techconsult
TECHNOLOGY MARKET ANALYSTS
30 YEARS ANNIVERSARY

CYBER SECURITY NEU GEDACHT!

WIE ZERO TRUST ODER SASE BESTEHENDE SICHERHEITSKONZEPTE UMKREMPELN

In Zusammenarbeit mit

SEP Hybrid Backup

Informationen zur Studie

Diese Studie wurde erstellt durch

Kontakt

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

Erscheinungsdatum

04/2022

In Zusammenarbeit mit

SEP Hybrid Backup

Copyright

Diese Studie wurde von der techconsult GmbH verfasst und von den Unternehmen LANCOM Systems GmbH, macmon secure GmbH, McAfee Enterprise, NCP engineering GmbH, SEP AG und Sophos Technology GmbH unterstützt. Die darin enthaltenen Daten und Informationen wurden gewissenhaft und mit größtmöglicher Sorgfalt nach wissenschaftlichen Grundsätzen ermittelt. Für deren Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden. Alle Rechte am Inhalt dieser Studie liegen bei der techconsult GmbH. Vervielfältigungen, auch auszugsweise, sind nur mit schriftlicher Genehmigung der techconsult GmbH gestattet.

Disclaimer

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen etc. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. In dieser Studie gemachte Referenzen zu irgendeinem spezifischen kommerziellen Produkt, Prozess oder Service durch Markennamen, Handelsmarken, Herstellerbezeichnung etc. bedeuten in keiner Weise eine Bevorzugung durch die techconsult GmbH.

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.

Inhaltsverzeichnis

Einleitung 4
Cyberangriffe werden immer zahlreicher 5
Cyberangriffe führen zu erheblichen Schäden 7
Budgets für Cybersicherheit wachsen 8
Identitätsmanagement und Datenschutz Topthemen 9
Basisschutzlösungen weit verbreitet 10
Stellenwert der Cybersicherheit 11
Investitionen in moderne Sicherheitslösungen 12
Probleme bei der Netzwerkausrichtung 13
Mit SASE & Zero Trust gegen zukünftige Cybergefahren 14
Zero Trust - Gründe und Nutzen 15
Gründe für SASE 16
Vorteile von SASE 17
Was verhindert die Einführung von Zero Trust und SASE 18
Technische/organisatorische Maßnahmen im Zuge von Zero Trust und SASE 19
Security-Verantwortung bleibt In-House 21
Externe Unterstützung bei der Umsetzung 22
Fazit 23
Stichprobe 24
Weitere Informationen 25

Einleitung

Cyberattacken sind allgegenwärtig und eine enorme Bedrohung für die gesamte Wirtschaft, ganz unabhängig von Größe und Branche. Der rasante Anstieg von mobiler Arbeit und Cloud-Diensten trägt sein Übriges dazu bei, um Unternehmen noch anfälliger für Cyberangriffe zu machen. Wo auf der einen Seite eine Erhöhung der Flexibilität durch Remote-Arbeit und Cloud-Dienste erreicht wird, schaffen die neuen Strukturen gleichzeitig neue Angriffsvektoren für Cyberkriminelle, die bei IT-Sicherheitsexperten die Alarmglocken schrillen lassen müssen. Aber auch die Verbreitung von Schatten-IT oder die Anbindung neuer Standorte erhöhen die Risiken zunehmend.

Dass Cyberangriffe in nie da gewesener Härte kommen, zeigen auch prominente Beispiele aus dem Jahr 2021. So wurden die Handelsriesen Media Markt und Saturn zum Jahresende Opfer einer großen Ransomware-Attacke – mit immensen Folgen. Kassen- und Warenwirtschaftssysteme waren durch die Ransomware verschlüsselt worden, die Betriebsabläufe massiv gestört und die Cyberkriminellen forderten insgesamt 50 Millionen Dollar Lösegeld. Das ist nur eines von zahlreichen Beispielen, bei denen Cyberkriminelle die Schutzmechanismen aushebeln konnten, um Schaden anzurichten. Darüber hinaus wird die Zahl der Cyberangriffe auch zukünftig weiter exorbitant ansteigen. Laut des „Check Point Software's 2022 Security Report" sind in Deutschland die Zahl von Angriffen auf Unternehmensnetzwerke in 2021 in Deutschland gegenüber dem Vorjahr um 62 Prozent, in Österreich um 117 und in der Schweiz um 65 Prozent gestiegen.

Gleichzeitig werden Cyberkriminelle immer raffinierter und es gelingt ihnen zunehmend traditionelle IT-Sicherheitsinfrastrukturen zu umgehen. Denn diese alten, statischen Strukturen sind im Zeitalter der Digitalisierung mit einem riesigen Zuwachs des Datenverkehrs durch immer mehr Geräte und Teilnehmer nicht mehr zeitgemäß. Unternehmen müssen umdenken und sich neuer Sicherheitskonzepte bedienen, die auch außerhalb des eigenen Unternehmensnetzwerks greifen und dafür sorgen tragen, dass die IT-Sicherheit gewährleistet bleibt.

Zwei dieser Schlüsselkonzepte stellen dabei der Zero-Trust-Ansatz sowie Secure Access Service Edge (SASE) dar. Zero Trust ist ein Sicherheitskonzept, bei dem prinzipiell jedes Gerät, Nutzer oder Dienst von vornherein misstraut wird, ohne dabei einen Unterschied zu machen, ob der Dienst, das Gerät oder der Nutzer sich innerhalb oder außerhalb des eignen Netzwerks befindet. In traditionellen Sicherheitskonzepten wird alles, was sich innerhalb befindet, als vertrauenswürdig eingestuft. SASE versteht sich als Cloud-Architekturmodell, das Netzwerk und Security-as-a-Service-Funktionen in einen gemeinsamen Cloud-Service bündelt. Dazu zählen Firewalls, Secure Web Gateways und auch der Netzwerkzugang nach dem Zero-Trust-Prinzip.

Die Ergebnisse dieser Studie zeigen, wie weit deutsche Unternehmen auf Cloud-Dienste setzen und welche Maßnahmen sie ergreifen, um den sicheren Zugriff privater Endgeräte auf Cloud-Dienste zu gewährleisten. Darüber hinaus gaben die befragten Unternehmen Auskunft darüber, wie oft sie von Cyberangriffen betroffen waren, welche Konsequenzen das für sie hatte, welche Mittel sie zur Bekämpfung von Cyberattacken verwenden und wie der Reifegrad ihrer Umsetzung von Zero Trust und SASE-Konzepten ist.

Quelle:
https://www.ict-channel.com/security/letztes-jahr-62-prozent-mehr-cyberangriffe.126621.html

Cyberangriffe werden immer zahlreicher

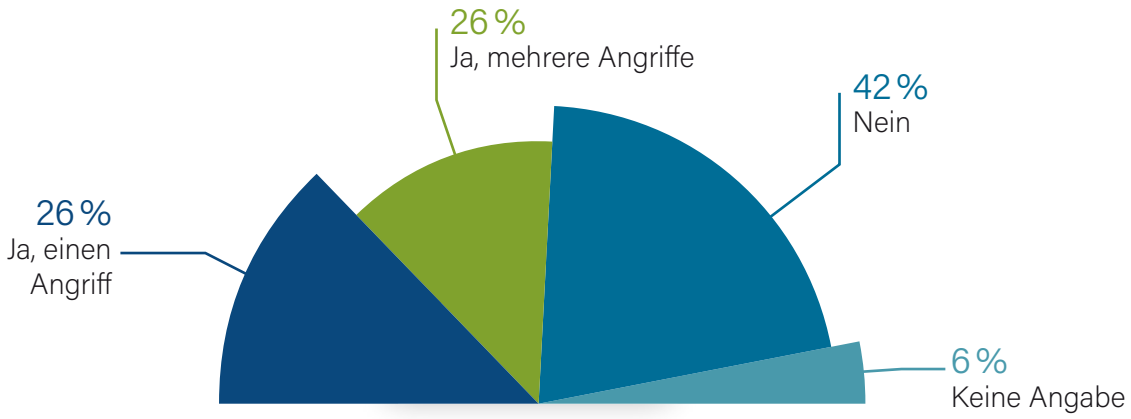
Weltweit sind Unternehmen mit einer sich schnell entwickelnden Bedrohungslandschaft konfrontiert. Die Qualität und die Häufigkeit der Cyberangriffe haben in den letzten Jahren ständig zugenommen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ermittelte, dass allein zwischen Juni 2020 und Mai 2021 144 Millionen neue Varianten gängiger Schadprogramme im Umlauf waren - täglich also 394.000 neue Schadprogrammvarianten. Auch bedingt durch die größere Verbreitung von Homeoffice und Cloud-Diensten sind weitere Angriffsvektoren entstanden, die Cyberkriminelle mit immer neuen Methoden aktive auszunutzen versuchen.

In den letzten 12 Monaten waren beispielsweise mehr als die Hälfte der Unternehmen von Cyberangriffen betroffen. Knapp ein Viertel sogar mehr als ein einziges Mal. Besonders im Fokus der Cyberkriminellen waren dabei Energie- und Wasserversorger (80 Prozent mindestens einmal angegriffen worden) sowie Finanz- und Versicherungsdienstleister (55 Prozent).

Zwar gaben 42 Prozent der Unternehmen an, überhaupt keinen Cyberangriff erlitten zu haben. Diese Zahl ist jedoch mit Vorsicht zu genießen. Möglicherweise blieben die Cyberangriffe unentdeckt. Man sollte von einer gewissen Dunkelziffer ausgehen.

Cyberattacken auf Unternehmen in den letzten 12 Monaten

Basis: 204 Unternehmen



Phishing häufigste Angriffsart

Cyberkriminelle nutzen dabei besonders gerne das schwächste Glied der Sicherheitskette, um in Unternehmensnetzwerke einzudringen: den Menschen. Dabei bildet Phishing die Hauptangriffsform für Cyberkriminelle. Hier werden Mitarbeiter beispielsweise durch täuschend echt wirkende E-Mails oder Webseiten so getäuscht, dass Cyberkriminelle Zugriff auf sensible Unternehmensdaten erlangen. 42 Prozent aller erfolgreichen Angriffe sind auf Phishing zurückzuführen. Hier waren vor allem die größten Unternehmen Opfer erfolgreicher Angriffsversuche.

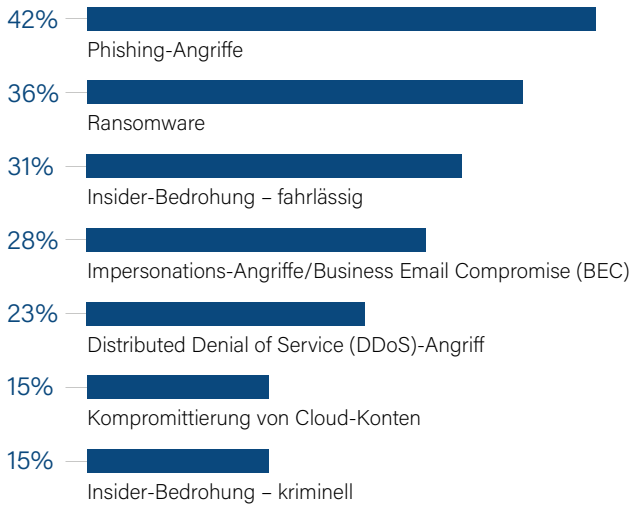
Fast 60 Prozent der Unternehmen mit mehr als 5000 Mitarbeitern gaben an, von Phishing-Versuchen betroffen gewesen zu sein. Das verwundert nur wenig, denn mehr Mitarbeiter und mehr mit dem Netzwerk verbundene Endgeräte bedeuten auch mehr Angriffsfläche.

Die zweithäufigste Methode bilden Cyberangriffe mittels Ransomware (36 Prozent). Solche Angriffe haben das Ziel, Unternehmensnetzwerke zu befallen und Unternehmensdaten zu verschlüsseln.

