techconsult
TECHNOLOGY MARKET ANALYSTS

Cybersecurity im deutschen Mittelstand

Veränderte Bedrohungslage birgt große Gefahren

Unterstützt durch

DriveLock

Inhalt

Sonstige Informationen

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.

Aufgrund von Rundungsdifferenzen summieren sich einige Summen möglicherweise nicht zu 100%

Einleitung

In den vergangenen Jahren wurde viel über IT-Sicherheit gesprochen. So viel, dass jedes Unternehmen eigentlich eine übergreifende IT-Security-Strategie aufweisen müsste. Schließlich ist nicht von der Hand zu weisen, dass sich Cyberkriminelle die durch die Digitalisierung gestiegenen Möglichkeiten für Cyberangriffe zu eigen machen. Denn in den vergangenen Jahren ist die Anzahl und die Schwere von Cyberangriffen kontinuierlich gestiegen.

Dabei sind nicht nur große Unternehmen von Cyberangriffen betroffen, kleine und mittelgroße Unternehmen sind gleichermaßen bedroht. Großunternehmen verfügen im Gegensatz zum Mittelstand über deutlich mehr Ressourcen und Know-how zur Abwehr von Cyberattacken. Knappere Budgets und weniger personelle Kapazitäten, um das eigene Unternehmen auf sich verändernde Bedrohungslagen anzupassen, setzen kleine und mittlere Unternehmen einem enormen Gefahrenpotenzial aus.

Bereits im Jahr 2019 wurden im Rahmen der Studie „IT-Sicherheit im Mittelstand“ kleine und mittlere Unternehmen zu ihrem Umgang mit IT-Sicherheit befragt. In dieser Neuauflage betrachten wir, was sich in den vergangenen vier Jahren, speziell auch durch den Digitalisierungsbeschleuniger „Corona“, in Sachen IT-Sicherheit im Mittelstand verändert hat.

Im Rahmen dieser Studie sollen folgende Fragen geklärt werden:

- Hat die IT-Sicherheit den notwendigen Stellenwert in den mittelständischen Unternehmen?
- Welche Gründe verhindern den Aufbau einer robusten IT-Security-Infrastruktur?
- Was sind die Hauptursachen für Sicherheitsvorfälle?
- Welche Maßnahmen werden ergriffen, um die IT-Sicherheit zu gewährleisten?

Um diese und weitere Fragen zu beantworten, wurden im Rahmen dieser Studie 201 mittelständische Unternehmen aller Branchen im Mai 2023 bezüglich ihrer IT-Sicherheitsmaßnahmen untersucht. Im Fokus standen Unternehmen bis 499 Mitarbeitende.

IT-Sicherheit im Mittelstand: Paradigmenwechsel vollzogen

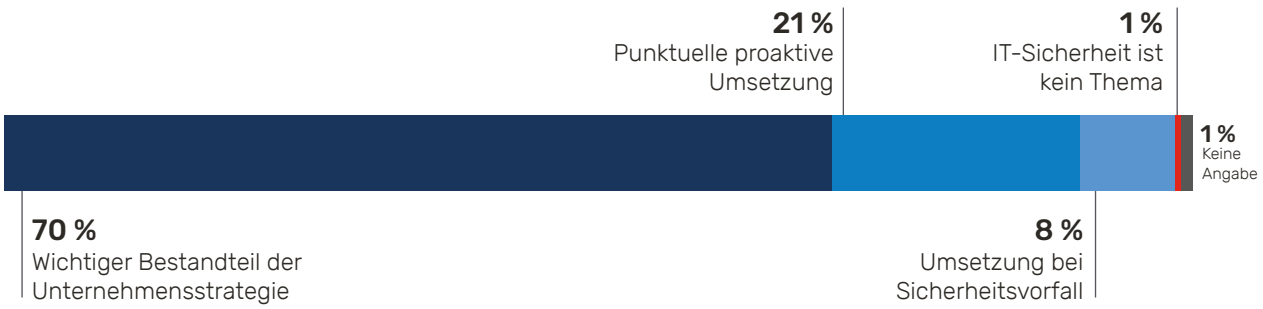
Cyberkriminalität stellt eine lukrative Industrie dar und heute ist es einfacher denn je, Cyberangriffe zu starten. Beispielsweise werden ganze Services angeboten, um auch ohne umfassende Programmierkenntnisse, Attacken auf Unternehmen durchzuführen. Der Einsatz von künstlicher Intelligenz wird diese Entwicklung beschleunigen. Dennoch ist Cyberkriminalität nur eine Gefahr von vielen mit denen Unternehmen konfrontiert werden. Weitere Risiken liegen in der Sabotage durch z.B. staatliche Akteure oder gar Wettbewerber, aber auch in der Unachtsamkeit und fehlenden Sensibilisierung der Mitarbeitenden – bspw. beim Öffnen von E-Mail-Anhängen, dem Verlust von Datenträgern oder der Nutzung leicht zu umgehender Passwörter.

Unter IT-Sicherheit wird der gesamtheitliche Schutz von IT-Systemen vor Schäden und Bedrohungen verstanden. Sie erstreckt sich über Dateien, Rechner, mobile Endgeräte, Netzwerke bis hin zu Cloud-Diensten. Es sind dabei nicht nur technische Mittel, sondern auch organisatorische Maßnahmen, die zur Erhöhung der IT-Sicherheit beitragen. Auf diese Weise sollen nicht nur akute Bedrohungen abgewehrt werden. Auch wenn sich der Einfluss von IT-Sicherheit nicht direkt in einem Return-on-Investment widerspiegelt, so verhindert eine robuste IT-Security-Infrastruktur, dass weitreichende Schäden im eigenen Unternehmen entstehen. Solche weitreichenden Schäden können etwa Datenverluste und damit zusammenhängende Reputationsverluste sowie DSGVO-Sanktionen, aber auch Produktionsausfälle im Rahmen einer Infektion mit Schadsoftware sein.

Die gute Nachricht: Viele Unternehmen haben bereits auf die zugespitzte Bedrohungslage reagiert und sehen IT-Sicherheit als wichtigen Pfeiler ihres Unternehmens. Während bei der letzten Erhebung im Jahr 2019 knapp 55 Prozent der Unternehmen die IT-Sicherheit als wichtigen Bestandteil der übergeordneten Unternehmensstrategie angesehen haben, sind es jetzt bereits 70 Prozent. Es lässt sich klar erkennen, dass ein Paradigmenwechsel innerhalb der letzten Jahre stattgefunden hat und das Bewusstsein für IT-Sicherheit heute deutlich stärker ausgeprägt ist, als dies noch vor vier Jahren der Fall war.

Dennoch setzen 21 Prozent der befragten Unternehmen IT-Sicherheitsmaßnahmen immer noch nur punktuell um und folgen keiner übergreifenden Strategie. Weitere 8 Prozent werden sogar erst dann aktiv, wenn ein Sicherheitsvorfall aufgetreten ist.

