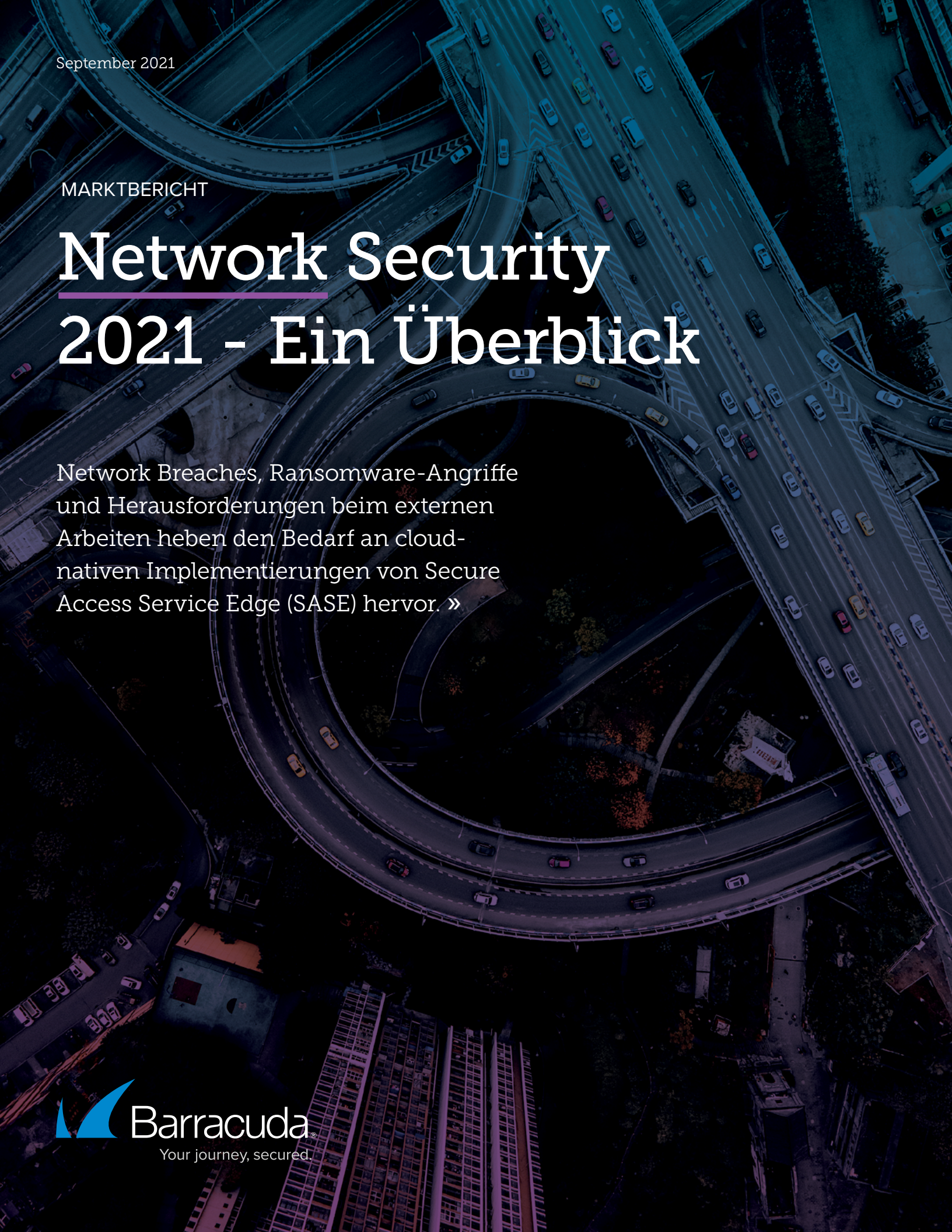


September 2021

MARKTBERICHT

Network Security 2021 - Ein Überblick

Network Breaches, Ransomware-Angriffe und Herausforderungen beim externen Arbeiten heben den Bedarf an cloud-nativen Implementierungen von Secure Access Service Edge (SASE) hervor. »

Barracuda®
Your journey, secured.

Inhalt

Einleitung

Digitale Transformation, Pandemie und Cybersecurity

Die COVID-19-Pandemie zwang globale Unternehmen dazu, in kürzester Zeit alle erforderlichen Maßnahmen zu ergreifen, um ihren Mitarbeitern die Arbeit im Homeoffice zu ermöglichen. Damit diente die Pandemie als Katalysator für die digitale Transformation, veranlasste Unternehmen jedoch auch dazu, ihre bestehenden Security-Architekturen neu zu evaluieren.