Erst gegen Zahlung eines „Lösegelds" geben die Cyberkriminellen die verschlüsselten Daten wieder frei. Diese Angriffsmethode steht auch stark in Verbindung mit Phishing. Denn oftmals verwenden Angreifer hier einen dreistufigen Angriff. Zuerst wird per Trojaner der E-Mail-Verkehr des Opfers analysiert, um eine täuschend echte Phishingmail zu generieren, die den Zweck hat, Schadsoftware in das System zu spielen. Anschließend spioniert die Schadsoftware die Systeme nach lohnenswerten Opfern aus und im letzten Schritt wird die Ransomware aufgespielt und Lösegeld gefordert. Besonders Unternehmen, bei denen ein möglichst hohes Lösegeld gefordert werden kann, stehen im Fokus der Angreifer. So wundert es nicht, dass fast die Hälfte der Unternehmen ab 5.000 Mitarbeitern Opfer eines Ransomwareangriffs geworden ist.

Arten von Cyberattacken auf Unternehmen in den letzten 12 Monaten

Basis: 107 Unternehmen | Filter: Unternehmen mit Angriffen | Mehrfachnennungen



Phishing auch in Zukunft besorgniserregend

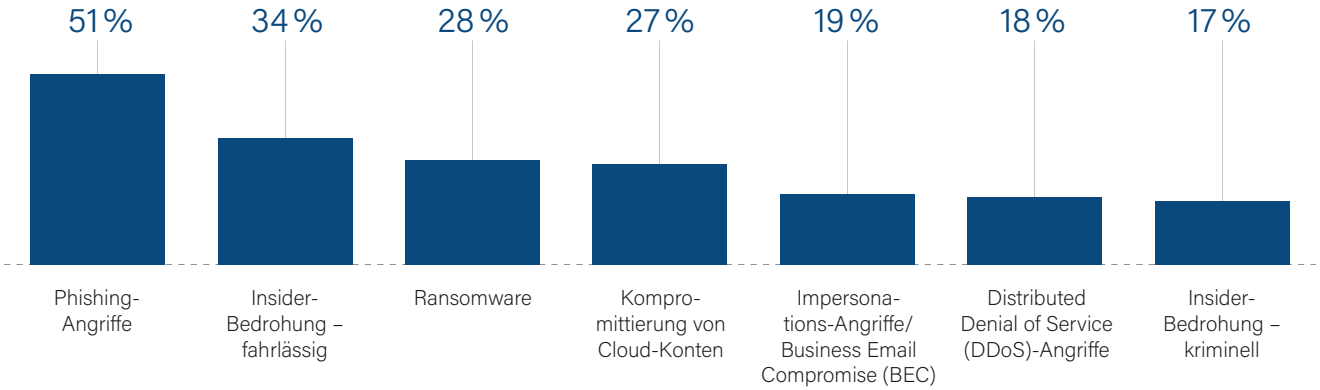
Der Ausblick der Unternehmen auf die Gefahren in den nächsten drei Jahren bestätigt die akute Bedrohung durch Phishing-Angriffe. Knapp die Hälfte der Unternehmen geht davon aus, dass Phishing-Angriffe die größte Cyberbedrohung der nächsten drei Jahre sein werden. Insbesondere Finanzdienstleister sehen hier erhebliches Gefahrenpotenzial, denn zwei Drittel der befragten Unternehmen aus dem Finanzsektor sieht Phishing als die Bedrohung der Zukunft an – mehr als jede andere Branche.

Dahinter folgt für ein Drittel der Unternehmen die Bedrohung durch Fahrlässigkeit beziehungsweise mangelndem Wissen der eigenen Mitarbeiter, externen Dienstleistern, Partnerunternehmen oder ehemaligen Mitarbeitern.

Im Gegenzug sehen sich Unternehmen in Sachen Ransomware für die Zukunft besser aufgestellt. Das kann mit möglichen Neuanschaffungen von Sicherheitstechnologie zusammenhängen, die Ransomware-Angriffe effizient abwehren kann.

Zukünftiges Bedrohungspotenzial durch Cyberangriffe

Basis: 204 Unternehmen | Mehrfachnennungen



Cyberangriffe führen zu erheblichen Schäden

Kommt es zu einem Sicherheitsvorfall, hat das für Unternehmen teils schwerwiegende Konsequenzen. Diese reichen von betrieblichen Störungen, entgangenen Einnahmen, Datenverlusten bis zu Reputationsschäden. Im allerschlimmsten Fall können Cyberangriffe sogar so schwerwiegende Folgen haben, dass das gesamte Unternehmen um seine Existenz fürchten muss.

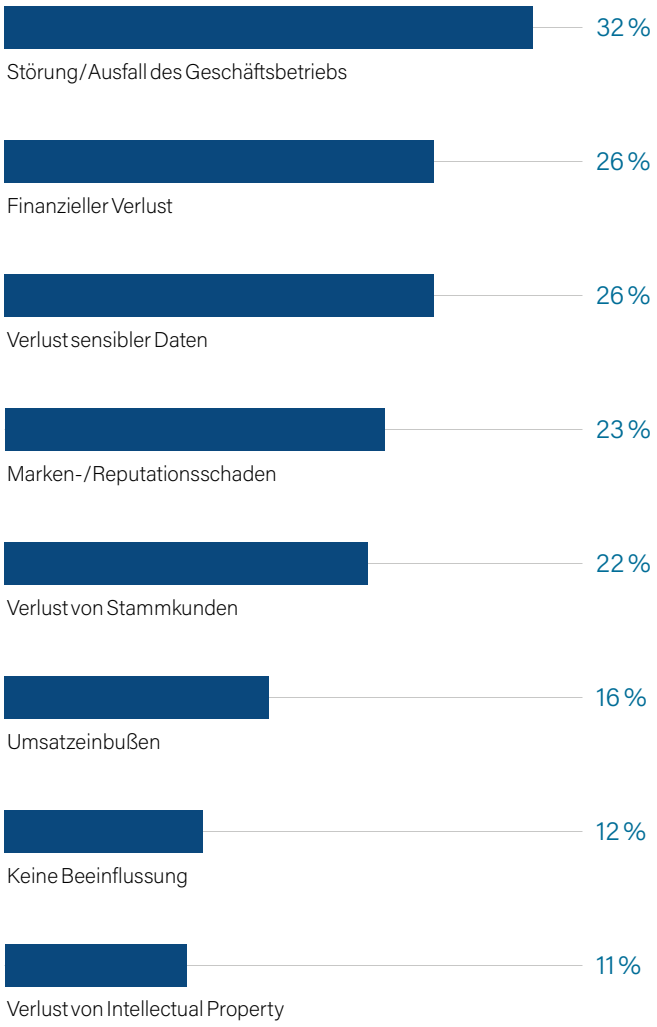
Die Art des Schadens aus den Sicherheitsvorfällen hängt dabei mit der Größe der betroffenen Unternehmen zusammen. Die Störung des Geschäftsbetriebs ist beispielsweise in 20 Prozent der Unternehmen mit bis zu 499 Mitarbeitern vorrangig gewesen. Bei Unternehmen mit mehr als 5000 Mitarbeitern wurde der Betriebsablauf in mehr als 47 Prozent der Unternehmen massiv gestört. Eine Störung des Geschäftsbetriebs und damit verbundener Produktionsausfall sorgt für verheerende finanzielle Folgen. Und nicht nur die Unternehmen selbst sind betroffen, auch die Lieferketten stehen immer mehr im Fokus der Cyberkriminellen. So gelang es einer Hackergruppe, einen Softwarehersteller erfolgreich zu infizieren und die Schadsoftware in ersten Schritt an IT-Dienstleister zu verteilen und schließlich auch deren Kunden. Mehr als 1.500 Unternehmen waren betroffen und die Betriebe standen mehrere Tage still.

Ähnliches ist beim direkten und indirekten finanziellen Verlust zu beobachten. Diese können Lösegelder für verschlüsselte Daten sein oder auch Aufwände zur Beseitigung der Schäden. Mit steigender Unternehmensgröße sind auch die finanziellen Verluste häufiger. Ein Fünftel der kleinen Unternehmen beklagt monetäre Einbußen, während es bei den größten Unternehmen knapp ein Drittel ist.

Das umgekehrte Bild ist beim Verlust von sensiblen Daten zu erkennen. Rund 21 Prozent der Unternehmen ab 5000 Mitarbeitern hatten einen Datenverlust zu vermelden. Bei Unternehmen mit weniger als 500 Mitarbeitern betraf dies ein Drittel.

Auswirkungen von Cyberattacken in den letzten 12 Monaten

Basis: 107 Unternehmen | Filter: Unternehmen mit Angriffen | Mehrfachnennungen



Budgets für Cybersicherheit wachsen

Um der Bedrohungslage Herr zu werden, müssen Unternehmen auch über die nötigen Security-Budgets verfügen, um beispielsweise neue Technologien zu erwerben oder die eigenen Mitarbeiter zu schulen. Und die überwiegende Mehrheit der Unternehmen stellt genügend Budget für die IT-Sicherheit zur Verfügung.

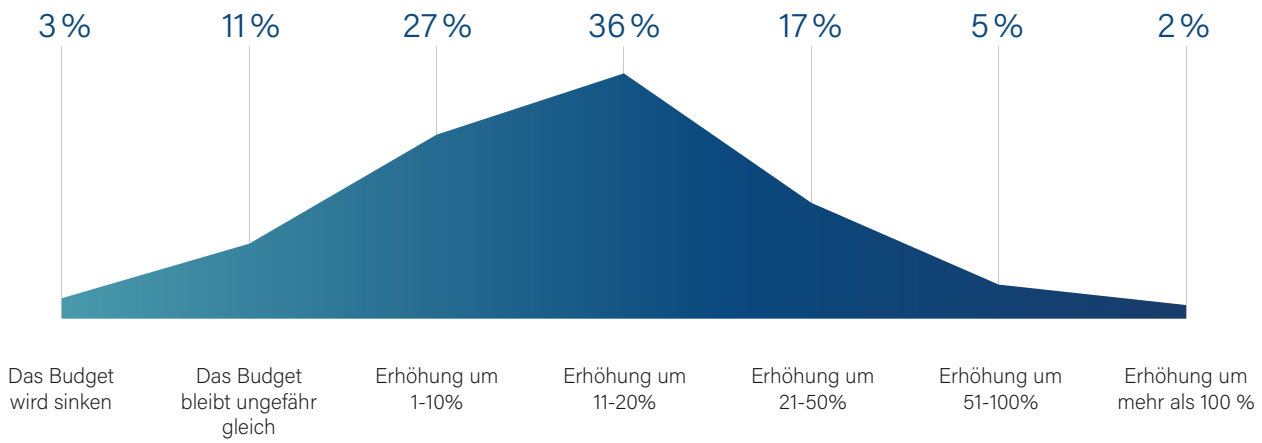
Dabei erwartet das Gros der Unternehmen (86 Prozent) in den kommenden zwei Jahren eine Erhöhung der Budgets für Cybersicherheit. Das zeigt, dass die Unternehmen sich der Gefahren durch Cyberkriminalität bewusst sind und diese in Zukunft verstärkt bekämpfen möchten.

Größere Unternehmen wollen dabei auch größere Sprünge in Sachen Budgets durchführen. 40 Prozent der Unternehmen ab 5000 Mitarbeitern wollen ihre Budgets um mehr als 20 Prozent erhöhen. Bei den kleinen und mittelgroßen Unternehmen beträgt dieser Anteil knapp 20 Prozent.

Die kleinen Unternehmen zwischen 50 und 249 Mitarbeitern sind bei ihren Budgets etwas verhaltener. 15 Prozent erwarten eine Stagnation des Budgets für IT-Sicherheit und knapp ein Drittel erwartet nur sehr leichte Steigerungen. Darüber hinaus gehen fast fünf Prozent der kleinen Unternehmen davon aus, dass ihre Budgets sogar noch sinken werden.