Stellenwert der IT-Security



Basis: 201 Unternehmen

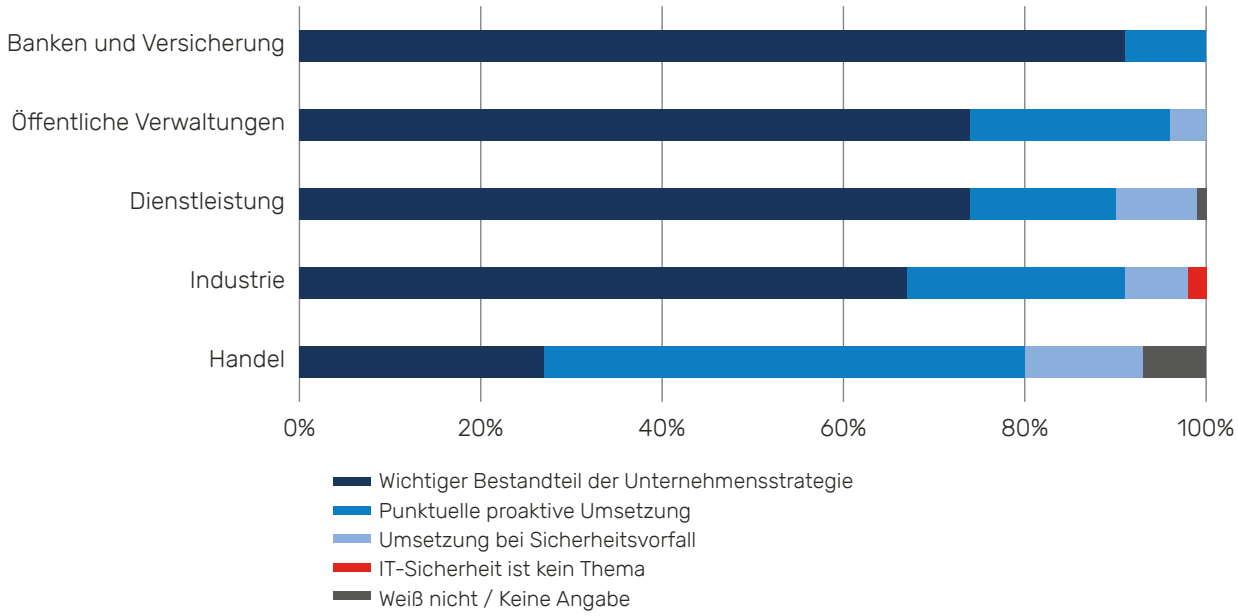
Handel mit viel Nachholbedarf

Auffällig ist die Einschätzung der Handelsunternehmen. Nur gut ein Viertel der Handelsunternehmen gewährt der IT-Sicherheit einen wichtigen Platz innerhalb der Unternehmensstrategie. Das ist sogar noch ein gutes Stück niedriger als bei der letzten Erhebung vor vier Jahren. Damals war noch für knapp 42 Prozent der befragten Handelsunternehmen die IT-Sicherheit wichtiger Bestandteil der Unternehmensstrategie. Die Mehrheit der Handelsunternehmen (53 Prozent) setzt IT-Sicherheitsmaßnahmen punktuell um und handelt beispielsweise erst dann, wenn vom Gesetzgeber neue Vorgaben gemacht werden. Woran das genau liegt, ist schwer zu bestimmen. Vielleicht liegt bei vielen Handelsunternehmen der Fokus primär auf dem Ausbau gewinnbringender Geschäftsmodelle und für IT-Sicherheit bleiben nur noch geringfügige finanzielle wie personelle Ressourcen übrig.

Wie es richtig geht, können Unternehmen am Beispiel von Banken und Versicherungen sehen. Hier stieg der Anteil an mittelständischen Unternehmen aus dem Finanzsektor, die IT-Sicherheit als wichtigen Teil ihrer Unternehmensstrategie sehen, von 75 Prozent auf nun 91 Prozent an.

Stellenwert der IT-Security

Vergleich der Branchen

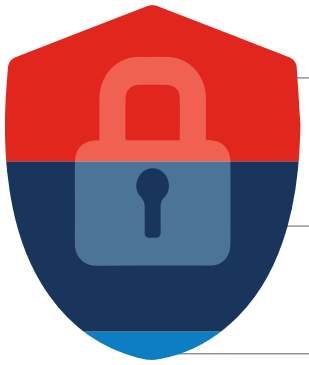


Basis: 201 Unternehmen

Keine Entspannung in Sicht

Wie wichtig Cybersicherheit für alle Unternehmen ist, zeigen die Ergebnisse dieser Umfrage: So gehen 48 Prozent der befragten Unternehmen von einer konstant hohen Gefahr durch Cyberkriminelle in den nächsten Jahren aus. Weitere 44 Prozent erwarten sogar noch eine deutliche Anspannung der Situation. Das deckt sich auch mit den Ergebnissen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieses konnte in seinem 2022er Jahresbericht unter anderem eine Erhöhung von Schwachstellen in Softwaresystemen feststellen und erkannte, dass die Anzahl von DDoS-Angriffen oder auch gezielten, langhaltenden Attacken auf Perimeter-Systeme wie Firewalls (Advanced Persistent Threats) weiter anstieg. Darüber hinaus nahm die Anzahl neuer Schadprogramm-Varianten um knapp 319.000 zu – täglich.

Bedrohungslage für Unternehmen



44 %
Wir erwarten eine deutliche Anspannung der Bedrohungslage

48 %
Wir glauben, dass die Häufigkeit von Cyberangriffen konstant bleibt

8 %
Wir erwarten ein Absinken der Cyberangriffe

Basis: 201 Unternehmen

Top-Verhinderer effektiver IT-Sicherheit: Kosten und Zeit

Warum es in Unternehmen an der Umsetzung von IT-Sicherheit mangelt, liegt vor allem an den Kosten die Unternehmen im Rahmen einer Optimierung ihrer IT-Security erwarten. Die Hälfte der Unternehmen, die noch keine explizite Security-Strategie verfolgen, sieht Kosten als wichtigsten Faktor, der gegen eine Veränderung der IT-Sicherheit spricht.

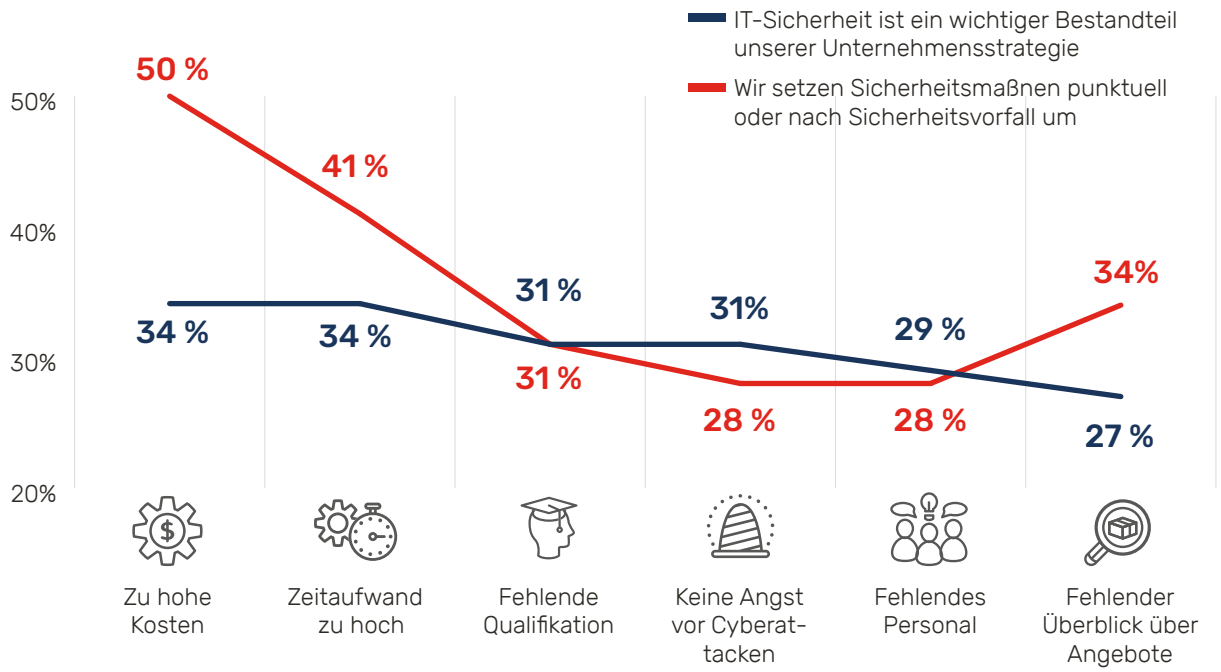
Im Vergleich dazu, würden nur ein knappes Drittel der Unternehmen mit einer übergeordneten IT-Security-Strategie der Aussage „IT-Security-Kosten sind zu hoch“ zustimmen. Im Vergleich zur letzten Erhebung im Jahr 2019 scheint dem Mittelstand die Kostenproblematik mehr zu schaffen zu machen. Damals war nur für rund ein Fünftel der mittelständischen Unternehmen, die IT-Sicherheit mit einer hohen Priorität ausgewiesen haben, die Kostenfrage ein großes Problem. Heute haben zwar deutlich mehr mittelständische Unternehmen eine IT-Security-Strategie, doch scheinen die Budgets nicht in dem Maße angestiegen zu sein, um die Strategie auch wirklich effektiv umzusetzen.