Die Public Cloud ist der digitalen Transformation schon lange Zeit förderlich und wird dies auch zukünftig bleiben. In diesem Kontext gibt es gute und schlechte Neuigkeiten. Die schlechte Nachricht ist, dass Unternehmen ständig unter Beschuss stehen und ein beträchtlicher Teil der auf sie ausgeübten Angriffe Ransomware beinhalten. Die gute Nachricht ist, dass Unternehmen mehr und mehr in SASE-Lösungen (SASE = Secure Access Service Edge) investieren, um Angriffe abzuwehren, ihre Netzwerke zu schützen und gleichzeitig ein hybrides Arbeitsmodell unterstützen zu können.

In diesem Bericht befassen wir uns nun eingehend mit dem Wechsel in die Cloud, dem externen Arbeiten und damit verbundenen Sicherheitsbedenken sowie einer Vielzahl von Problemen und Herausforderungen im Zusammenhang mit Cybersecurity-Risiken.

Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer globalen Umfrage unter **IT-Entscheidungsträgern, die für das Networking, die Public Cloud und die Security ihres Unternehmens verantwortlich sind**. Befragt wurden **750 Umfrageteilnehmer** aus zahlreichen unterschiedlichen Branchen, darunter **aus dem Bauwesen, der Energiewirtschaft, dem Finanzdienstleistungsbereich, der Medienbranche, der Fertigung, dem Einzelhandel und der Technologiebranche**. Die Umfrageteilnehmer aus den **USA, Europa und der APAC-Region** vertraten Unternehmen mit mindestens 500 Mitarbeitern. Die europäischen Teilnehmer stammen aus dem Vereinigten Königreich, Frankreich und Deutschland, Teilnehmer aus der APAC-Region aus Indien, Australien, Singapur und Hongkong. Die Umfrage wurde zwischen Juli und August 2021 durchgeführt.

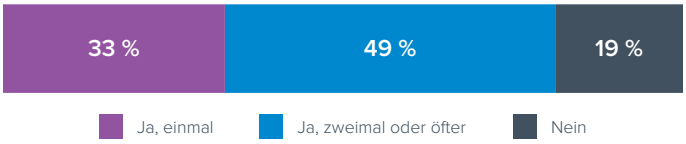
Sicherheitsverletzungen

ERKENNTNIS Nr. 1

Die Systeme von Unternehmen werden immer wieder angegriffen – häufig kommt dabei Ransomware zum Einsatz.

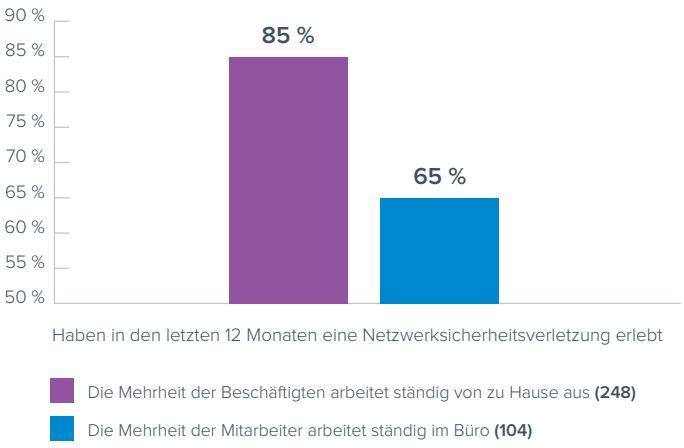
Hat Ihr Unternehmen in den letzten 12 Monaten eine Sicherheitsverletzung als direkte Folge eines Netzwerkangriffs erlitten?

(n=750)



Ein Drittel der Befragten (33%) gab an, dass ihr Unternehmen im letzten Jahr einmal Opfer eines Sicherheitsverstoßes geworden ist, und fast die Hälfte (49%) gab an, zweimal oder öfter erfolgreich angegriffen worden zu sein.

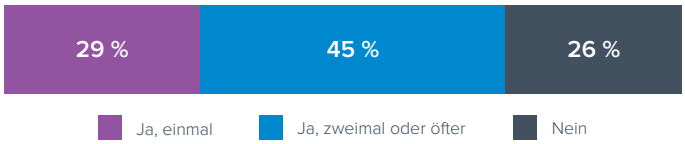
Verstöße gegen die Netzwerksicherheit im Zusammenhang mit externen Arbeiten



Unternehmen mit Mitarbeitern, die überwiegend von zu Hause aus arbeiteten, verzeichneten mit 85% deutlich häufiger Netzwerksicherheitsverletzungen im Vergleich zu Unternehmen, deren Mitarbeiter hauptsächlich im Büro arbeiteten – mit nur 65%. Interessanterweise führte die Ausgabe von unternehmenseigenen Geräten zu keiner Verbesserung. Im Gegenteil: Unternehmen, die unternehmenseigene Geräte für Mitarbeiter bereitstellten, erlebten etwas mehr Sicherheitsverletzungen (82%) als Unternehmen, die das nicht getan hatten (81%).

