situation überfordert sind und sich nicht in der Lage dazu sehen, jetzt und besonders in der Zukunft, für einen sicheren Betrieb zu sorgen, sollten die Hilfe eines Experten in Anspruch nehmen. Denn ein erfolgreicher Cyberangriff wird nicht nur finanzielle Schäden verursachen sondern vor allem auch das Vertrauen von Kunden und Partnern erschüttern.

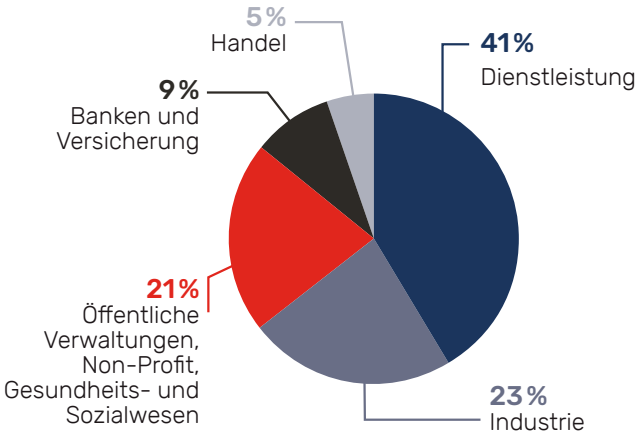
Stichprobe

Die vorliegende Studie „New Work, aber sicher – Die Zukunft mobiler Arbeitsumgebungen" wurde von der tech**consult** GmbH im Auftrag der Drivelock SE konzipiert und durchgeführt. Dabei wurden 201 IT-Verantwortliche und -Entscheider aus Unternehmen im deutschsprachigen Raum zu den Veränderungen der Arbeitswelt, Sicherheitsvorfällen in Bezug auf mobile Arbeit und Abwehrmechanismen gegen Cyberkriminalität befragt. Die Befragung erfolgte im Juni 2021 über einen Online-Fragebogen. Die Stichprobe umfasste Unternehmen ab 250 Mitarbeitern aller Branchen. Ansprechpartner waren in erster Linie IT-Leiter, IT-Fachbereichsleiter sowie IT-Spezialisten.

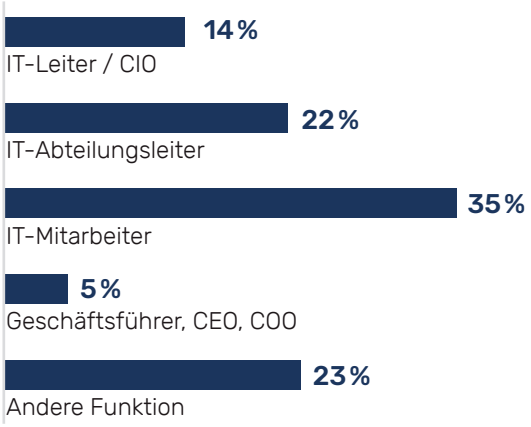
Mitarbeitergrößenklassen



Branchenverteilung



Position



Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.
Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Weitere Informationen

Kontakt für mehr Informationen

Raphael Napieralski
Analyst
tech**consult** GmbH
Baunsbergstr. 37
D-34131 Kassel

E-Mail: raphael.napieralski@techconsult.de
Tel.: +49-561-8109-181

Impressum

tech**consult** GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de
Tel.: +49-561-8109-0
Fax: +49-561-8109-101
Web: www.techconsult.de

Über techconsult GmbH

Die tech**consult** GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt tech**consult** über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

DriveLock SE

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für cloud-basierte Endpoint- und Datensicherheit mit Repräsentanzen in Deutschland, Australien, Singapur, Middle East und USA.

In Zeiten der digitalen Transformation hängt der Erfolg von Unternehmen maßgeblich davon ab, wie zuverlässig Menschen, Unternehmen und Dienste vor Cyberangriffen und vor dem Verlust wertvoller Daten geschützt sind. DriveLock hat es sich zum Ziel gesetzt, Unternehmensdaten, -geräte und -systeme zu schützen. Hierfür setzt das Unternehmen auf neueste Technologien, erfahrene Security-Experten und Lösungen nach dem Zero Trust-Modell. Zero Trust bedeutet in heutigen Sicherheitsarchitekturen einen Paradigmenwechsel nach der Maxime „Never trust, always verify". So können auch in modernen Geschäftsmodellen Daten zuverlässig geschützt werden.

Die DriveLock Zero Trust Plattform vereint die Elemente

- Data Protection
- Endpoint Protection
- Endpoint Detection & Response
- Identity & Access Management

Cloud-basierte Lösungen von DriveLock bieten mehrschichtige Sicherheit; sie sind sofort verfügbar und wirtschaftlich effizient mit niedrigen Investitionskosten. Die DriveLock-Lösungen Device Control und Application Control sind in der Version des Agent 2019.2 nach Common Criteria EAL3+ zertifiziert: Mit dieser international anerkannten Zertifizierung werden die hohe Vertrauenswürdigkeit und der Sicherheitsstandard des DriveLock Agent 2019.2 auf Basis eines vorgegebenen Sets an Konfigurationen attestiert.

Auszeichnungen:

Als Ergebnis der Marktuntersuchung „Cyber Security – Solutions & Services Germany 2020" des Technologieberatungsunternehmens ISG wurde DriveLock als Leader im Segment "Data Leakage/Loss Prevention" ausgezeichnet. In der Anwenderbefragung "Professional User Rating Security Solutions 2021 (PUR-S)" des Analystenhauses tech**consult** positionierten mehr als 2000 Anwenderunternehmen DriveLock als Champion im Bereich Endpoint Protection unter 32 IT-Lösungsanbietern und deren Lösungen in Deutschland.

DriveLock ist Made in Germany und „ohne Backdoor".

- Mehrere Millionen verwaltete Endgeräte in 30 verschiedenen Ländern
- Kundenumgebungen mit über 180.000 verwalteten Endgeräten
- Made in Germany: Entwicklung und technischer Support aus Deutschland

Erstellt durch

techconsult
The IT Market Analysts

Unterstützt durch

DriveLock