Ein weiterer Faktor, der Unternehmen daran hindert, sich verstärkt mit IT-Sicherheit zu befassen, ist der Zeitaufwand. Rund 40 Prozent der Unternehmen ohne IT-Security-Strategie geben an, dass sie nicht über genügend zeitliche Kapazitäten verfügen.

Bedenklich ist zudem Folgendes: Fast 30 Prozent der Unternehmen, die punktuell Sicherheitsmaßnahmen umsetzen oder erst reagieren, wenn ein Vorfall eintritt, gehen davon aus, gar nicht erst Opfer von Cyberangriffen zu werden.

Aussagen bezüglich der Umsetzung von IT-Sicherheitsmaßnahmen

Vergleich der Unternehmen mit hoher IT-Security-Priorität zu Unternehmen mit niedriger Priorität



Basis: 201 Unternehmen
Nennungen mit „Stimme voll und ganz zu“ und „Stimme zu“

Der Mensch bleibt das beliebteste Einfallstor für Cyberkriminelle

Dass es auch für den Mittelstand ausgesprochen wichtig ist, über eine funktionierende IT-Sicherheitsstrategie zu verfügen, zeigt die Frage, ob es in den letzten Jahren IT-Sicherheitsvorfälle gab. Knapp 64 Prozent der befragten Mittelstandsunternehmen waren in den vergangenen zwei Jahren Opfer von IT-Sicherheitsvorfällen. Das entspricht in etwa dem Anteil der letzten Erhebung. Vor vier Jahren waren 61 Prozent der mittelständischen Unternehmen Opfer von Cyberangriffen.

Die für Cyberkriminelle erfolgreichste Angriffsmethode waren dabei Phishing E-Mails. Mehr als ein Drittel der befragten Unternehmen war von dieser Art von Angriff betroffen. Das ist im Vergleich zu 2019 ein signifikanter Anstieg. Damals war ein Viertel der Unternehmen von Phishing betroffen. Insbesondere zu Beginn der Pandemie stieg der Versand von Phishing-Mails rasant an. Cyberkriminelle nutzten das damals vorherrschende Thema, um große Phishing-Kampagnen durchzuführen.

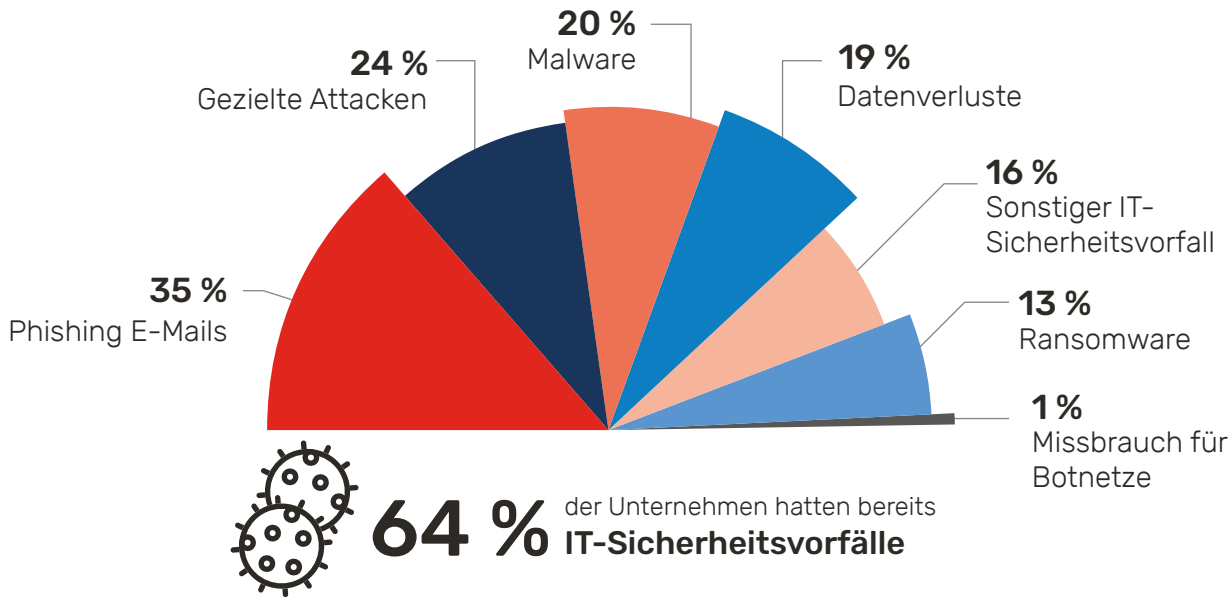
Darüber hinaus gaben knapp ein Viertel der Unternehmen an, Opfer von gezielten Angriffen auf ihre Systeme gewesen zu sein. Zu diesen gezielten Angriffen zählen unter anderem DDoS-Attacken, um die Server des Unternehmens zu überlasten oder gezielte und über einen längeren Zeitraum hinweg andauernde Attacken oder Spionageaktionen (Advanced Persistent Threats).

Nicht zu ermitteln ist die Dunkelziffer der Unternehmen, die aktuell nicht in der Lage sind, einen Sicherheitsvorfall oder einen Datenverlust auch als solchen zu erkennen. Die Folgen einer Ransomware-Attacke, die alle relevanten Daten verschlüsselt, sind für jeden Mitarbeitenden offensichtlich und spürbar. Um aber Datenabfluss zu erkennen, braucht es entsprechende Erkennungsmethoden. Um Datenverlust (z. B. wenn Mitarbeitende eine externe Festplatte verlieren) zu vermeiden, braucht es ebenso entsprechende Prozesse und die Verschlüsselung dieser Datenträger.

Mehrschichtiges Sicherheitssystem notwendig

Um ein ausreichend hohes IT-Security-Niveau zu gewährleisten, braucht es eine Strategie, in der mehrere relevante Lösungen und Maßnahmen zum Einsatz kommen. Um Angreifenden entlang der Kill-Chain ihres Angriffs das Leben so schwer wie möglich zu machen, benötigt es eine mehrschichtige IT-Sicherheit. Wenn das Eindringen in ein Unternehmensnetzwerk mit erheblichem Mehraufwand verbunden ist, wird es für die Angreifenden entsprechend teuer und sie wenden sich leichter anzugreifenden Zielen zu.

IT-Sicherheitsvorfälle in den vergangenen zwei Jahren



Basis: 201 Unternehmen
Mehrfachnennungen

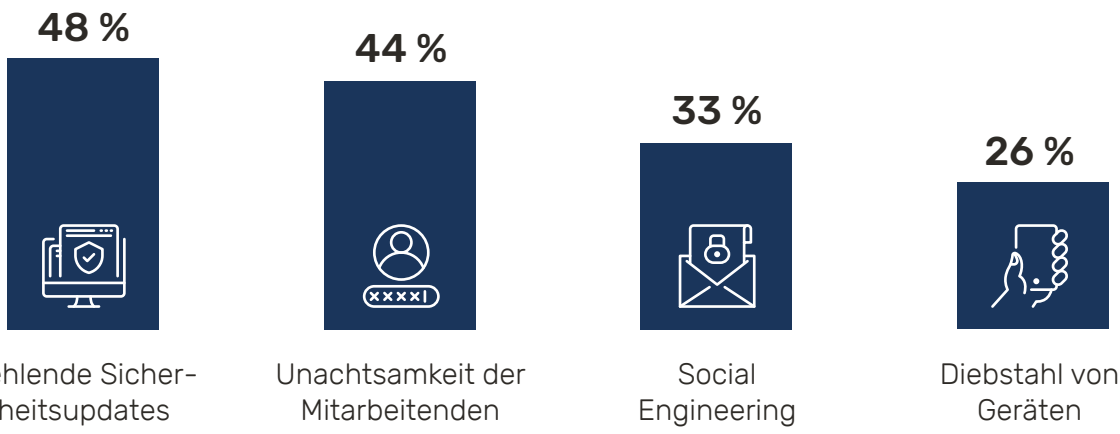
Menschliche Faktoren oft der Grund für Sicherheitsvorfälle