Wurde Ihr Unternehmen in den letzten 12 Monaten Opfer eines Ransomware-Angriffs?

(n=750)

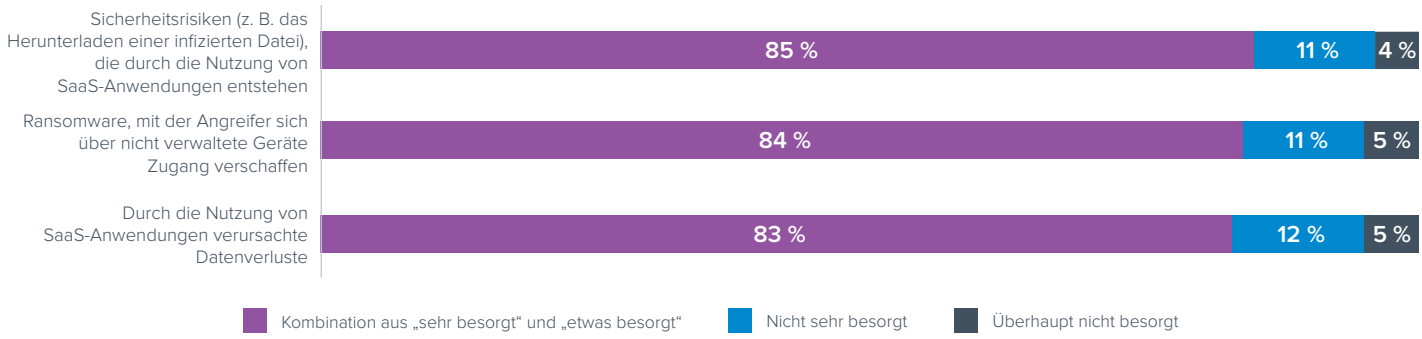


Ganze 74% der Befragten gaben an, dass ihr Unternehmen im letzten Jahr Opfer mindestens eines Ransomware-Angriffs wurde. Fast die Hälfte (45%) gab an, in diesem Zeitraum zwei oder mehr Angriffe erlebt zu haben. Vergleicht man die Ransomware-Angriffsraten mit den oben erörterten Raten der Netzwerksicherheitsverletzungen, so wird deutlich, dass die meisten Verletzungen auf Netzwerkebene mit Ransomware einhergehen.

Das externe Arbeiten kann zu einem erhöhten Risiko erfolgreicher Sicherheitsverletzungen und Ransomware-Angriffe führen, da einerseits die Heim-IT-Systeme nicht ordnungsgemäß kontrolliert werden können und Mitarbeiter andererseits mit einer höheren Wahrscheinlichkeit COVID-19-bezogene Phishing-E-Mails erhalten.

Wie besorgt sind Sie über: Sicherheitsrisiken, Datenverluste und Ransomware, mit der Angreifer sich über nicht verwaltete Geräte Zugang verschaffen?

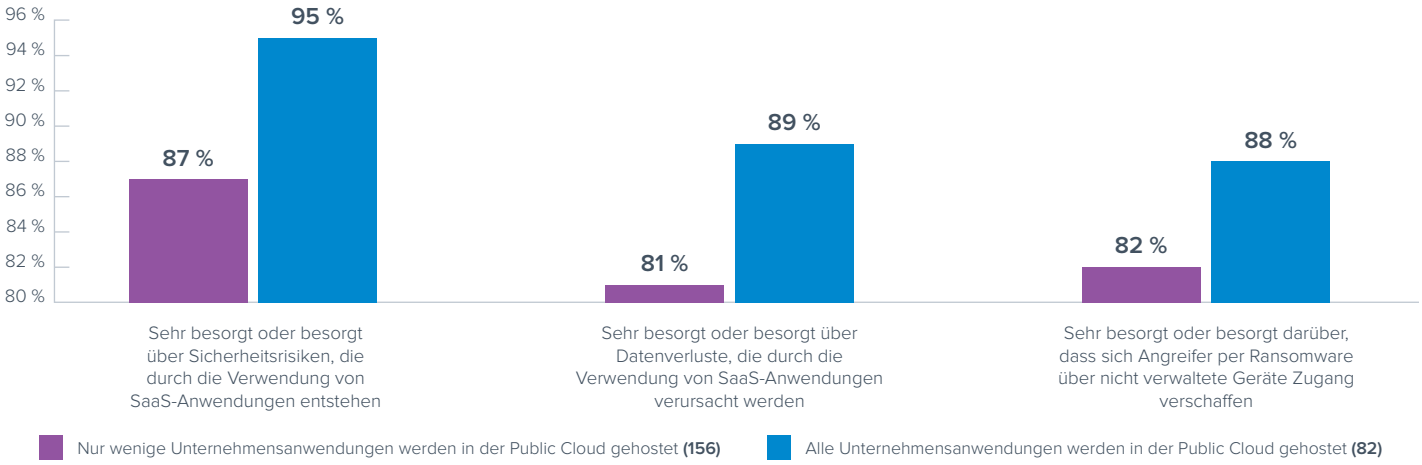
(n=750)