Entwicklung des Budgets für Cybersicherheit in den nächsten 2 Jahren

Basis: 196 Unternehmen



Identitätsmanagement und Datenschutz Topthemen

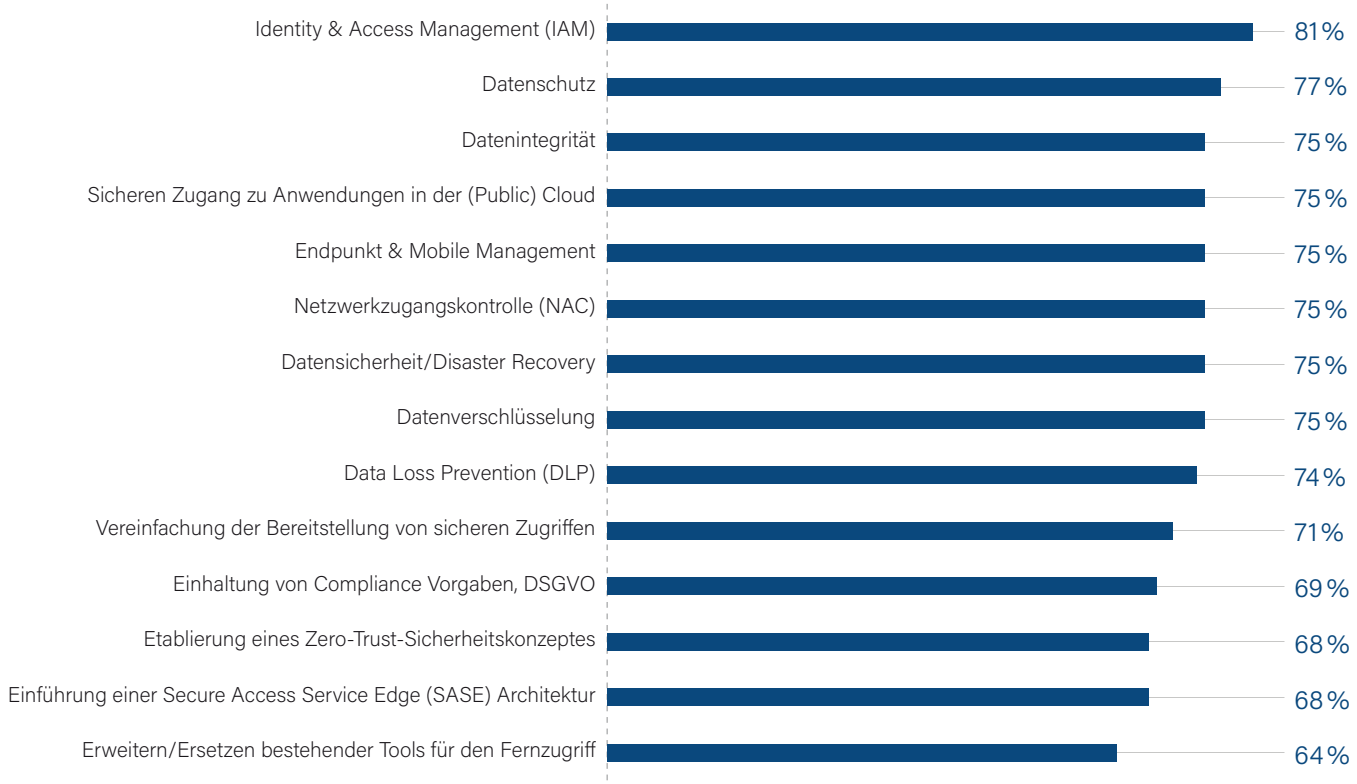
Unternehmen stehen etliche Mittel zur Stärkung der eigenen IT-Sicherheit zur Verfügung. Vor allem im Hinblick auf die Zukunft müssen einige Ansätze überdacht werden. Beispielsweise erfordert die steigende Tendenz von mobilen Arbeitsplätzen und dem Einsatz von Cloud-Diensten auch die Absicherung außerhalb der Unternehmensgrenzen. Was die Unternehmen genau planen, wurde im Rahmen dieser Studie erhoben.

Auf die Frage, welche Themen innerhalb der IT-Security-Strategie in Zukunft besonders wichtig sind, gaben 81 Prozent der Unternehmen an, dass Identity und Access Management von höchster Relevanz ist. Mit einer solchen Lösung können Unternehmen sicherstellen, dass nur autorisierte Geräte und Nutzer auf das Firmennetzwerk und auf sensible Firmendaten zugreifen können.

Weiterhin von höchster Bedeutung ist für 77 Prozent der Unternehmen der Datenschutz im Rahmen der DSGVO. Hier haben immer noch viele Unternehmen deutlichen Nachholbedarf. Oftmals glauben vor allem kleinere Unternehmen, dass sie unter dem Radar der Aufsichtsbehörden fliegen und nur die Großen sanktioniert werden. Vor allem durch den Ausbau des Homeoffice oder auch spezielle Verordnungen im Rahmen von Corona-Maßnahmen können Datenschutzverletzungen schnell entstehen. Ein Beispiel dafür könnten unberechtigte Zugriffe auf Daten zur Kontaktnachverfolgung sein. Ein typisches Szenario wäre das unerlaubte Nutzen der Listen für Marketing-Zwecke.

Themen/Aufgaben innerhalb zukünftiger IT-Security-Strategien

Basis: 204 Unternehmen | Nennungen mit "Sehr wichtig" und "Wichtig"



Basisschutzlösungen weit verbreitet

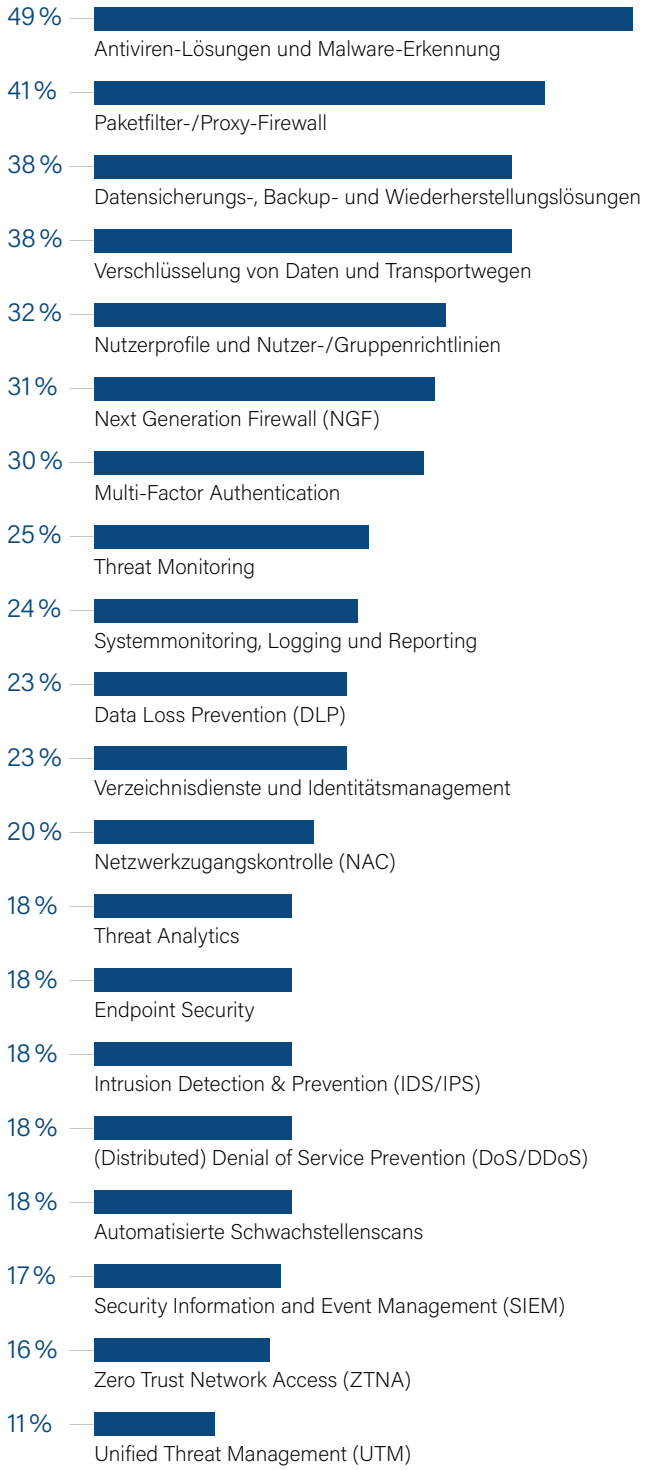
Um die Cyberbedrohungen abzuwehren, stehen Unternehmen eine Vielzahl unterschiedlicher Lösungen und Maßnahmen zur Verfügung. Diese reichen von Basisschutzmaßnahmen rund um Firewall und Antivirus bis zu komplexeren Themen wie automatisierten Schwachstellenscans.

Am häufigsten werden dabei Lösungen zur Abwehr von Malware eingesetzt. Diese setzen sich aus klassischen Client-Security-Lösungen wie Antiviren-Programmen (49 Prozent), aber auch ganzheitlichen Lösungen zur Endpunktsicherheit (19 Prozent), sowie diverser Firewall-Lösungen zusammen. Insgesamt lässt sich feststellen, dass der überwiegende Teil der Unternehmen Basisschutzlösungen zur Sicherheit der Netzwerke einsetzt.

Neuere Konzepte hingegen sind nur sporadisch im Einsatz. Beispielsweise nutzen nur 16 Prozent der Unternehmen einen Zero-Trust-Netzwerkzugang und 18 Prozent der Unternehmen verwenden Lösungen aus dem Bereich Advanced Cyber Defense, wie beispielsweise SIEM-Lösungen. Hier sind teilweise deutliche Unterschiede im Größenklassenvergleich zu erkennen. Je größer das Unternehmen, umso größer auch der Einsatzgrad von neuen und komplexen Sicherheitslösungen. Während in 11 Prozent der Unternehmen mit weniger als 500 Mitarbeitern Zero Trust eingesetzt wird, sind es bei den größten Unternehmen doppelt so viele (22 Prozent). Ähnliches lässt sich auch bei SIEM-Lösungen erkennen. Nur sechs Prozent der kleinen Unternehmen setzen eine solche Lösung ein. Bei den größten Unternehmen sind es knapp 30 Prozent.

Technischen Maßnahmen/Lösungen für die Sicherstellung der Cyber Security

Basis: 204 Unternehmen



Stellenwert der Cybersicherheit

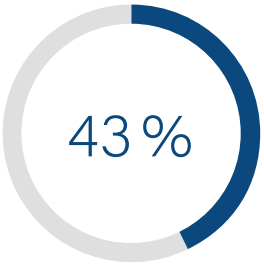
Im Rahmen der Studie wurden den Teilnehmern verschiedene Aussagen rund um ihre eigene Einschätzung zur IT-Security im eigenen Unternehmen präsentiert. Dabei gaben nur knapp 40 Prozent der Unternehmen an, dass sie sich auf einen Cyberangriff vorbereitet fühlen. Das bedeutet im Umkehrschluss, dass sechs von zehn Unternehmen sehr leicht Opfer von erfolgreichen Cyberangriffen werden können. Ein erschreckendes Ergebnis angesichts der starken Bedrohungslage für die Unternehmen.

Passend dazu gaben auch 37 Prozent der befragten Unternehmen an, dass ihre derzeitige Security-Infrastruktur nicht für zukünftige Bedrohungsszenarien ausreicht. Stand jetzt mögen die Unternehmen zwar noch auf Bedrohungen reagieren können, doch zukünftige Gefahren könnten unter Umständen nicht mehr geblockt werden. Hier zeigt sich, dass die alten IT-Infrastrukturen ihre beste Zeit hinter sich haben und neue, moderne Ansätze für eine sichere Zukunft von Nöten sind.