Doch wie konnten Cyberkriminelle trotz vorherrschender Sicherheitskonzepte die Systeme der Unternehmen infiltrieren? Zwei Ursachen haben sich als Hauptgründe für erfolgreiche Attacken durch Cyberkriminelle herauskristallisiert. Zum einen gaben 48 Prozent der befragten Unternehmen an, fehlende Sicherheitsupdates haben Cyberkriminelle geradezu eingeladen in ihre Netzwerke einzudringen. Vor vier Jahren jedoch, waren bei weniger als 30 Prozent der mittelständischen Unternehmen fehlende Sicherheitsupdates ein Grund für erfolgreiche Cyberangriffe. Eine mögliche Ursache könnte sein, dass IT-Abteilungen im Zuge der Pandemie und der schnellen Bereitstellung von Home-Office-Arbeitsplätzen stark belastet waren. So ist es durchaus vorstellbar, dass IT-Security und das manuelle Aufspielen von Updates im Meer von IT-Aufgaben untergingen bzw. dass mit der Bereitstellung von Home-Office-Arbeitsplätzen auch eine Vielzahl neuer Tools zum Einsatz kam

Zum anderen waren bei rund 44 Prozent der Unternehmen die eigenen Mitarbeitenden für Sicherheitsvorfälle verantwortlich, indem sie beispielsweise schwache Passwörter verwendeten, auf schadhafte E-Mail-Anhänge klickten oder auch ungesicherte öffentliche WLANs benutzten. Ein knappes Drittel der Unternehmen wurde Opfer gezielter Social-Engineering-Kampagnen wie etwa Phishing. Insbesondere die in den letzten Jahren stark wachsende Anzahl an Remote-Arbeitsplätzen stellt Unternehmen vor große Sicherheitsprobleme. Denn nicht selten fehlt es in den heimischen vier Wänden an den nötigen Sicherheitsstandards, vor allem wenn auf privaten Geräten gearbeitet wird. Das zeigt, dass selbst wenn die technische Infrastruktur vorhanden ist, diese nicht genügt, um ein hohes Security-Niveau zu garantieren. Im Vergleich zur Erhebung von 2019 haben sich diese Zahlen praktisch überhaupt nicht verändert. Damals waren in 47 Prozent der mittelständischen Unternehmen die eigenen Mitarbeitenden für Sicherheitsvorfälle verantwortlich und bei einem Drittel gezielte Social-Engineering-Kampagnen.

Hier ist es für Unternehmen essenziell, mitarbeiterzentrierte Maßnahmen durchzuführen, um die eigene Belegschaft für IT-Sicherheit zu sensibilisieren und beispielsweise aufzuzeigen, wie Phishing-Versuche erkannt werden können. Wichtig ist jedoch, dass es nicht bei einmaligen Maßnahmen bleibt, sondern die Sensibilisierungsmaßnahmen und Sicherheitstrainings kontinuierlich stattfinden. Auch anlassbezogene Maßnahmen können das Bewusstsein für IT-Sicherheit nachhaltig verbessern. So könnten beispielsweise sicherheitsrelevante Hinweise beim Anschließen von mobilen Datenträgern ausgespielt werden.

Ursachen von Sicherheitsvorfällen



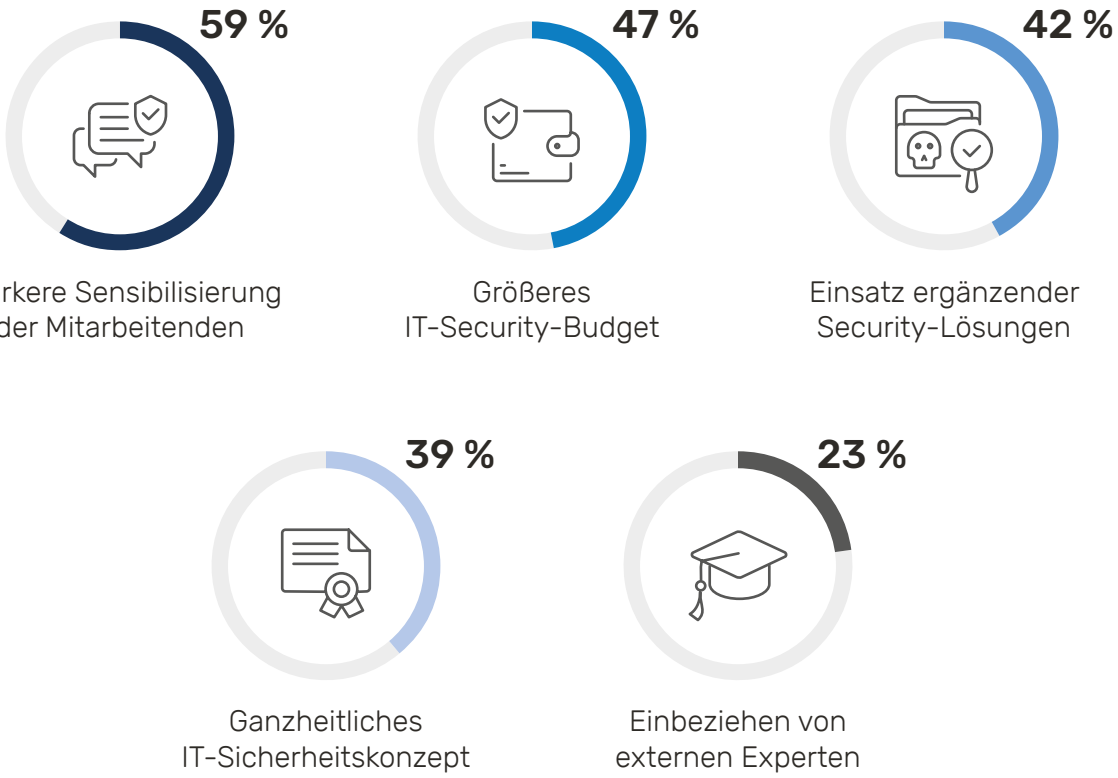
Basis: 123 Unternehmen | Mehrfachnennungen
Filter: Unternehmen, die bereits Sicherheitsvorfälle hatten

Sensibilisierung senkt das Sicherheitsrisiko

Fast 60 Prozent der befragten Unternehmen sind überzeugt, dass vor allem Sensibilisierungsmaßnahmen zur Reduzierung des Sicherheitsrisikos beitragen. Die Tatsache, dass ein großer Teil der erfolgreichen Sicherheitsvorfälle durch Unachtsamkeit der eigenen Mitarbeitenden stattfand, zeigt wie wichtig Sensibilisierungsmaßnahmen für mittelständische Unternehmen sind. Auch in Zukunft ist nicht damit zu rechnen, dass Phishing-Versuche weniger werden. Es ist eher damit zu rechnen, dass Unternehmen von Jahr zu Jahr stärker gefährdet sein werden.

Anschließend folgt der Wunsch nach einem größeren Budget für IT-Sicherheitsmaßnahmen. Dieser Wunsch ist nicht verwunderlich angesichts der Tatsache, dass Kosten als einer der wesentlichen Hinderungsgründe für mehr IT-Sicherheit genannt wurden. Interessant ist in diesem Zuge der Unterschied zwischen Unternehmen mit Security-Strategie und jenen ohne. So sagt beispielsweise knapp die Hälfte der Unternehmen mit Strategie, dass ganzheitliche Sicherheitskonzepte wie Zero-Trust ein wichtiges Werkzeug zur Verbesserung der IT-Sicherheit sind. Auf der anderen Seite sehen nur sechs Prozent der Unternehmen, die erst handeln, wenn etwas passiert, solche Sicherheitskonzepte als wichtig an.