Es herrscht große Unsicherheit unter unseren Teilnehmern hinsichtlich Cybersecurityrisiken und Angriffen im Zusammenhang mit der Nutzung von Software-as-a-Service(SaaS)-Anwendungen. Fast die Hälfte aller Befragten ist sehr besorgt über Security, Datenverluste und Ransomware. Nimmt man die Befragten hinzu, die etwas besorgt sind, steigt die Rate auf über 80% an.

Wenn Unternehmen mehr Anwendungen in der Public Cloud hosten, machen sie sich auch mehr Sorgen um die Sicherheit ihrer SaaS-Anwendungen. Dieser Zusammenhang ist schlüssig und ist auch ein Indiz dafür, dass seitens der Unternehmen Sicherheitsbedenken in Bezug auf ihre SaaS-Apps bestehen.

SaaS-Sicherheitsbedenken in Bezug auf die Einführung der Public Cloud



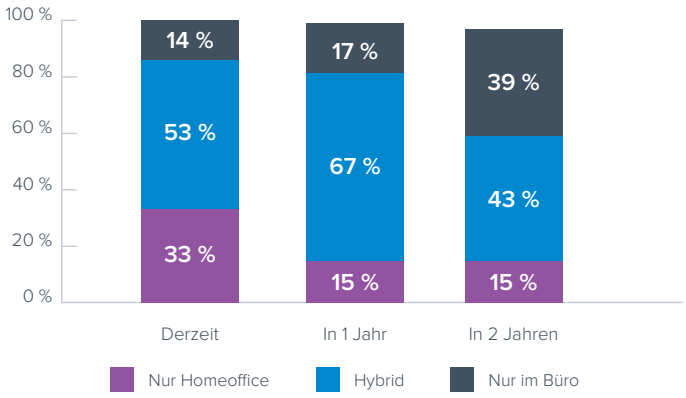
Extern arbeiten

ERKENNTNIS Nr. 2

Trotz schneller Internetanbindung erleben Mitarbeiter im Homeoffice weiterhin Herausforderungen in Bezug auf Arbeitsprozesse und Servicequalität.

Wie hoch ist der Anteil der Mitarbeiter Ihres Unternehmens, die in den folgenden Zeiträumen per Fernzugriff arbeiten bzw. arbeiten werden?

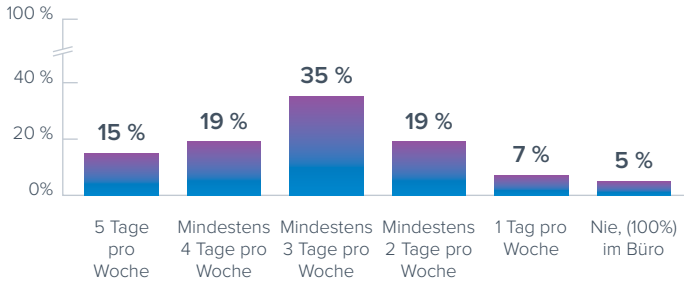
(n=750)



Im Durchschnitt arbeiten derzeit nur 14% der Beschäftigten in den befragten Unternehmen ausschließlich im Büro. In einem Jahr wird dieser Prozentsatz voraussichtlich geringfügig auf 17% ansteigen. Selbst in zwei Jahren werden voraussichtlich nur 39% der Beschäftigten ständig im Büro arbeiten. Die Mehrheit wird teilweise (43%) oder vollständig von zu Hause aus arbeiten (15%). Offensichtlich wird zukünftig ein hybrides Arbeitsmodell bevorzugt, daher sollten IT-Teams sich auf die Unterstützung einer hybriden Belegschaft vorbereiten.

Wie oft arbeiten Sie von zu Hause aus?