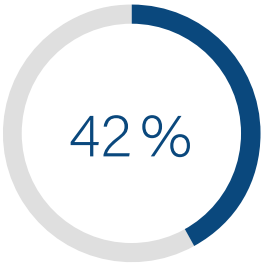
Dabei reicht es nicht nur einzelne Lösungen einzuführen. Um sich auf die wachsende Bedrohung durch Cyberkriminelle einzustellen, muss vor allem auch strategisch von ganz oben vorgegangen werden. Doch nur 43 Prozent der Unternehmen gaben an, dass Cybersicherheit in den nächsten 12 Monaten ein Thema auf Vorstandsebene wird.

Stellenwert von Cybersicherheit

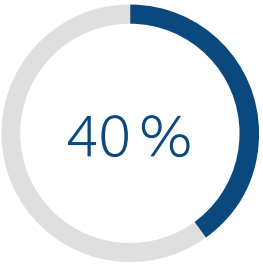
Basis: 204 Unternehmen | Nennungen mit „Stimme zu“ und „Stimme voll zu“



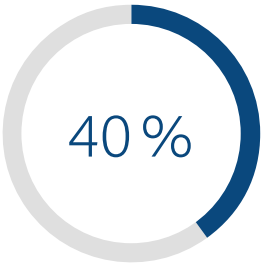
Cybersicherheit ist für unser Unternehmen in den nächsten 12 Monaten ein Thema auf Vorstandsebene



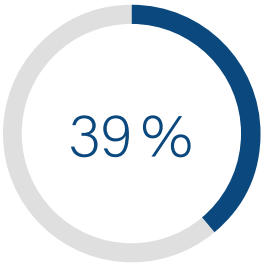
Wir haben eine abgestimmte Sicherheits- und Netzwerkstrategie



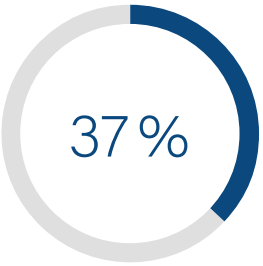
Unser Unternehmen ist auf einen Cyberangriff vorbereitet



Menschliches Versagen/mangelndes Sicherheitsbewusstsein ist das größte Risiko für unser Unternehmen



Wir sind gut gerüstet, der neuen „New Work“-Anforderung zu begegnen



Unsere bisherige Security-Infrastruktur und -Strategie reicht für zukünftige Bedrohungsszenarien nicht aus

Investitionen in moderne Sicherheitslösungen

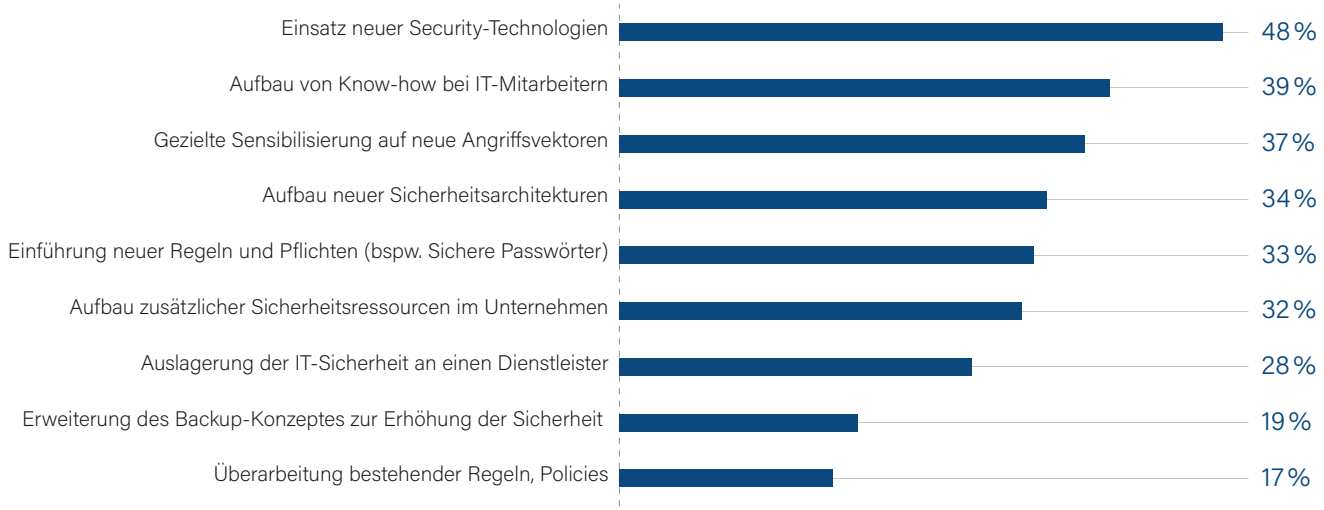
Um auch in Zukunft den wachsenden Gefahren durch Cyberkriminalität zu begegnen, müssen Unternehmen ihre IT-Sicherheitsvorkehrungen anpassen. Knapp die Hälfte der befragten Unternehmen möchte dabei in neue und moderne Security-Technologien investieren. Wie bereits festgestellt wurde, sind viele Unternehmen der Meinung, ihre derzeitigen Lösungen reichen nicht länger aus, um Cyberangriffe auch in Zukunft zu verhindern. Moderne Technologien helfen dabei, sich auf die sich stetig verändernde Sicherheitslage einzustellen und auch neue, vielleicht bislang unbekannte Gefahren abzuwehren.

Dahinter folgen zwei mitarbeiterzentrierte Maßnahmen. Zum einen wollen 39 Prozent der Unternehmen das Know-how der eigenen IT-Mitarbeiter verbessern, um schneller auf sich verändernde Gefahrenparameter zu reagieren.

Zum andern wollen 37 Prozent der Unternehmen die eigenen Mitarbeiter gezielt sensibilisieren. Sieht man sich beispielsweise die hohe Erfolgsquote von Phishing-Angriffen an, ist dieser Schritt mehr als nötig. Vor allem auch in Hinblick auf neue Angriffsvektoren, die Cyberkriminelle nutzen werden, um in Unternehmensnetzwerke einzudringen. Wenn zum Beispiel Phishing-Angriffe dank Sensibilisierung nicht mehr erfolgversprechend sind, werden andere Methoden zum Einsatz kommen. Cyberkriminelle schlafen nie und so ist es mehr als nötig, neben technischen Maßnahmen auch dafür Sorge zu tragen, dass die eigenen Mitarbeiter immer auf dem aktuellen Stand der Dinge sind, um auch neue Angriffsmethoden als solche zu erkennen und entsprechend zu handeln.

Maßnahmen zur Reduktion zukünftiger Cyber-Bedrohungen

Basis: 204 Unternehmen



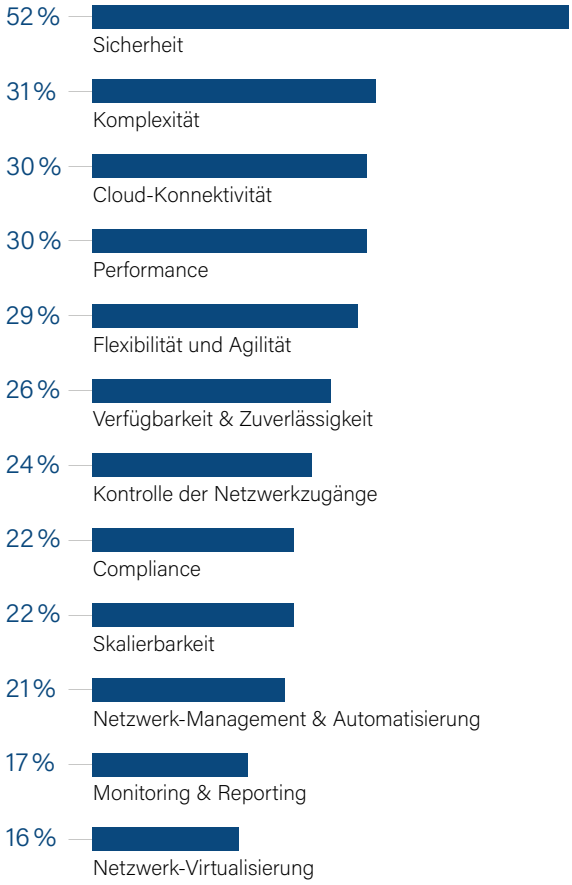
Probleme bei der Netzwerkausrichtung

Unternehmen stehen nicht nur vor IT-Security Herausforderungen, auch die Netzwerke müssen an die neuen Gegebenheiten angepasst werden. Die größte Herausforderung bei der zukünftigen Netzwerkausrichtung ist dabei mit weitem Abstand die Gewährleistung der Sicherheit. Für mehr als die Hälfte der Unternehmen ist die Sicherheit die Top-Herausforderung. Insbesondere Finanzdienstleister sehen hier ein großes Problemfeld. In dieser Branche sind 70 Prozent der Unternehmen besorgt, was die Sicherheit der zukünftigen Netzwerkausrichtung betrifft.

Dahinter folgen gleichauf mit knapp 30 Prozent die Komplexität der Netzwerke, die Performance und auch die Konnektivität zur Cloud.

Herausforderungen bei der zukünftigen Netzwerkausrichtung

Basis: 204 Unternehmen | Mehrfachnennungen



Mit SASE & Zero Trust gegen zukünftige Cybergefahren

Viele Unternehmen sehen sich mit den Sicherheitsherausforderungen der Zukunft überfordert. Daher müssen neue Ansätze in Erwägung gezogen werden, um die Netzwerksicherheit zu garantieren. Werkzeuge, um eine moderne und zukunftssichere Security-Architektur zu gestalten sind beispielsweise Zero Trust oder auch SASE. Vor allem im Hinblick auf die zunehmende Anzahl von Remote Mitarbeitern sind diese Ansätze für eine ganzheitliche Sicherheit nahezu unabdingbar.

Beim Zero-Trust-Ansatz handelt es sich um ein Sicherheitsprinzip, dass von vornherein niemandem vertraut und auf die Verifizierung jedes einzelnen Zugriffs auf Unternehmensressourcen setzt. Im Gegensatz zu traditionellen perimeterbasierten Ansätzen ist der Zero-Trust-Ansatz ein granularer, datenzentrierter Ansatz, der jeden Datenfluss auf Vertrauenswürdigkeit prüft.

SASE steht für Secure Access Service Edge und beschreibt ein Cloud-Architekturmodell, bei dem sowohl Netzwerk- als auch Security-as-Service-Funktionen gemeinsam in einem einzigen Cloud-Service bereitgestellt werden.

Dadurch können Unternehmen ihre Netzwerk- und Sicherheitswerkzeuge über eine einzige Verwaltungskonsole steuern und hat den Vorteil, nur wenig bis keine lokale Hardware nutzen zu müssen.