Erforderliche Maßnahmen zur Optimierung der IT-Sicherheit



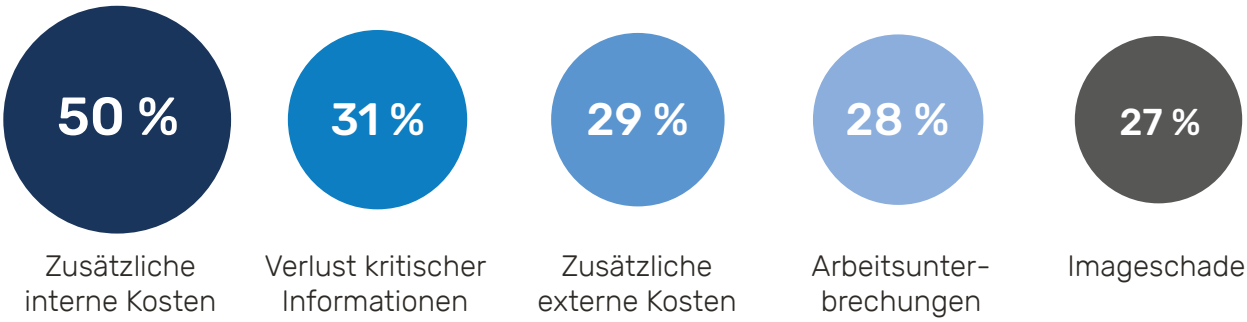
Basis: 201 Unternehmen | Mehrfachnennungen

Sicherheitsvorfälle sind teuer

Die Frage nach den entstandenen Schäden durch einen Sicherheitsvorfall macht vor allem eines deutlich: Während viele mittelständische Unternehmen die Investitionskosten als größten Verhinderer einer umfassenden IT-Sicherheit einschätzen, übersehen sie die massiven Schäden, die durch einen Angriff oder Sicherheitsvorfall entstehen. Wenn Cyberkriminelle mit ihren Versuchen in Unternehmensnetzwerke einzudringen erfolgreich sind, hat das für die betroffenen Unternehmen oft schwerwiegende Folgen.

In erster Linie sorgen erfolgreiche Cyberangriffe für erhöhte Kosten. Für knapp die Hälfte aller Unternehmen, die Opfer von Cyberkriminalität wurden, stiegen die internen Kosten zur Fehlerbehebung beispielsweise in Form von Überstunden. Besonders stark betroffen waren Unternehmen ohne IT-Security-Strategie und entsprechende Notfallpläne. So geben 61 Prozent der Unternehmen, die gelegentlich proaktiv ihre IT-Sicherheit verbessern und ganze 75 Prozent derer, die nur handeln, wenn ein Sicherheitsvorfall eintritt, an zusätzliche interne Kosten erlitten zu haben. In 29 Prozent der Unternehmen fielen darüber hinaus noch zusätzliche externe Kosten zur Fehlerbehebung an. Doch auch Schäden, die auf den ersten Blick nicht direkt monetär bewertet werden können, sind für Unternehmen ein großes Problem. So hatten 31 Prozent der Unternehmen, die Opfer von Cyberkriminalität wurden, den Verlust unternehmenskritischer Informationen erlitten. In diesem Kontext wurden Unternehmen häufig Opfer von Ransomware-Attacken. Bei dieser Art des Angriffs werden wichtige Daten verschlüsselt und eine Lösegeldforderung für diese hinterlegt. Haben Unternehmen keine entsprechende Recovery Strategie, können diese Daten ohne Zahlung eines hohen Lösegelds verloren gehen. Ebenfalls problematisch ist der Abfluss von Daten. Geraten beispielsweise sensible Daten in die Hände von Cyberkriminellen, so handelt es sich dabei um datenschutzrelevante Vorfälle, die mit Bußgeldern einhergehen können und darüber hinaus einen großen Vertrauensverlust bei Kunden nach sich ziehen. Es zeigt sich also, dass Sicherheitsvorfälle aufgrund mangelhafter IT-Security nicht nur hohe direkte Kosten verursachen, sondern auch zu indirekten Belastungen führen. Beispielsweise dann, wenn durch den Verlust von Daten, das Vertrauen der Kunden nachträglich beeinträchtigt wird. In IT-Sicherheit zu investieren, ist in jedem Fall die deutlich bessere Alternative.

Schäden durch Sicherheitsvorfälle
Top 5



Basis: 201 Unternehmen | Mehrfachnennungen

Sicherheitsvorfälle gefährden Unternehmen

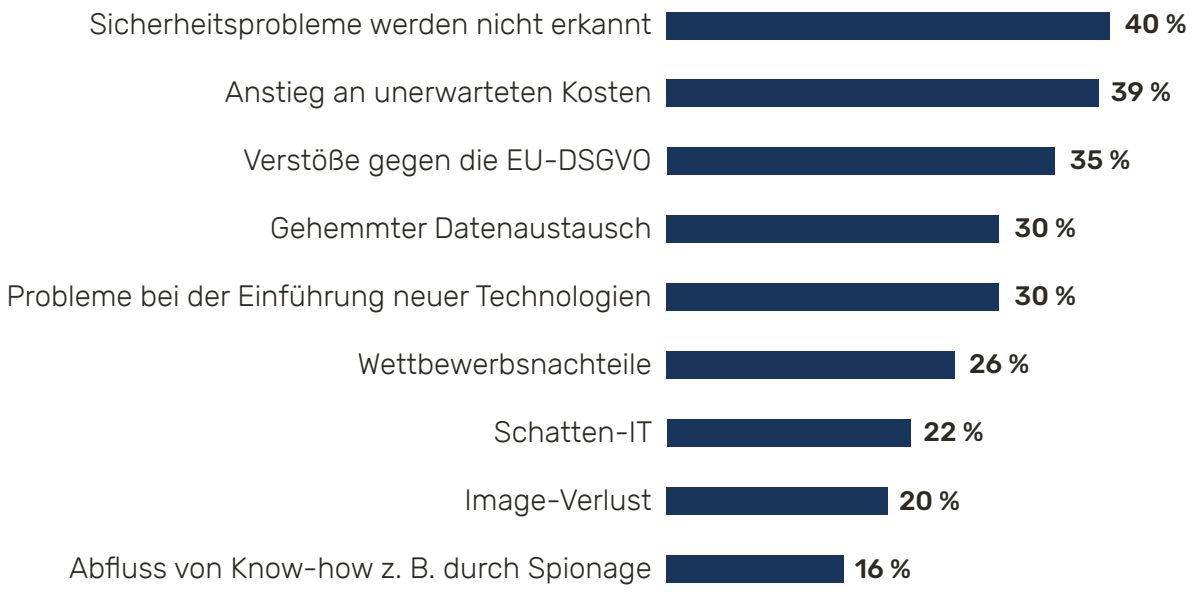
Auf die Frage welche Auswirkungen die Unternehmen durch mangelnde IT-Sicherheitsmaßnahmen spüren, antworteten rund 40 Prozent, wie schon in der letzten Erhebung, dass sie befürchten, Sicherheitsprobleme zu spät oder gar nicht zu erkennen. Das wäre ein äußerst fatales Szenario. Beispielsweise könnten Cyberkriminelle sich unbemerkt über einen langen Zeitraum im Unternehmensnetzwerk ausbreiten, sensible oder geheime Daten entwenden oder Maschinen, Systeme oder Prozesse manipulieren.

An zweiter Stelle folgt die Furcht vor dem Anstieg unerwarteter Kosten. Und diese Angst ist nicht unbegründet, waren doch die häufigsten tatsächlichen Folgen von Sicherheitsvorfällen gestiegene externe sowie interne Kosten. Auf dem dritten Rang folgt die Angst vor Verstößen gegen die DSGVO. Solche Verstöße können schnell zu einem finanziellen Risiko werden, denn der Bußgeldkatalog hält entsprechende Sanktionen bereit: Bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist, können im Maximalfall fällig werden.

Ein warnendes Beispiel für die Schäden, die ein Sicherheitsvorfall nach sich ziehen kann, lässt sich anhand des Vorfalls in Anhalt-Bitterfeld sehen. Am 09.07.2021 hat eine deutsche Kommune erstmals aufgrund eines Cyberangriffs den Katastrophenfall ausgerufen. Damals wurde die Kommune Opfer einer Ransomware-Attacke. Der Angriff jedoch begann bereits einen Monat vorher und blieb bis zum 09.07. unentdeckt. So konnten sich die Angreifer über längere Zeit im Netzwerk ausbreiten und eine massive Menge an Daten kompromittieren. Nachdem sich der Landkreis weigerte die Lösegeldforderung zu erfüllen, wurden die erbeuteten persönlichen Daten, wie etwa Handynummern, Anschriften oder auch Bankverbindungen ins Darknet gestellt. Insgesamt flossen ca. 63 GB an Daten in die Hände der Cyberkriminellen. Darüber hinaus wurde die Behörde komplett lahmgelegt und wichtige behördliche Dienstleistungen wie etwa die Auszahlung von Sozialleistungen konnten für mehrere Wochen nicht ausgeführt werden. Die Wiederherstellung der Daten dauerte mehr als ein Jahr, verschlang Millionen und einige Schäden konnten nicht beseitigt werden.