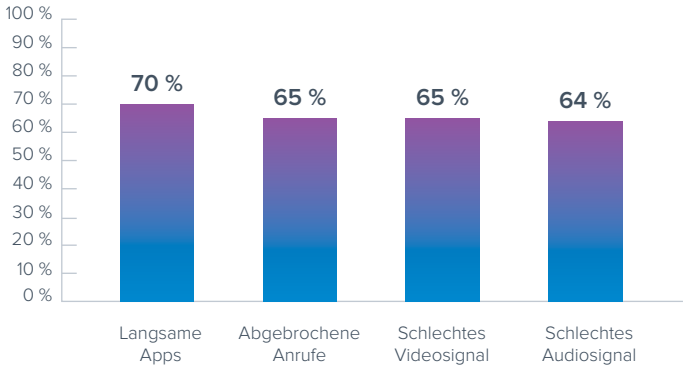
(n=750)



95% der Befragten arbeiten mindestens einen von fünf Arbeitstagen im Homeoffice. Fast ein Fünftel (19%) arbeitet an mindestens vier Tagen pro Woche im Homeoffice. Etwas mehr als ein Drittel (35%) arbeitet an mindestens drei Tagen pro Woche zu Hause.

Wenn Sie von zu Hause aus arbeiten, wie häufig treten dann die folgenden IT-Probleme auf, die Ihre Arbeit behindern?

(n=712)

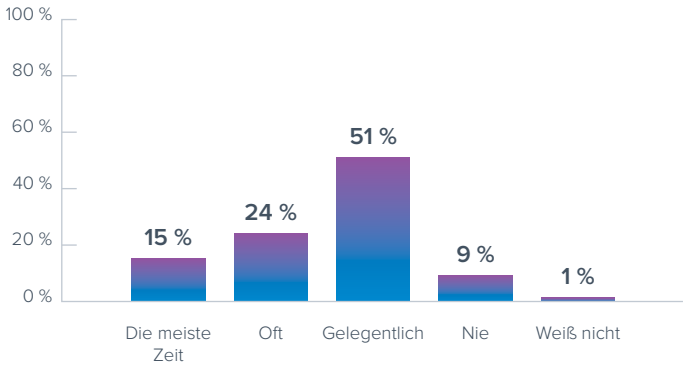


Mehr als 75% der Befragten, die von zu Hause aus arbeiten, haben High-Speed-Internet, sind aber immer noch mit Schwierigkeiten konfrontiert – darunter aufgrund von langsamen Apps, Anrufabbrüchen sowie schlechter Video- und Audioqualität.

94% der Befragten mit unternehmenseigenen Geräten teilen ihre private Internetverbindung mit anderen Mitgliedern ihres Haushalts. Nur 6% nutzen eine separate Verbindung. Das Risiko von Sicherheitsverstößen besteht also weiterhin.

Wie oft kommt es vor, dass Ihre Benutzer bei der Arbeit von zu Hause aus IT-Probleme haben, die sie bei ihrer Arbeit behindern?

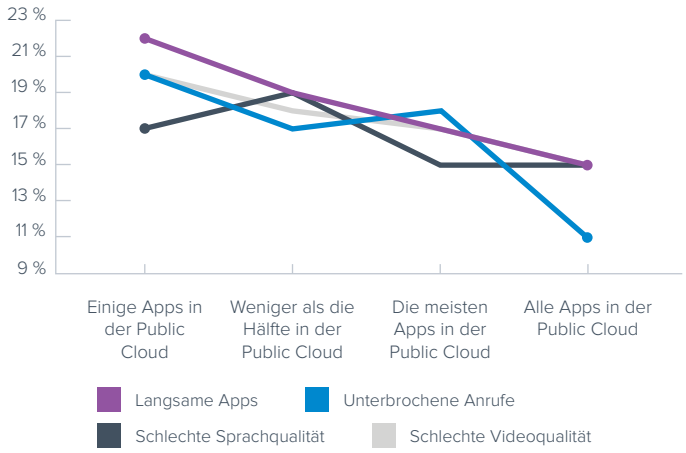
(n=646)



Mehr als die Hälfte der Befragten (51%) gab an, dass Nutzer gelegentlich Störungen erleben. 39% gaben an, dass sie oft oder meistens Störungen erleben. Nur 9% gaben an, dass ihre Nutzer nie Störungen erleben.

Selbst die IT-Teams haben mit solchen Schwierigkeiten zu kämpfen. 70% haben mit langsamen Anwendungen, unterbrochenen Anrufen (65%), schlechter Sprachqualität (64%) und schlechter Videoqualität (65%) zu kämpfen. Etwa 30% gaben an, dass sie im Homeoffice nie auf eines dieser Probleme stoßen.