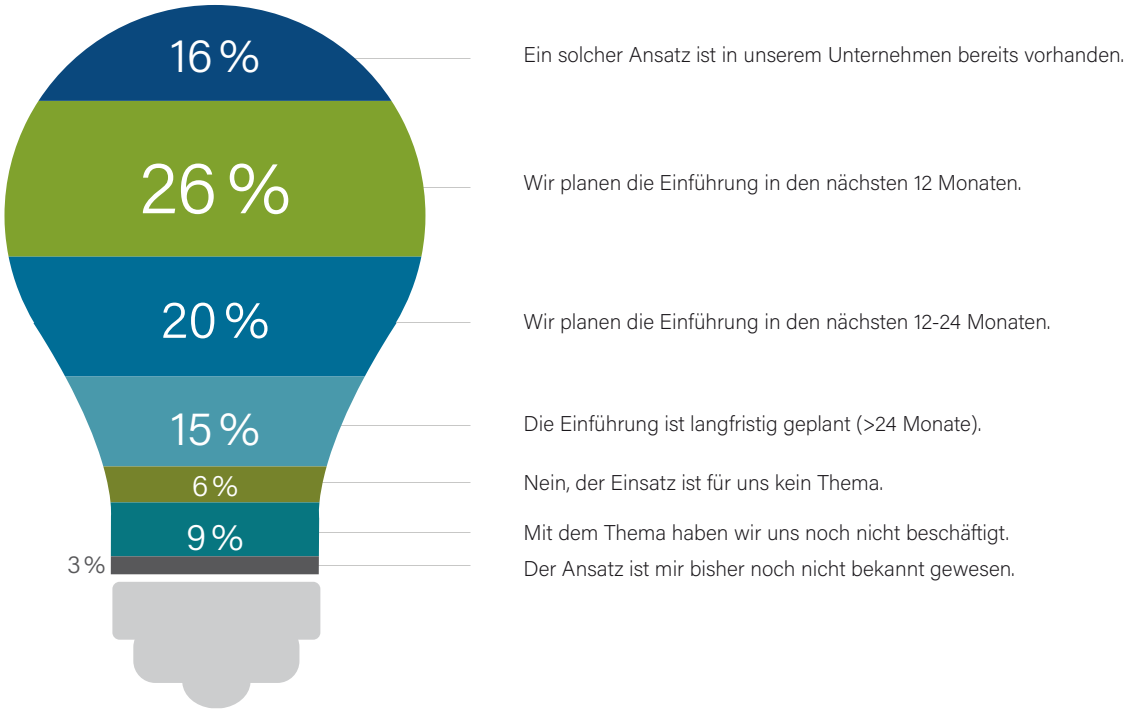
SASE und Zero Trust gehen dabei Hand in Hand. Erst durch den Zero Trust Network Access (ZTNA) kann das SASE-Rahmenwerk umgesetzt werden.

Beide Ansätze sind bislang nur in knapp 15 Prozent der Unternehmen im Einsatz. Jedoch wird der Anteil in den nächsten Jahren stark ansteigen. So geben 26 Prozent der Unternehmen an, in den nächsten 12 Monaten Zero Trust einzuführen, weitere 20 Prozent werden dies in den nächsten zwei Jahren durchführen und weitere 15 Prozent planen dies langfristig. Nur für knapp jedes zehnte Unternehmen hat es Zero Trust nicht einmal in die Planungsphase geschafft. Insgesamt lässt sich sagen, dass sich Zero Trust in den nächsten Jahren etablieren wird.

Ähnlich verhält es sich mit der Einführung einer SASE-Sicherheitsarchitektur. Hier wollen 25 Prozent der Unternehmen in den nächsten 12 Monaten auf SASE bauen, 17 Prozent planen dies innerhalb der nächsten zwei Jahre und weitere 13 Prozent langfristig.

Einsatz und Planung von Zero Trust

Basis: 204 Unternehmen | Keine Angabe 4 %



Zero Trust - Gründe und Nutzen

Die Gründe, warum Unternehmen Zero Trust einsetzen beziehungsweise einsetzen wollen, sind vielfältig. Besonders Aspekte in Bezug auf sichere standortübergreifende Arbeit stehen dabei im Fokus. So geben 58 Prozent der Unternehmen die sichere Anbindung und Vernetzung von Niederlassungen eine Bewertung von wichtig bis sehr wichtig und weitere 56 Prozent sehen die Aufrechterhaltung der Homeoffice-Infrastrukturen als wichtige Punkte an. Da Mitarbeiter heute zunehmend von außerhalb des Unternehmensnetzwerks auf Anwendungen zugreifen, ist es von besonderer Relevanz, dass die Zugriffe auch sicher sind. Denn alles, was außerhalb der Grenzen des Unternehmens stattfindet, ist außerhalb des Kontrollbereichs der Unternehmen und führt zu erhöhten Sicherheitsrisiken. Mit einer Zero-Trust-Architektur kann diese Sicherheit wiederhergestellt werden. Denn mit einem solchen Ansatz werden Unternehmensdaten geschützt, unabhängig davon, ob die Nutzer und Endgeräte innerhalb oder außerhalb des Unternehmens sind.

Faktoren & Treiber für die Einführung von Zero Trust

TOP 10

Basis: 204 Unternehmen | Anteil der Nennungen mit „Sehr wichtig" und „Wichtig"

58 % **Sichere Anbindung und Vernetzung von Niederlassungen**

56 % **Erhöhung Datensicherheit/Datenschutz**

56 % **Aufrechterhaltung der Homeoffice-Infrastrukturen**

55 % **Einhaltung von Vorschriften, Regeln, Richtlinien**

55 % **Schutz vor Insider-Bedrohungen**

54 % **Erhöhte Sicherheitsanforderungen hybrider IT-(Cloud-)Umgebungen**

53 % **Reduzierung Bedrohung Endpunkt- und IoT-Sicherheit**

53 % **Schutz vor Sicherheitslücken/Neuen Angriffsvektoren**

52 % **Unterstützung neuer agiler Entwicklungs-/Betriebskonzepte**

51 % **Steigerung der Betriebseffizienz**

Diese Erhöhung der IT-Sicherheit wird auch als größter Nutzen von Zero Trust angesehen. 60 Prozent der Unternehmen sagen, dass die Verringerung von Sicherheitsvorfällen der wichtigste Nutzen von Zero Trust ist. Passend dazu folgt auf dem zweiten Rang die höhere Zugriffssicherheit auf Cloud-Applikationen. Remote Arbeit und Cloud-Anwendungen sind aus den Unternehmen nicht mehr wegzudenken und werden auch in Zukunft nicht nur bestehen bleiben, sie werden auch noch ausgebaut. Der sichere Zugriff auf Cloud-Anwendungen ist daher essenziell für die Unternehmen.

Auch die Erhöhung der Netzwerksicherheit, die größte Herausforderung der Unternehmen im Bezug auf die Neuausrichtung ihrer Netzwerke, wird als besonders großer Nutzen angesehen. Es zeigt sich also, dass die Einführung von Zero Trust ein wesentlicher Bestandteil sein kann, um im Zuge des Aufbaus einer neuen und modernen Netzwerkarchitektur für größtmögliche Sicherheit zu sorgen.

Nutzen des Zero-Trust-Ansatzes

TOP 10

Basis: 204 Unternehmen | Anteil der Nennungen mit „Sehr hoher Nutzen" und „Hoher Nutzen"

60 % **Senkung von Sicherheitsvorfällen**

57 % **Höhere Zugriffssicherheit auf Applikationen in der Cloud**

57 % **Erhöhung der Netzwerksicherheit und Senken der Risiken**

56 % **Onboarding von Mitarbeitern und Unterstützung von New Work**

55 % **Einfachere Verwaltung und Agilität**

55 % **Unterstützung der IT-Strategie**

54 % **Verbesserte Netzwerkleistung**

54 % **Vereinfachung des Datenmanagements**

51 % **Reduktion von Kosten und Komplexität**

51 % **Reduktion von Ausfallzeiten**

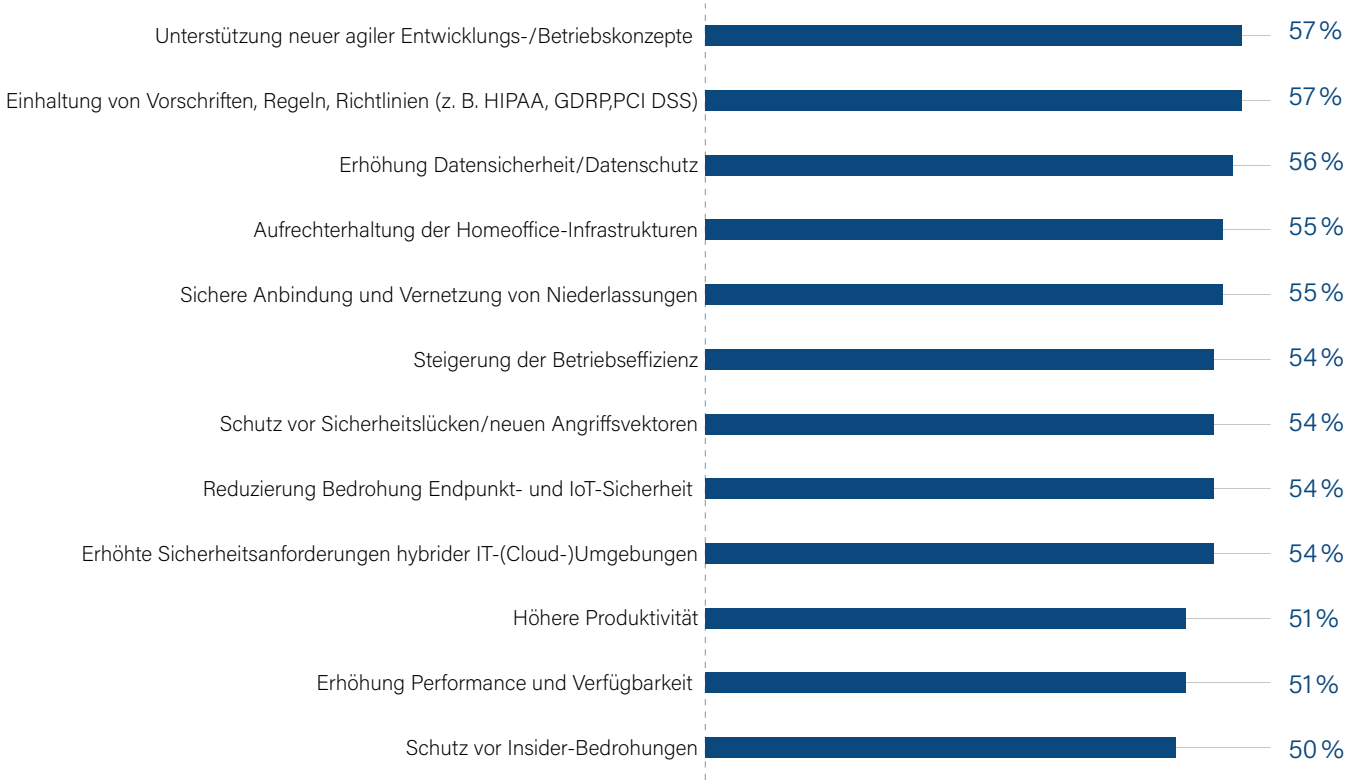
Gründe für SASE

Einer der Hauptgründe für die Einführung von SASE ist die Einhaltung von Richtlinien, Vorschriften und Regeln. 57 Prozent der Unternehmen geben diesem Punkt die höchste Relevanz. Beispielsweise lassen sich im Rahmen von SASE Unternehmensrichtlinien zentralisiert definieren, ähnlich wie bei Zero Trust. So kann die Plattform jederzeit die Vertrauenswürdigkeit der Geräte prüfen und nicht autorisierte Zugriffe blockieren.

Aber nicht nur Unternehmensrichtlinien können mit SASE implementiert werden, auch gesetzliche Anforderungen lassen sich damit durchsetzen. Beispielsweise lässt sich der gesamte Netzwerkverkehr in Übereinstimmung mit der DSGVO überwachen, womit Datenschutzverstöße frühzeitig abgewehrt werden.