Dieser Vorfall zeigt eindrucksvoll, dass ein einziges unentdecktes Sicherheitsproblem gleich mehrere gravierende Folgen nach sich ziehen kann. Angefangen von Arbeitsausfall, über hohe Kosten, bis hin zu datenschutzrelevanten Datenverlusten und Image-Schäden.

Einschätzung von Problemen



Basis: 201 Unternehmen | Mehrfachnennungen

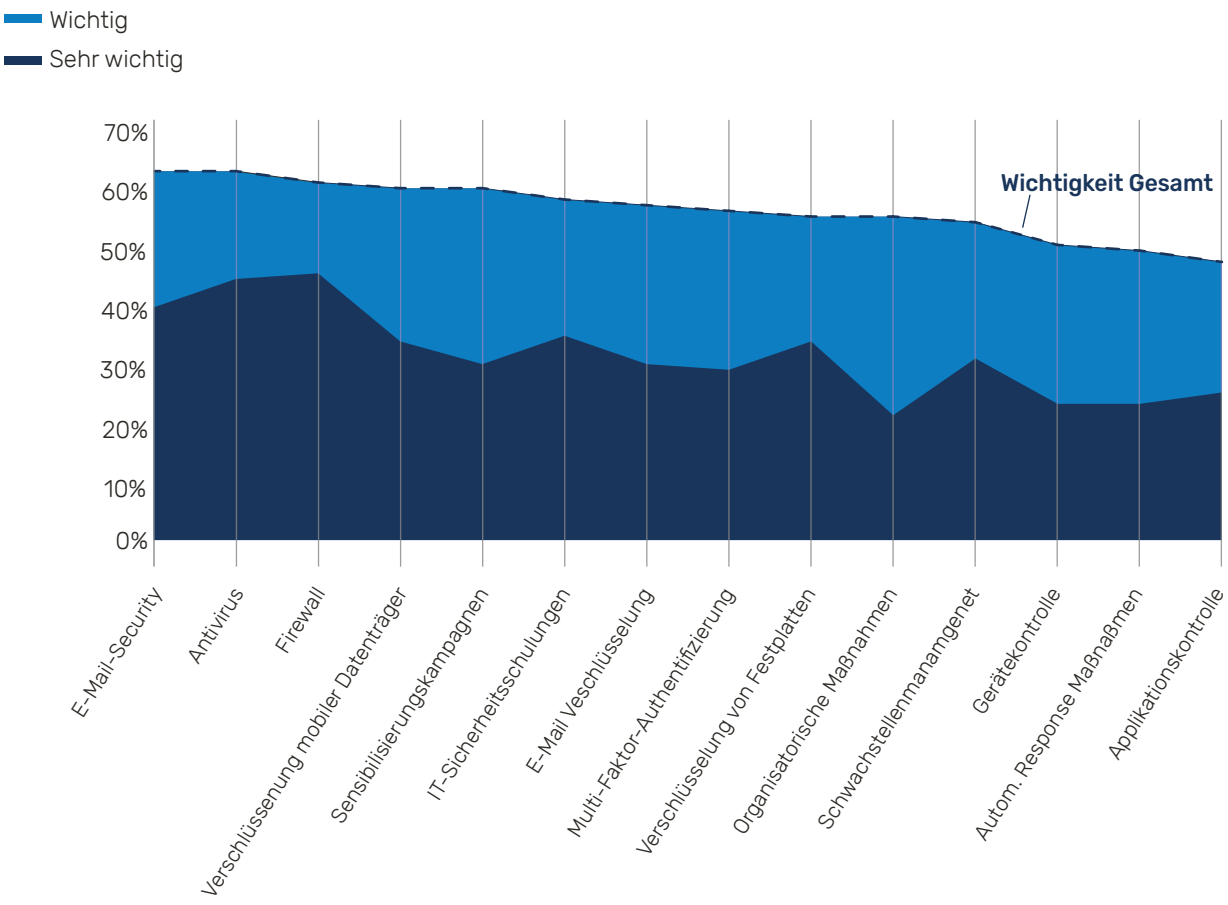
Der Mittelstand setzt noch immer nur auf Basisschutz

Fragt man nach der Relevanz bestimmter Sicherheitsmaßnahmen, stehen wie bereits 2019 auch heute noch die drei Cyber-Security-Klassiker E-Mail-Sicherheit, Antiviren-Software und die Firewall im Fokus der Unternehmen. Diese etablierten Schutzlösungen stellen den absoluten Basisschutz für die Mehrheit der Unternehmen dar. Nur knapp dahinter sind die Verschlüsselung mobiler Datenträger, sowie Sensibilisierungskampagnen angesiedelt.

Vor allem Unternehmen, die IT-Sicherheit als wichtigen Bestandteil ihrer Unternehmensstrategie verstehen, sehen weitergreifende, komplexere Sicherheitslösungen als deutlich wichtiger an, als dies bei jenen Unternehmen der Fall ist, die der IT-Sicherheit nicht die höchste Priorität zuweisen. Dieses Ergebnis ist nicht überraschend, setzen sich doch Unternehmen im Rahmen ihrer Security-Strategie mit einer Vielzahl von ergänzenden Sicherheitslösungen auseinander. Denn nur mit Basisschutz lässt sich heute keine robuste IT-Security-Infrastruktur mehr aufbauen. Dafür sind nicht nur die Angriffsmethoden der Cyberkriminellen zu komplex und ausgeklügelt, auch die Struktur von Unternehmen hat sich beispielsweise durch Cloud-Infrastrukturen oder auch Remote-Arbeit stark verändert. Und diese Veränderung muss sich auch im Einsatz von IT-Security-Maßnahmen widerspiegeln.