Häufig gemeldete IT-Probleme bei der Arbeit im Homeoffice vs. Wechsel in die Public Cloud



Einen positiven Effekt scheint in diesem Kontext die Anzahl der in der Cloud gehosteten Apps zu bewirken – je mehr Cloud-Apps verwendet werden, desto besser das Nutzererlebnis. Fazit: SaaS-Anwendungen und Cloud-Bereitstellungen tragen zur Verbesserung der Benutzerfreundlichkeit bei.

Unternehmen, die ihre Sicherheitsprobleme im Griff haben, berichten auch von deutlich weniger IT-Problemen bei der Arbeit im Homeoffice. In Unternehmen, die von einer Netzwerksicherheitsverletzung betroffen waren, berichteten 44% der Mitarbeiter von IT-Problemen. Nur 16% der Mitarbeiter von Unternehmen, die nicht von einer Netzwerksicherheitsverletzung betroffen waren, berichteten von IT-Problemen. Das sind gute Neuigkeiten, denn das zeigt, dass Verbesserungen im Bereich der Security sich auch positiv auf die Benutzerfreundlichkeit auswirken.

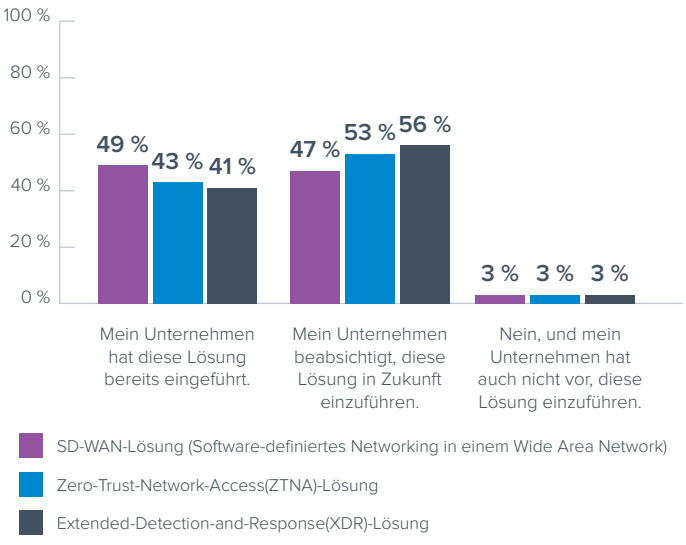
SASE: Software-Defined Wide Area Network (SD-WAN)

ERKENNTNIS Nr. 3

Secure-Access-Service-Edge(SASE)-Technologien werden zur Abwehr von Angriffen auf die Security und zur Lösung von Problemen beim Arbeiten im Homeoffice in Betracht gezogen.

Hat Ihr Unternehmen bereits eine der folgenden Lösungen eingeführt oder plant, diese in den nächsten zwei Jahren oder darüber hinaus einzuführen?

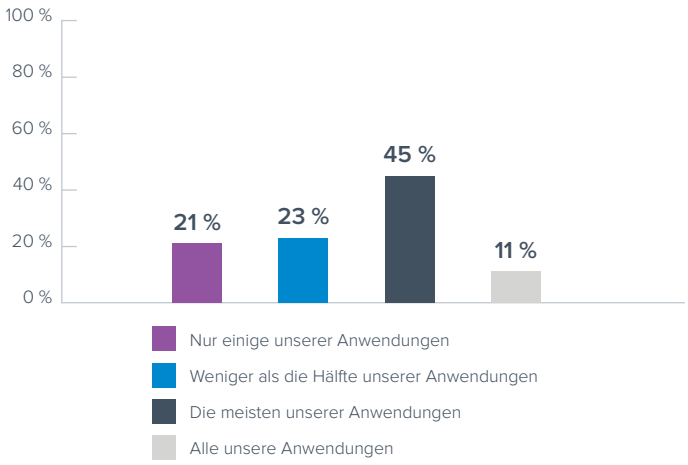
(n=750)



96% der Befragten gaben an, dass sie SD-WAN bereits einsetzen (49%) oder planen, dies in Zukunft zu tun (47%).

Wie viele Ihrer Unternehmensanwendungen werden derzeit in der Public Cloud gehostet?