Faktoren & Treiber für den Einsatz von SASE

Basis: 204 Unternehmen | Mehrfachnennungen | Nennungen mit "Sehr wichtig" und "Wichtig"



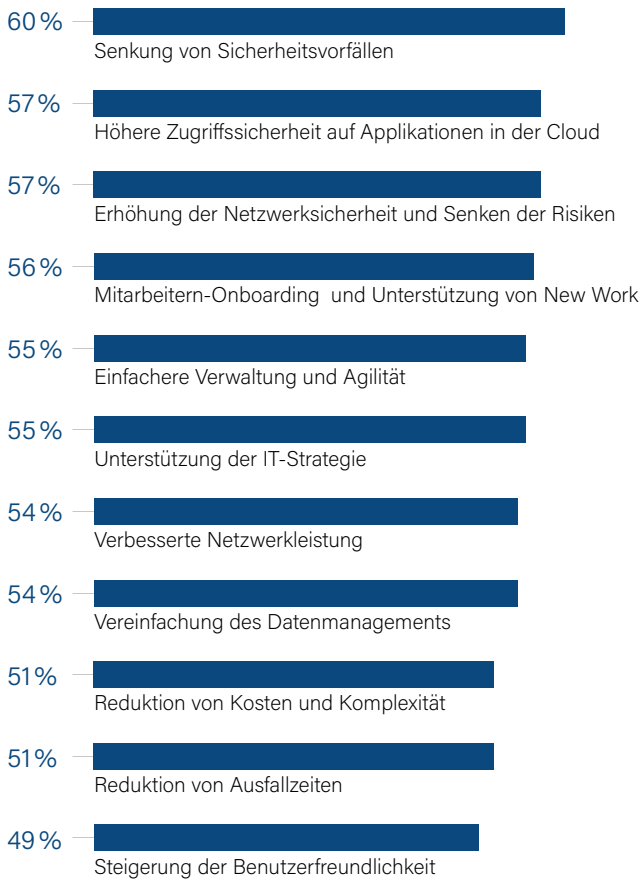
Vorteile von SASE

Analog zu Zero Trust sehen Unternehmen vor allem die massive Absenkung von Sicherheitsvorfällen als Hauptnutzen von SASE. Zwei Drittel der Befragten nannten dies als Kriterium mit hohem bis sehr hohem Nutzen für das eigene Unternehmen. Besonders die Unternehmen mit mehr als 5.000 Mitarbeitern sehen dies so. Mehr als 80 Prozent der Unternehmen in dieser Größenklasse sind überzeugt davon, mit SASE die Sicherheitsvorfälle drastisch zu verringern. Kein Wunder, bei der enormen Anzahl an Mitarbeitern, mit dem Netzwerk verbundenen Endgeräten, verschiedenen angebundenen Standorten und wahrscheinlich noch vielen teils veralteten Insellösungen. Für Cyberkriminelle bieten sich viele Gelegenheiten sich über die unterschiedlichen Angriffsvektoren Zugriff zu verschaffen.

Ebenfalls als großer Nutzen wird das Onboarding von Mitarbeitern gesehen. Denn das Onboarding einer großen Anzahl an Remote Workern erfordert eine schnelle Skalierung der Fernzugriffskapazität. Klassische VPN-Lösungen sind heute unzureichend, denn sie sind weder für die Cloud optimiert, sonderlich ressourcenschonend und auch nicht ganzheitlich sicher. Eine cloudbasierte Lösung wie SASE vereinfacht das Onboarding durch die schnelle Skalierung und sorgt dafür, dass mobile Mitarbeiter sicher agieren können.

Nutzen einer SASE-Architektur

Basis: 204 Unternehmen | Mehrfachnennungen | Nennungen mit "Sehr hoher Nutzen" und "Hoher Nutzen"



Was verhindert die Einführung von Zero Trust und SASE

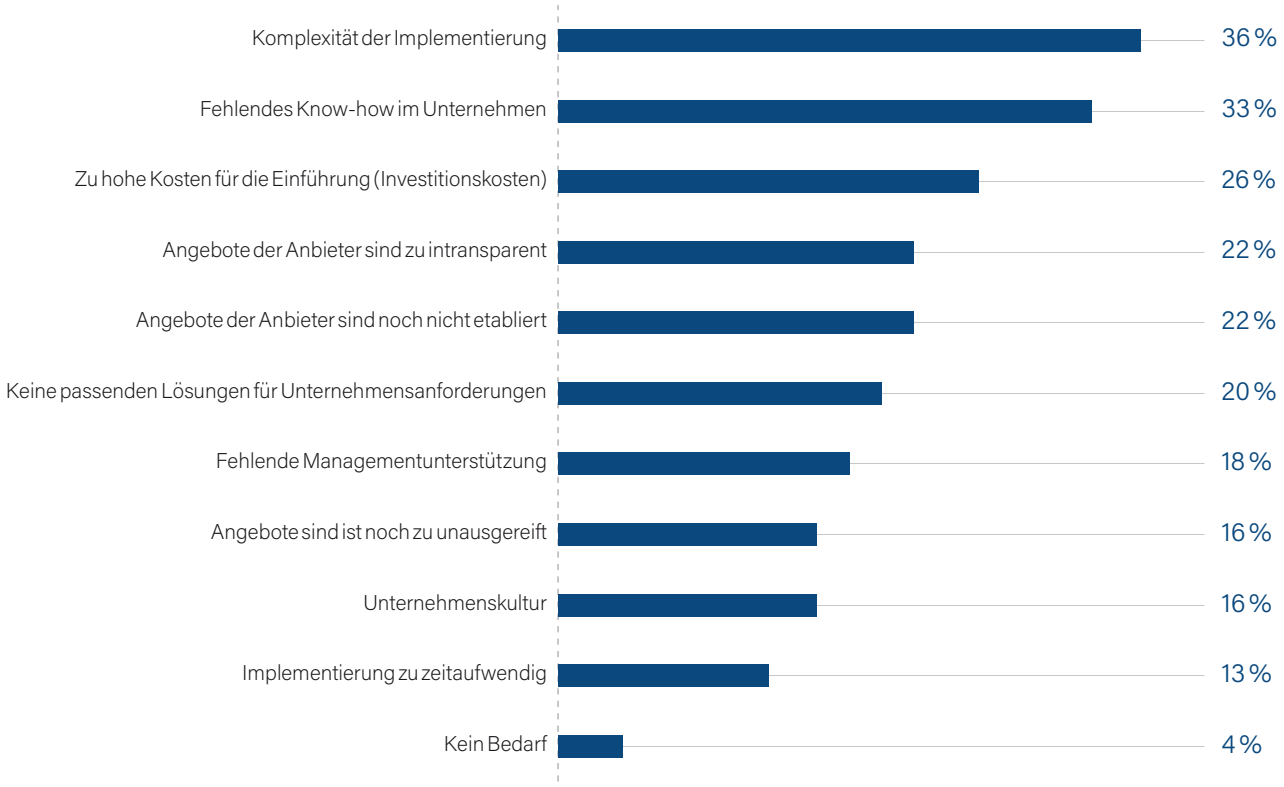
Obwohl die Vorteile und der Nutzen von modernen Sicherheitsarchitekturen wie Zero Trust oder SASE klar auf der Hand liegen, sind viele Unternehmen bisher noch zögerlich bei der Implementierung gewesen oder sind es auch in Zukunft noch.

Auf die Frage, welche Gründe bislang oder auch dauerhaft gegen eine Einführung neuer Sicherheitskonzepte stehen, sagten 36 Prozent der befragten Unternehmen, die Komplexität der Implementierung erweise sich als große Hürde.

Die Einführung moderner Sicherheitskonzepte hängt auch mit den Fortschritten der Unternehmen in Themen wie der Cloud-Transformation oder auch die allgemeine Komplexität von Identitätsmanagement zusammen. Um neue Sicherheitskonzepte einzuführen, müssen zuallererst die Rahmenbedingungen gegebenenfalls mit einer Nachrüstung der bestehenden Systeme, Anwendungen und Netzwerke umgesetzt werden.

Gründe gegen den Einsatz von Zero Trust/SASE

Basis: 175 Unternehmen | Mehrfachnennungen | Filter: Unternehmen, die Zero Trust, SASE noch nicht implementiert haben



Technische/organisatorische Maßnahmen im Zuge von Zero Trust und SASE

Um im Zuge der Implementierung von Zero Trust oder SASE von allen Vorteilen profitieren zu können, planen Unternehmen auch weitere Veränderungen in ihrer Sicherheitsarchitektur. Beispielsweise stellt die Erstellung von Nutzerprofilen und dementsprechend auch die Einführung von Nutzerrichtlinien hoch im Kurs. Ein Drittel der Unternehmen plant hier in den nächsten Jahren Veränderungen. Die Anforderungen an Zugänge zu Unternehmensdaten werden durch Remote-Arbeit und Cloud immer komplexer.

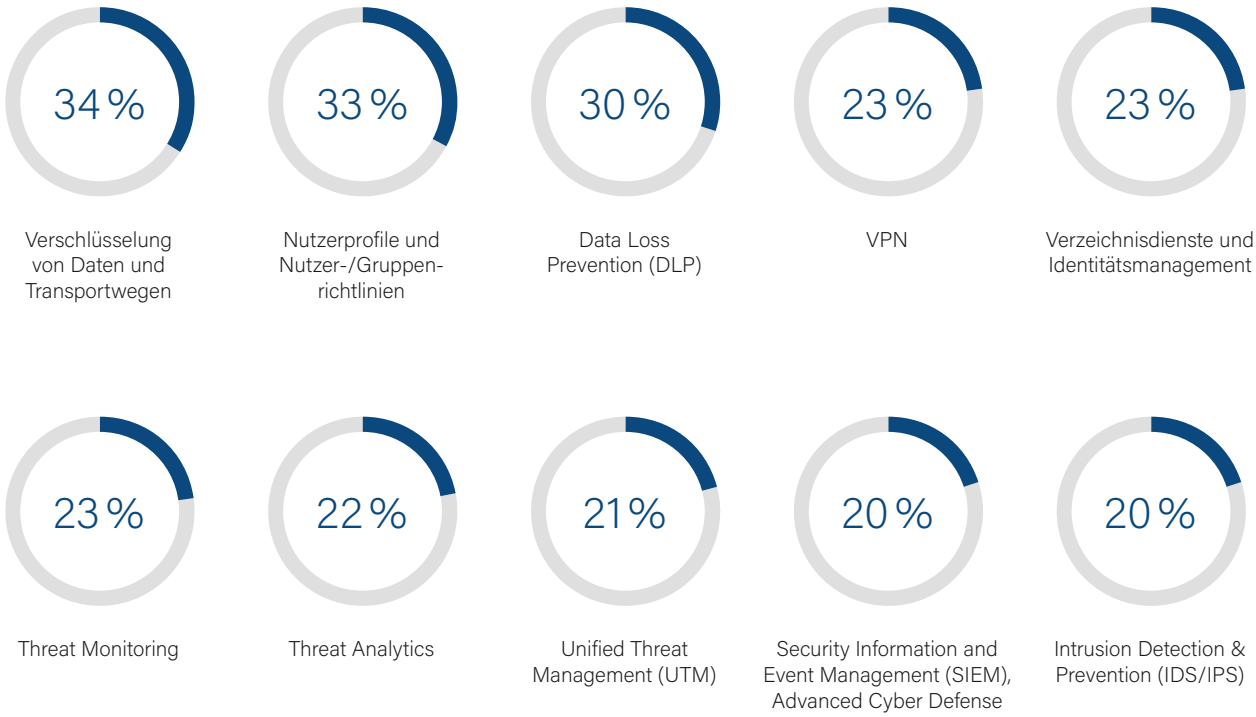
Auch die Verschlüsselung von Daten und insbesondere Transportwegen wird für die Unternehmen in Zukunft ein wichtiger Faktor sein. Vor allem der Zugriff auf Cloud-Applikationen birgt Gefahren.

Auf der einen Seite sind Cloud-Dienste schnell eingerichtet, oftmals wird aber auch die Sicherheit vernachlässigt. Viele Cloud-Dienste nutzen nur eine Transportverschlüsselung wie SSL und sichern den Traffic zwischen dem Browser und dem Server ab. Wichtig ist allerdings auch die Daten auf dem Cloud-Server erneut zu verschlüsseln, denn hier liegen die Daten im Klartext vor und können von Cyberkriminellen ausgelesen werden. Und nur diejenigen Nutzer, die auch berechtigt sind, auf die Daten zuzugreifen, sollten im Rahmen der vorher definierten Nutzerprofile die nötigen Entschlüsselungscodes erhalten.