Relevanz von Security-Maßnahmen

Nennungen mit „Sehr wichtig“ und „Wichtig“



Basis: 201 Unternehmen
Mehrfachnennungen

Umsetzung mit Luft nach oben

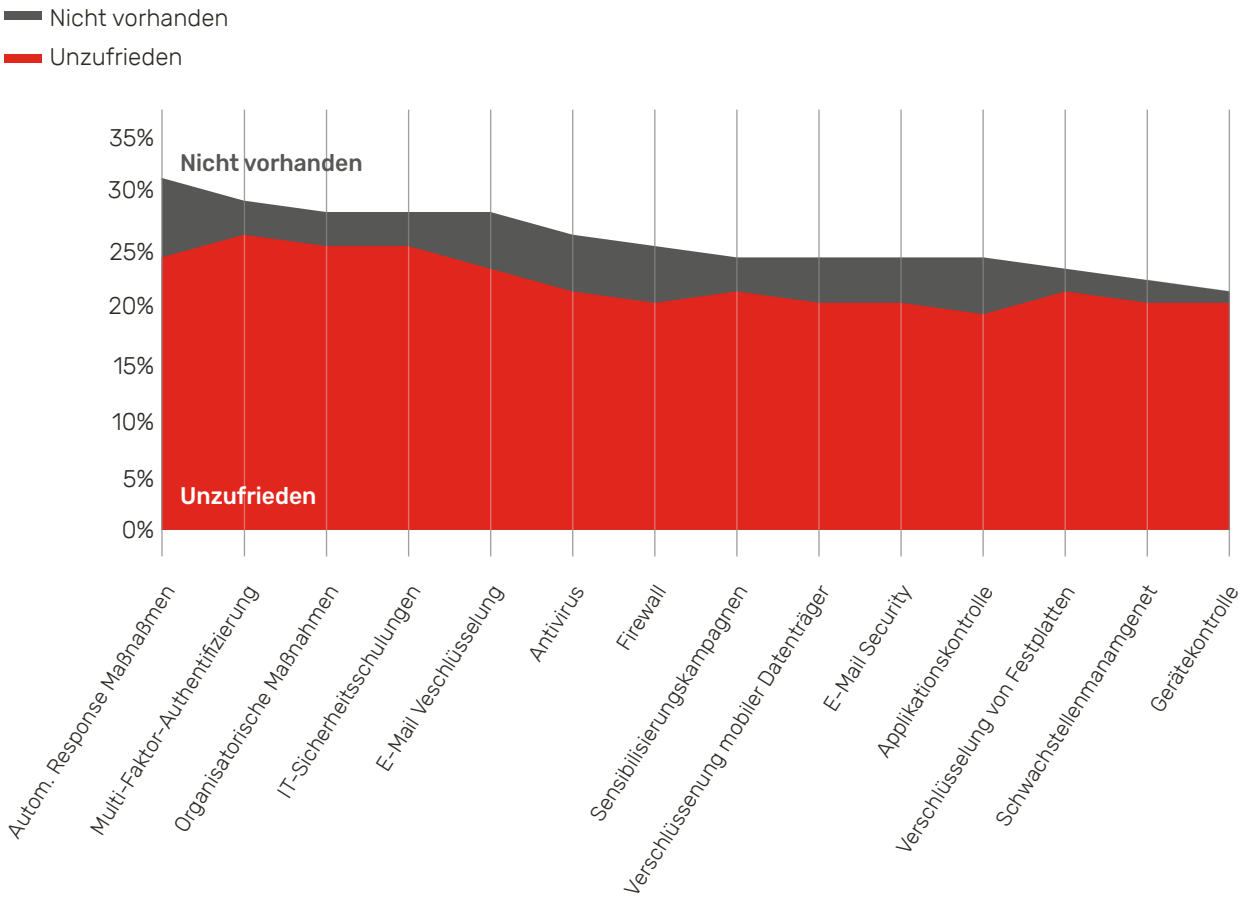
Betrachtet man dann die tatsächliche Umsetzung der einzelnen Security-Bereiche lässt sich an vielen Stellen eine Diskrepanz zwischen Anspruch und Wirklichkeit erkennen. Wie bereits vor vier Jahren sind rund 20 Prozent der Unternehmen mit der Aufstellung ihrer Basisschutzlösungen wie Antiviren-Schutz, E-Mail-Sicherheit oder Firewall nicht zufrieden. Das bedeutet, dass sie zwar Lösungen in diesem Bereich einsetzen, diese jedoch nicht in dem gewünschten Maß schützen und Malware oder ähnliches trotzdem in die Unternehmensnetzwerke gelangen kann. Das liegt oftmals auch an den eingesetzten Lösungen selbst. Antiviren-Lösungen schützen beispielsweise nur vor bekannter Malware und können bislang unbekannte Malware-Varianten nicht entdecken. Bei knapp 319.000 neuen Schadcode-Varianten täglich können diese Lösungen mit der Entwicklung nicht Schritt halten.

Eine Applikationskontrolle hingegen schützt auch vor unbekannter Schadsoftware und kann hier entsprechend umfassenden Schutz bieten. Interessanterweise beurteilten aber nur knapp 50 Prozent der Unternehmen diese Maßnahme als relevant. Im Einsatz zeigt sich die Lösung aber erfolgreich: Von allen hier genannten Maßnahmen hat sie den niedrigsten Unzufriedenheitswert.

Das ist wenig überraschend, da vor allem diejenigen Unternehmen ohne ganzheitliches Sicherheitskonzept vermehrt Schwierigkeiten mit der Umsetzung haben.

Umsetzung von Security-Maßnahmen im Vergleich zur Relevanz

Nennungen mit „Sehr schlecht", „Schlecht" und „Nicht vorhanden"



Basis: 201 Unternehmen
Mehrfachnennungen

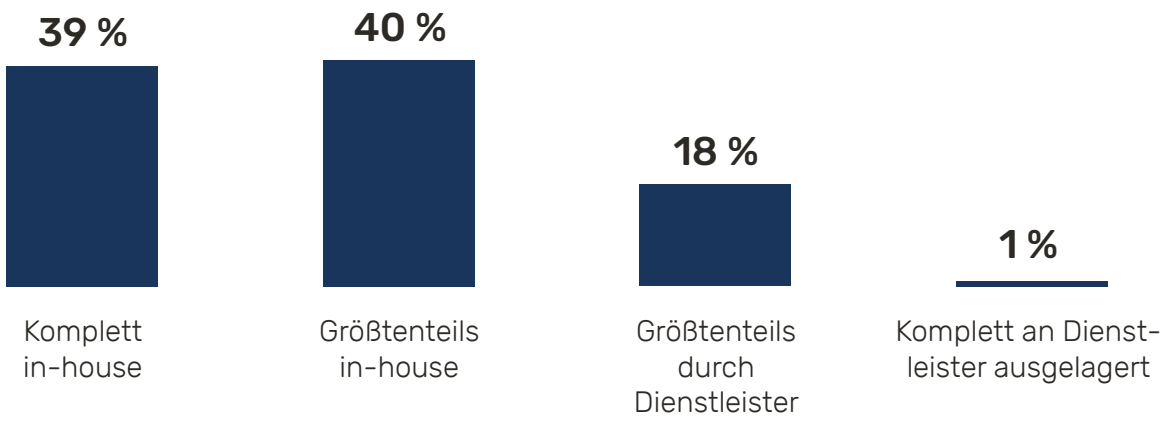
Der Mittelstand möchte die Kontrolle über IT-Sicherheit behalten

Wie viele andere Unternehmensfunktionen heutzutage, lässt sich auch die IT-Sicherheit auf verschiedene Art und Weise betreiben. Unternehmen können ihre IT-Sicherheit komplett im eigenen Rechenzentrum und mit den eigenen IT-Mitarbeitenden betreiben, einzelne Security-Bereiche an Experten auslagern oder auch den gesamten Betrieb in die Hände eines Dienstleisters geben. Vor allem für Unternehmen, die nicht über die personellen Kapazitäten und das Know-how verfügen, um die gesamte IT-Sicherheit im eigenen Haus zu betreiben, lohnt sich eine Teilauslagerung von Aufgaben bei denen Defizite vorliegen. Schwachstellen in der IT-Sicherheit werden von Cyberkriminellen gezielt ausgenutzt. Eine robuste IT-Security-Infrastruktur ist essenziell, um die Schäden aus Cyberangriffen zu minimieren.

Was überrascht: Trotz mangelnder zeitlicher Ressourcen wächst der Anteil an Unternehmen, die ihre IT-Sicherheit inhouse betreiben von 29 Prozent im Jahr 2019 auf nun 39 Prozent. Knapp 40 Prozent der mittelständischen Unternehmen setzen auf ein Modell, bei dem der größte Teil der IT-Sicherheit im eigenen Haus betrieben wird, einige Teile jedoch an Dienstleister ausgelagert werden. Bei der letzten Erhebung im Jahr 2019 waren es noch 47 Prozent.

Den Weg, bei dem die IT-Security in großen Teilen ausgelagert ist, einige kritische Funktionen jedoch im eigenen Haus betrieben werden, beschreiten nur rund 18 Prozent der Unternehmen. Ein vollständiges Outsourcing findet nur bei 2 Prozent der Unternehmen statt.