(n=750)



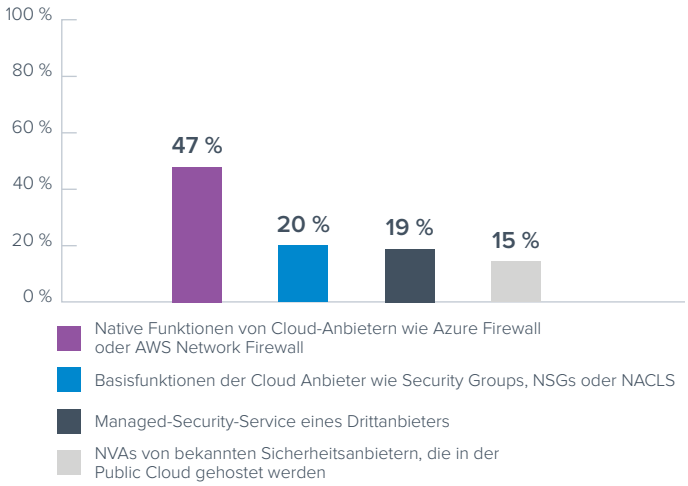
11% der Befragten gaben an, dass sie alle Apps in der Public Cloud hosten, und weitere 45%, dass sie die meisten ihrer Apps in der Public Cloud hosten. Zweifellos werden also viele Anwendungen in der Public Cloud bereitgestellt.

Public-Cloud-Bereitstellungen bringen in vielen Fällen auch die Einführung von SD-WAN und Zero Trust Network Access (ZTNA) mit sich, was Sinn macht, da beide Technologien zur Unterstützung von Cloud-Umgebungen entwickelt wurden.

Fast drei Viertel der Unternehmen, die alle ihre Anwendungen in der Public Cloud hosten, haben SD-WAN bereits implementiert (73%). Das sind doppelt so viele wie Unternehmen mit nur wenigen Anwendungen in der Public Cloud (37%). Ebenso haben 68% der Unternehmen, die alle ihre Anwendungen in der Public Cloud hosten, ZTNA eingeführt, während nur 38% der Unternehmen mit nur wenigen Anwendungen in der Public Cloud ZTNA einsetzen. Unternehmen, die stärker von der Public Cloud abhängig sind, haben mit größerer Wahrscheinlichkeit eine SD-WAN-Lösung implementiert.

Welche der folgenden Angebote nutzt Ihr Unternehmen hauptsächlich, um Security-Maßnahmen in seiner Public-Cloud-Umgebung umzusetzen?

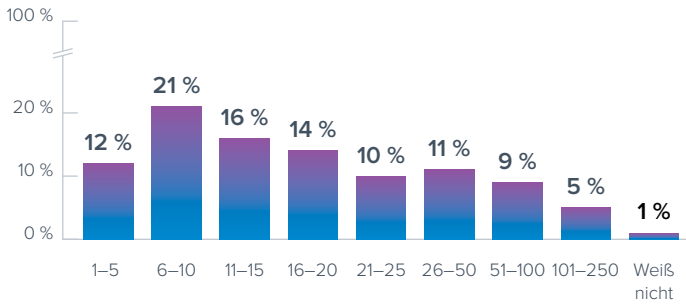
(n=750)



Nahezu die Hälfte der Befragten (47%) nutzt die Basisfunktionalität der Cloud-Anbieter, wie Azure Firewall oder AWS Network Firewall. Darüber hinaus nutzen 20% die grundlegenden Cloud-Angebote.

Wie viele SaaS-Anwendungen werden in Ihrem Unternehmen offiziell genutzt?

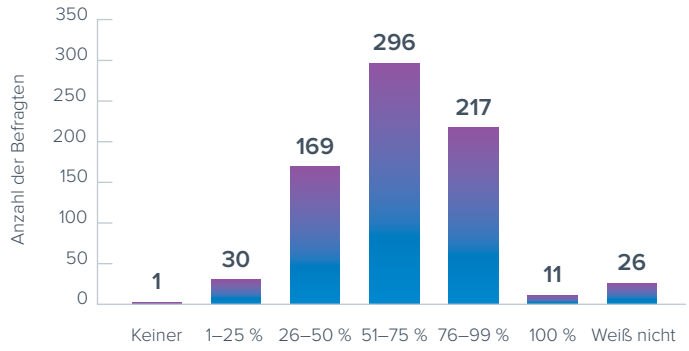
(n=750)



Im Durchschnitt kommen in Unternehmen 31 SaaS-Anwendungen zum Einsatz. 12% nutzen zwischen einer und fünf Anwendungen. 21%, also die Mehrheit, nutzen zwischen sechs und 10 Anwendungen. 5% nutzen mehr als 100 Anwendungen.