Geplante technischen Maßnahmen/Lösungen (Veränderungen innerhalb der bisherigen Sicherheitsarchitektur) innerhalb des Aufbaus von Zero-Trust-/SASE-Architekturen in den nächsten Jahren

TOP 10

Basis: 204 Unternehmen | Mehrfachnennungen | Top 10



Nicht nur technische Maßnahmen müssen von den Unternehmen ergriffen werden, um die IT-Sicherheit zu gewährleisten. Im Zuge des Aufbaus neuer Sicherheitsarchitekturen lohnt auch eine Neugestaltung oder Optimierung der organisatorischen Maßnahmen. Mehr als ein Drittel der Unternehmen möchte in absehbarer Zeit Notfall- und Reaktionspläne erstellen. Insbesondere der Handel (44 Prozent) und die Logistik (50 Prozent) sehen Nachholbedarf beim Aufbau eines Business Continuity Plans. Klar definierte Anweisungen wie in einem Notfall reagiert werden soll, stellen ein wichtiges Werkzeug für die Aufrechterhaltung des Geschäftsbetriebs dar.

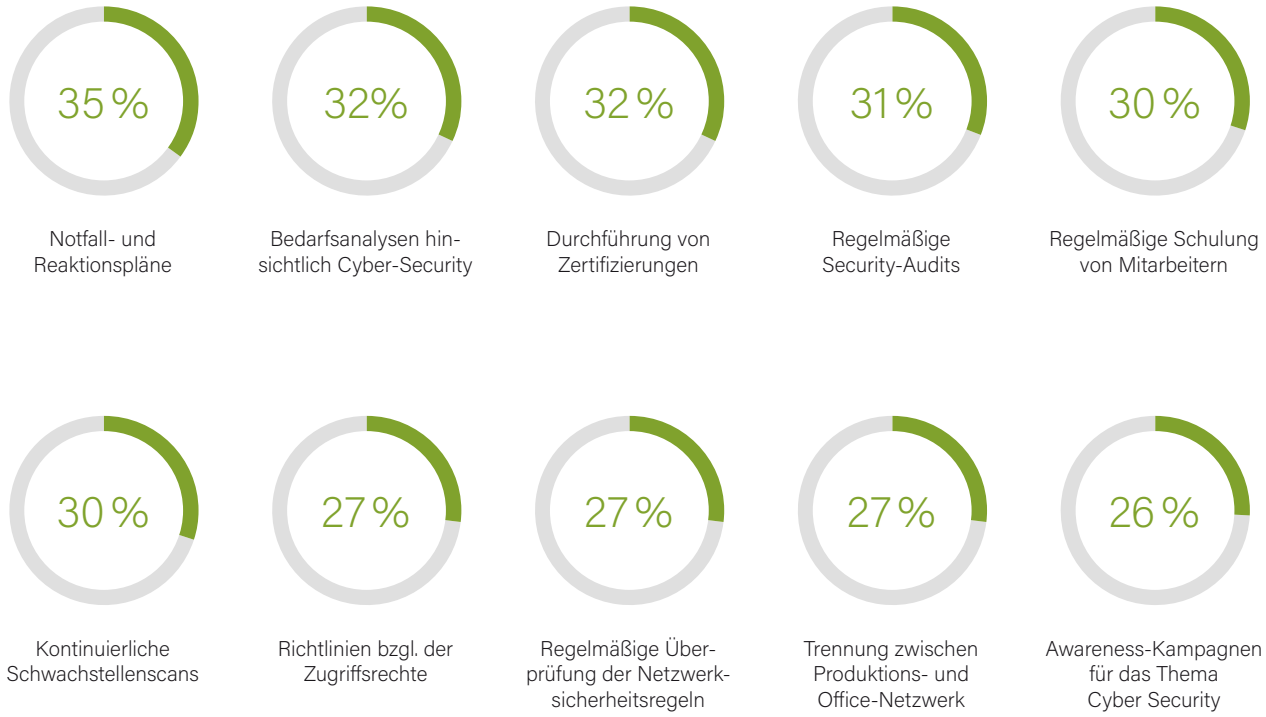
Dadurch entfällt im Ernstfall der Druck von schnellen und vielleicht falschen Entscheidungen und die Schäden lassen sich eindämmen.

Ebenfalls wichtig sind auch Maßnahmen wie die regelmäßige Schulung von Mitarbeitern, um ihnen das richtige Verhalten im Hinblick auf aktuelle Gefahren zu vermitteln oder auch regelmäßige Sicherheitsaudits, um die eigenen Systeme auf Schwachstellen hin zu untersuchen und diese schnell zu beheben.

Geplante organisatorische Maßnahmen innerhalb des Aufbaus von Zero-Trust-/ SASE-Architekturen in Unternehmen (Mehrfachnennungen möglich)

Basis: 204 Unternehmen | Mehrfachnennungen | Top 10

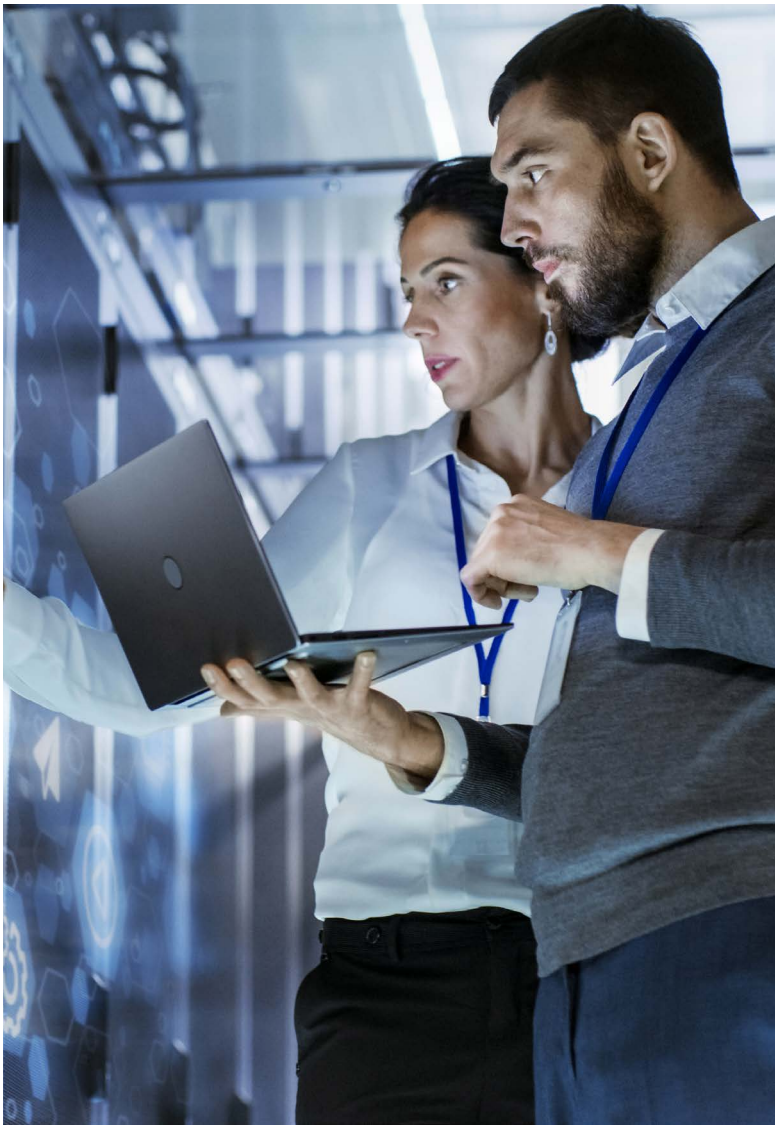
TOP 10



Security-Verantwortung bleibt In-House

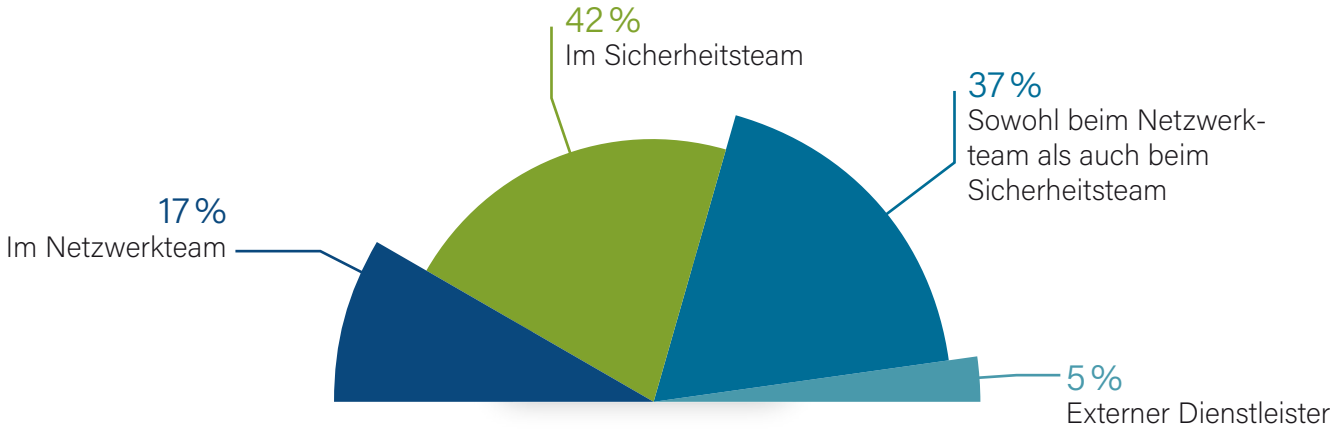
Obwohl das Auslagern von Cybersicherheit als Weg gegen den bekannten Fachkräftemangel innerhalb von Unternehmen sein kann, sind nur die wenigsten Unternehmen bereit dazu, ihre Verantwortung für Sicherheit abzugeben. Nur fünf Prozent der Unternehmen lagern die Verantwortung für Entscheidungen rund um die Architektur und zu Produkten im Rahmen von Cyber Security an einen externen Dienstleister aus. Dabei bedienen sich tendenziell eher kleinere Unternehmen der Expertise von externen Dienstleistern, wenn auch auf niedrigem Niveau. Während beispielsweise sechs Prozent der Unternehmen bis 999 Mitarbeitern die Verantwortung komplett in die Hände von Externen legen, sind es bei Unternehmen ab 1000 Mitarbeitern nur knapp zwei Prozent. Auf Branchenseite ist es vor allem der öffentliche Sektor, der die Verantwortung an Externe abgibt (15 Prozent). Hier macht sich der Fachkräftemangel besonders bemerkbar.

Sicherheitsrelevante Themen werden entweder nur im Security-Team (42 Prozent) oder in Kooperation zwischen Sicherheits- und Netzwerkteam (37 Prozent) angegangen. Signifikante Unterschiede bezogen auf Unternehmensgrößen gibt es dabei kaum. Lediglich in Unternehmen zwischen 1000 und 4999 Mitarbeitern wird deutlich stärker interdisziplinär gearbeitet. Hier geben 42 Prozent an, dass sowohl das Netzwerk- als auch das Sicherheitsteam gemeinsam die Verantwortung übernehmen und bei einem Drittel ist es nur das Sicherheitsteam. In den anderen Größenklassen ist das Verhältnis genau umgekehrt.