Betriebsmodelle IT-Sicherheit



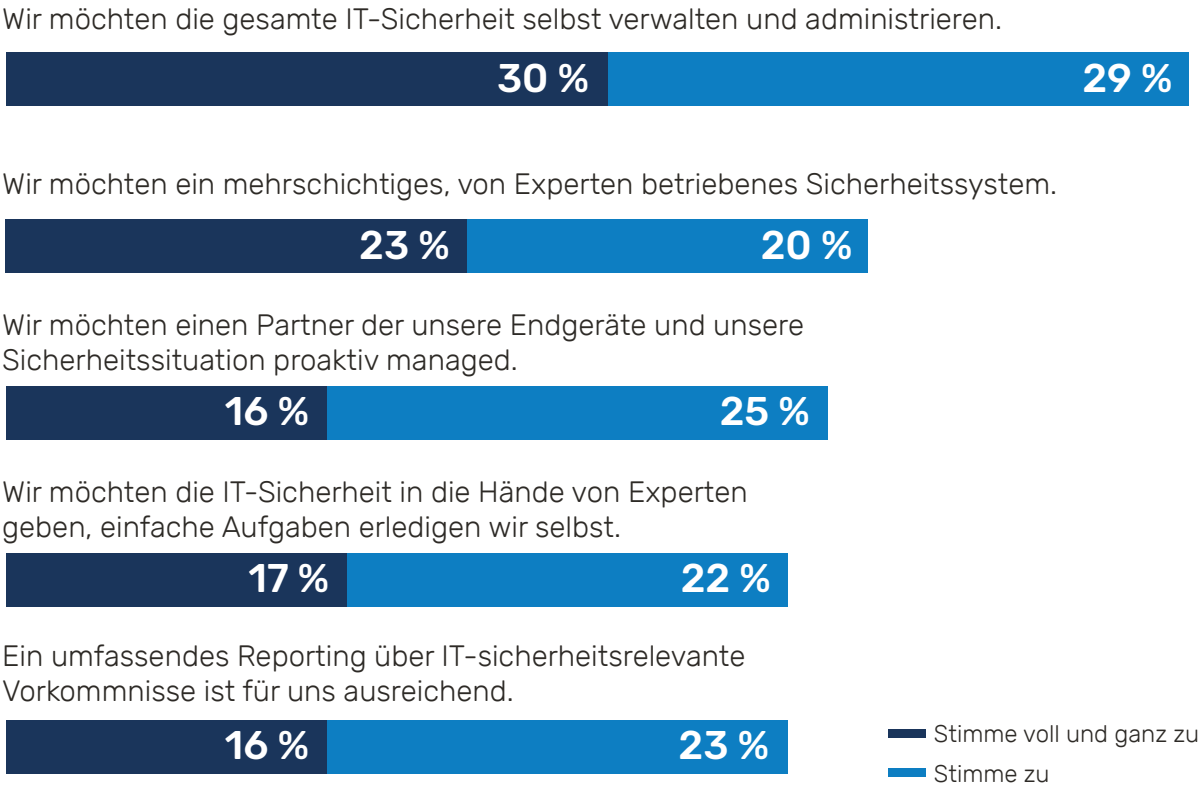
Basis: 201 Unternehmen

Dass Unternehmen auch weiterhin einen Teil ihrer IT-Sicherheit selbst betreiben möchten, zeigt ein weiteres Ergebnis dieser Erhebung. Knapp 60 Prozent stimmen der Aussage „Wir möchten die gesamte IT-Sicherheit selbst verwalten" zu – ein Anstieg von rund 12 Prozentpunkten im Vergleich zur letzten Befragung. Der Wunsch nach eigens betriebener IT-Sicherheit ist offenkundig da, jedoch fehlt es oftmals an der nötigen Expertise, um dies heute auch so umzusetzen.

43 Prozent der befragten Unternehmen wünschen sich ein mehrschichtiges von Experten betriebenes Sicherheitssystem. Auch hier ist ein klarer Anstieg erkennbar. 2019 hatten hieran nur 28 Prozent der mittelständischen Unternehmen Interesse. 41 Prozent möchten den größten Teil ihrer IT-Sicherheit in die Hände eines Dienstleisters geben, kleinere Aufgaben jedoch selbst übernehmen.

Die Ergebnisse zeigen, wie ausgeprägt der Wunsch im Mittelstand nach Selbstbestimmtheit in der IT-Sicherheit ist – trotz mangelnder Budgets und personeller Ressourcen.

Wunsch Betriebsmodelle



Basis: 201 Unternehmen

Fazit

Die Bedrohungslage durch Cyberkriminalität ist so hoch wie noch nie und die Lage wird sich auch in Zukunft nicht verbessern. Höchste Zeit also, sich auf diese Situation einzustellen und proaktiv das eigene Unternehmen vor den Gefahren zu schützen.

Das fängt damit an, dass man IT-Sicherheit ganz nach oben auf die Prioritätenliste setzt und diese auch in einer ganzheitlichen Unternehmensstrategie verankert. Nur so kann sichergestellt werden, dass IT-Security flächendeckend in allen Bereichen des Unternehmens inklusive Remote-Arbeitsplätzen zuverlässig umgesetzt wird.

Endgeräte-Sicherheit ist einer der wichtigsten Punkte, wenn es um den Schutz von Daten und Systemen geht. Dafür braucht es mehrschichtige Security-Lösungen, denn diese bilden wirksame Schutzwälle gegen Cyberkriminelle und weitere Sicherheitsrisiken.

Zuverlässige IT-Sicherheit muss nicht teuer und aufwändig sein. Stoßen Unternehmen beim Aufbau einer sicheren Infrastruktur beispielsweise durch mangelnde Expertise oder beschränkte Budgets an ihre Grenzen, sollten sich diese mit cloudbasierten Endpoint-Security-Lösungen beschäftigen. Die Vorteile liegen auf der Hand: Unternehmen heben ihre IT-Sicherheit schnell auf ein höheres Level ohne eigene Ressourcen für die Verwaltung, Infrastruktur oder Hard- und Software bereitstellen zu müssen.

Für den Mittelstand braucht es Lösungen, die vorkonfigurierte Best-Practice-Szenarien mit hochindividuellen Konfigurationsmöglichkeiten kombinieren. Die Best-Practice-Szenarien reduzieren personellen Aufwand; individuelle Konfigurationsmöglichkeiten gewährleisten die Kontrolle über die eigene IT-Sicherheit und die individuellen Unternehmensbedürfnisse.

Doch die bloße Einführung von neuer Security-Technologie genügt nicht. Denn der Mensch bleibt stets das schwächste Glied der IT-Security-Kette. Die Unwissenheit der Mitarbeitenden kann auch neueste Technologie aushebeln und Cyberkriminelle in die eigenen Netzwerke einladen. Gezielte Schulungsmaßnahmen und Sensibilisierungskampagnen sind ein gutes Mittel, um das Sicherheitsbewusstsein der eigenen Belegschaft zu verbessern und die Gefahren zu reduzieren.

Weitere Informationen

Kontakt für mehr Informationen

Raphael Napieralski
Analyst

E-Mail: raphael.napieralski@techconsult.de
Tel.: +49 561 8109181

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 Individualuntersuchungen 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.

Über Drivelock SE

Hypersecure IT aus Deutschland: DriveLock ist der führende Spezialist für innovative IT-Sicherheitslösungen aus Deutschland. Das Unternehmen bietet eine einzigartige Kombination aus präventiven und proaktiven Modulen für Endgerätesicherheit und erfüllt auf diese Weise selbst die anspruchsvollsten Sicherheitsanforderungen.

DriveLock Hypersecure IT Lösungen schützen digitale Arbeitsplätze konsequent und schaffen Synergien aus den folgenden Elementen:

- Data & Endpoint Protection
- Data Loss Prevention
- Data Encryption
- Security Awareness
- Risk & Vulnerability Management
- Security Configuration Management

Die digitalisierte Welt erfordert kompromisslose IT-Sicherheit, um Organisationen, Menschen und Dienste vor Cyberrisiken und Datenverlust zu schützen und digitales Arbeiten für alle sicher zu gestalten.

Hypersecure IT von DriveLock bietet mehrschichtige Sicherheit, ist Cloud-basiert, sofort verfügbar und wirtschaftlich effizient mit niedrigen Investitions- und Betriebskosten.

Die DriveLock-Lösungen Device Control und Application Control sind nach Common Criteria EAL3+ zertifiziert: Diese international anerkannte Zertifizierung attestiert die hohe Vertrauenswürdigkeit und den Sicherheitsstandard des DriveLock Agents.

DriveLocks wegweisende Tools und ein engagiertes Team sorgen dafür, dass Cyberattacken dort bleiben, wo sie hingehören: außen vor.

Auszeichnungen:

- Als Ergebnis der Marktuntersuchung „Cyber Security – Solutions & Services Germany 2023“ des Technologieberatungsunternehmens ISG wurde DriveLock erneut als ein Leader im Segment „Data Leakage/Loss Prevention“ ausgezeichnet.
- In der Anwenderbefragung „Professional User Rating Security Solutions 2022 (PUR-S)“ des Analystenhauses techconsult positionierten mehr als 2.000 Anwenderunternehmen DriveLock als Champion im Bereich Endpoint Protection unter 37 IT-Lösungsanbietern und deren Lösungen in Deutschland.

DriveLock Lösungen sind Made in Germany und ohne Backdoor.

- ✓ Schutz von mehreren Millionen verwalteter Endgeräte weltweit
- ✓ Kompromisslos abgesicherte Kundenumgebungen mit über 180.000 verwalteten Endgeräten
- ✓ Made in Germany: Entwicklung und technischer Support aus Deutschland