Hauptverantwortung für Entscheidungen zur Architektur/zu Produkten für Cyber-Security-Lösungen

Basis: 204 Unternehmen



Externe Unterstützung bei der Umsetzung

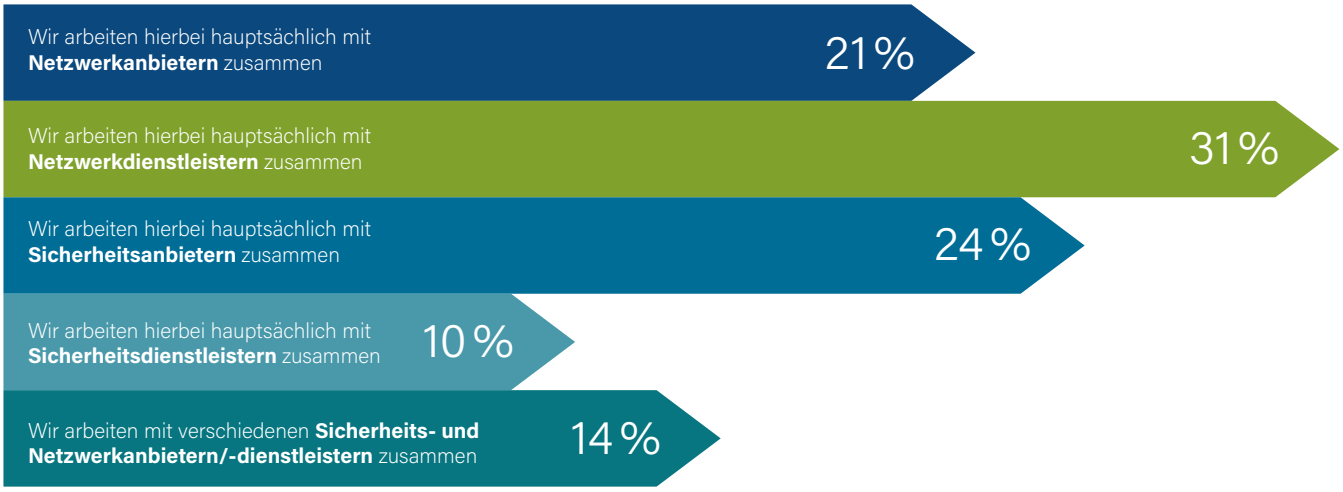
Um die technischen sowie organisatorischen Maßnahmen im Hinblick auf die Umgestaltung der Netzwerk- und IT-Sicherheit im Unternehmen zu implementieren, stehen den Unternehmen verschiedene Wege zur Auswahl. Sie können direkt mit den Herstellern von Netzwerk- oder Sicherheitsinfrastruktur zusammenarbeiten oder auch mit Dienstleistern in diesen Bereichen.

Primär arbeiten die Unternehmen mit Netzwerkdienstleistern zusammen (31 Prozent). Dahinter folgen mit knapp einem Viertel die Anbieter von Lösungen für IT-Sicherheit.

Je größer das Unternehmen, desto seltener wird direkt mit Netzwerkanbietern zusammengearbeitet. Kleinere Unternehmen bis 499 Mitarbeitern wählen tendenziell öfter die Anbieter von Netzwerktechnologie (27 Prozent) als Hauptumsetzungspartner aus, als dies bei den größten Unternehmen der Fall ist (17 Prozent).

Implementierung/Umsetzung von Cyber-Security-Maßnahmen

Basis: 173 Unternehmen



Knapp 14 Prozent nutzen sowohl die Expertise von Sicherheits- als auch Netzwerkanbietern/-dienstleistern. Solche interdisziplinären Teams finden sich in den größeren Unternehmen öfter als in den kleineren. So setzen beispielsweise 17 Prozent der Unternehmen ab 5.000 Mitarbeitern auf einen Mix aus Sicherheits- und Netzwerkanbietern/-dienstleistern. Im Gegenzug dazu sind nur knapp 11 Prozent der Unternehmen bis 499 Mitarbeitern bereit sich mit mehreren Anbietern bzw. Dienstleistern an die Maßnahmenumsetzung zu begeben.

Fazit

Cyberrisiken gehören zu den größten Risiken, denen Unternehmen ausgesetzt sind. Seien es Phishing-Angriffe oder Ransomware, jedes Jahr steigt die Anzahl an Cyberattacken und die Heftigkeit dieser an. Die Konsequenzen reichen von finanziellen Verlusten durch Beseitigung der Schäden oder Zahlungen von Lösegeldern über Störungen oder Komplettausfälle des Geschäftsbetriebs bis hin zu Reputationsverlusten oder im allerschlimmsten Fall sogar existenzbedrohenden Folgen.

Das Schutzniveau mag heute in vielen Unternehmen gerade noch so ausreichen, um Cyberangriffe zu verhindern, doch in Zukunft werden die über Jahre gewachsenen alten, perimeterbasierten Security-Infrastrukturen an ihre Grenzen stoßen.

Denn die Zunahme an Remote-Arbeit und der Siegeszug der Cloud erfordern mehr denn je neue Ansätze bei der IT-Sicherheit. Die klassische Netzwerksicherheit reicht heutzutage nicht länger aus, um auch in Zukunft noch für ein robustes und sicheres Netzwerk zu sorgen, denn Cyberkriminelle schlafen nicht und machen sich die veränderten Arbeitsstrukturen sowie den fehlerbehafteten Menschen zunutze. So nutzen diese beispielsweise ungesicherte Geräte, die von außerhalb der Mauern des Unternehmensnetzwerks auf Unternehmensdaten zugreifen.

Unternehmen müssen sich daher der veränderten Gefahrenlage anpassen und mit neuen Ansätzen wie Zero Trust oder auch SASE dagegen ansteuern. Heute haben erst die wenigsten Unternehmen Zero Trust beziehungsweise SASE-Architekturen in ihren Unternehmen implementiert. Doch in Zukunft wollen immer mehr Unternehmen auf diese modernen Ansätze zurückgreifen.

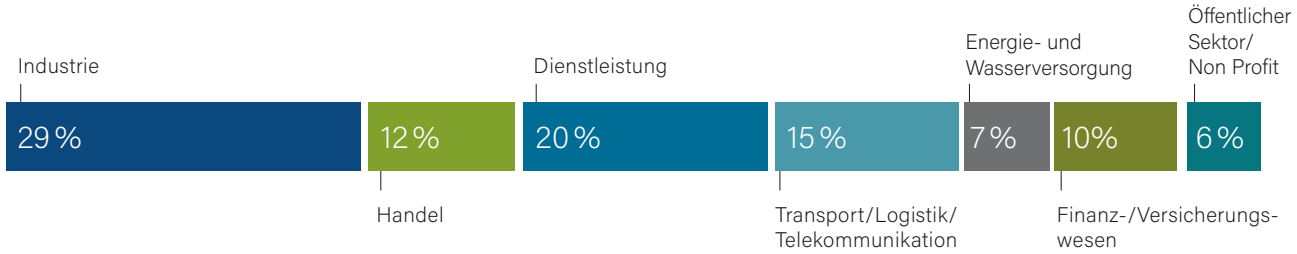
Zero Trust und SASE sorgen dafür, dass die IT-Sicherheit auch in Zukunft gewährleistet bleibt, egal von welchem Gerät oder welchem Ort auf Unternehmensdaten und -anwendungen zugegriffen wird. Beide Ansätze sind nicht voneinander zu trennen. SASE ohne Zero Trust wird kaum die gewünschten Effekte bringen.

Die Vorteile liegen dabei klar auf der Hand. SASE ist eine ganzheitliche Betrachtung der IT-Sicherheit und stellt eine strategische Herangehensweise dar, die eine Neugestaltung von modernen und sicheren IT-Infrastrukturen ermöglicht, die auf die neuen Anforderungen rund um Cloud und Remote-Arbeit ausgerichtet ist. Zero Trust bringt den nötigen Kontrollmechanismus mit ein, der durch kontinuierliche Validierung garantiert, dass nur die richtigen Nutzer und Geräte auf die für sie bestimmten Applikationen zugreifen können. Dadurch sinken die Angriffsflächen für Cyberkriminelle massiv und Unternehmen können die Vorteile von Cloud-Diensten und Remote Arbeit bei maximaler Sicherheit nutzen.

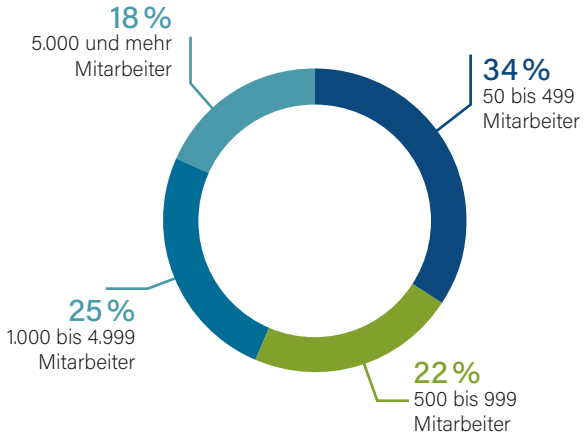
Stichprobe

Die Studie „Cyber Security neu gedacht! – Wie neue Konzepte wie Zero Trust oder SASE bestehende Sicherheitskonzepte umkrempeln" wurde von der techconsult GmbH in Zusammenarbeit mit den Unternehmen LANCOM Systems GmbH, macmon secure GmbH, McAfee Enterprise, NCP engineering GmbH, SEP AG und Sophos Technology GmbH konzipiert und durchgeführt. Im ersten Quartal 2022 wurden hierzu 204 Anwenderunternehmen aus allen relevanten Branchen ab 50 Mitarbeitern zu dem Stellenwert und der Entwicklung ihrer Cyber-Security-Maßnahmen in deutschen Unternehmen befragt und in dem vorliegenden Studienbericht beschrieben, wie oft sie von Cyberangriffen betroffen waren, welche Konsequenzen das für sie hatte, welche Mittel sie zur Bekämpfung von Cyberattacken verwenden und wie der Reifegrad ihrer Umsetzung von Zero Trust und SASE-Konzepten ist.

Branchen



Mitarbeitergrößenklassen



Position im Unternehmen

9%	Vorstand / Geschäftsführung
10%	Chief Information Officer (CIO) / IT-Leiter
24%	Leiter Informationssicherheit / CSO / CISO
19%	IT-/Informationssicherheitsbeauftragter
4%	Interner/externer Datenschutzbeauftragter
3%	Leiter IT-Infrastruktur / RZ
2%	Leiter Netzwerk
21%	Abteilungsleiter, Bereichsleiter, Projektleiter
8%	Berater/Consultant

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

Telefon: +49 (0)561 8109 181
E-Mail: **raphael.napieralski@techconsult.de**

techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

Telefon: +49 (0)561 8109 0
Fax.: +49 (0)561 8109 101
Web: **www.techconsult.de**

Über techconsult GmbH

Die techconsult 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 techconsult 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 SEP AG

Die SEP AG ist europäischer Pionier im Bereich von netzwerkweiten und plattformübergreifenden Datenverfügbarkeitssystemen. Seit 1992 werden dazu führende Technologien entwickelt und in eine der schnellsten und betriebssichersten Datenverfügbarkeitslösungen integriert. Die SEP Softwarelösungen sorgen in multinationalen Konzernen sowie in kleinen Unternehmen für eine sichere und funktionierende Datenverfügbarkeit. Mit den bewährten SEP-Produkten SEP sesam, SEP sesam bare system recovery und SEP live recovery ist in vielen, weltweit vernetzten Installationen die Datenverfügbarkeit eine sichere Realität.

Kontakt

SEP AG
Konrad-Zuse-Straße 5
83607 Holzkirchen

Telefon: +49 8024 46331 0
Fax: +49 8024 46331 666
E-Mail: **info@sep.de**
Web: **www.sep.de**

Eine Studie von

techconsult
TECHNOLOGY MARKET ANALYSTS
30 YEARS ANNIVERSARY

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de

Telefon: +49 561 8109 0
Telefax: +49 561 8109 101
Web: www.techconsult.de

In Zusammenarbeit mit

SEP Hybrid Backup