Abgesehen von dem Traffic für offiziell genutzte SaaS-Anwendungen, welcher Prozentsatz des geschäftsbezogenen Datenverkehrs Ihrer Büros oder entfernten Endpunkte wird Ihrer Einschätzung nach an Ihre öffentlichen Cloud-Anbieter (z. B. Azure, AWS) – im Vergleich zu anderen Büros oder Rechenzentren – geleitet?

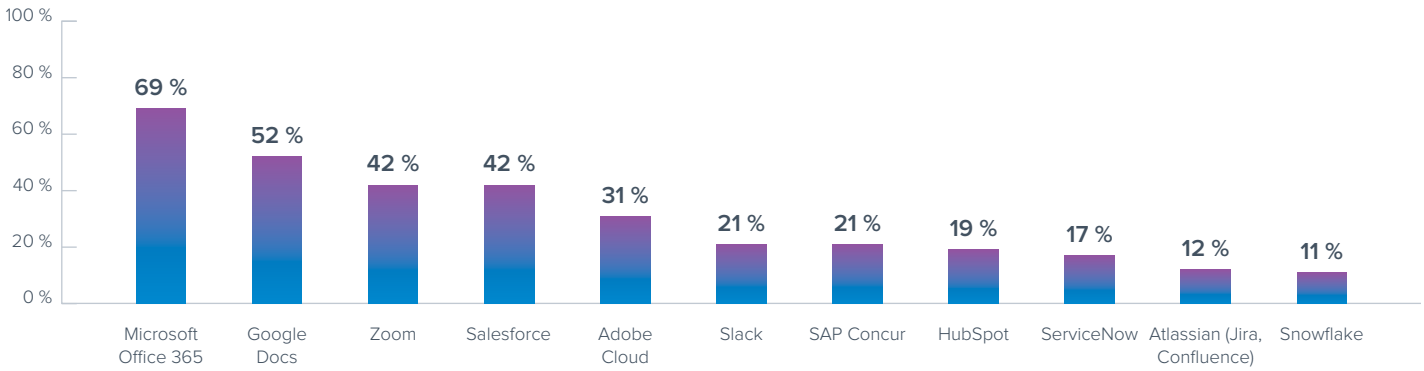
(n=750)



Durchschnittlich gaben die Befragten an, dass 64% ihres Datenverkehrs an Public-Cloud-Anbieter gesendet werden. 39% gaben an, dass zwischen der Hälfte und drei Vierteln des geschäftsbezogenen Datenverkehrs an ihre Public-Cloud-Anbieter geleitet wird.

Welche SaaS-Anwendungen werden in Ihrem Unternehmen am meisten genutzt?

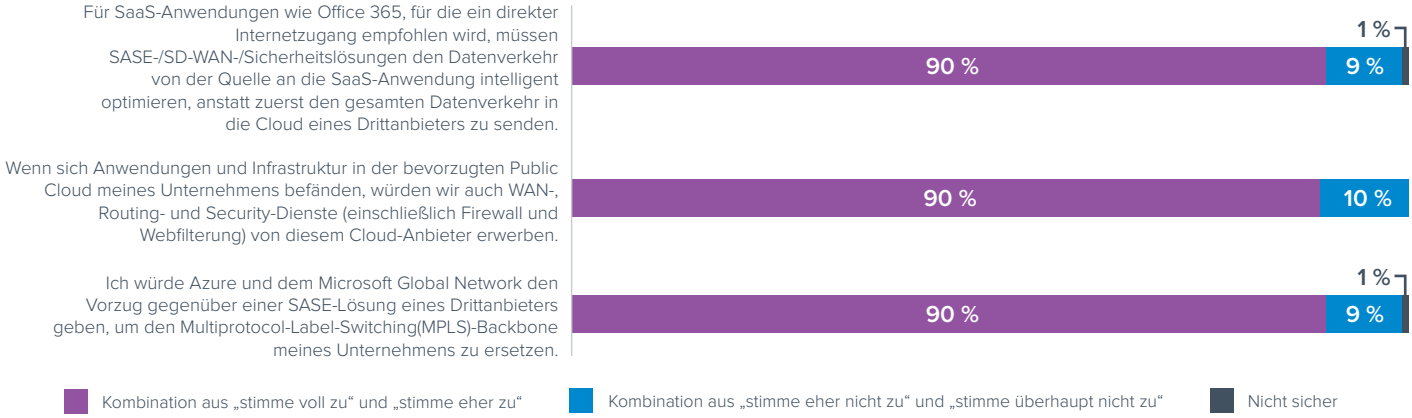
(n=749)



Office 365, Google Docs, Zoom und Salesforce sind die meistgenutzten Anwendungen.

Stimmen Sie diesen Aussagen zu oder nicht zu?

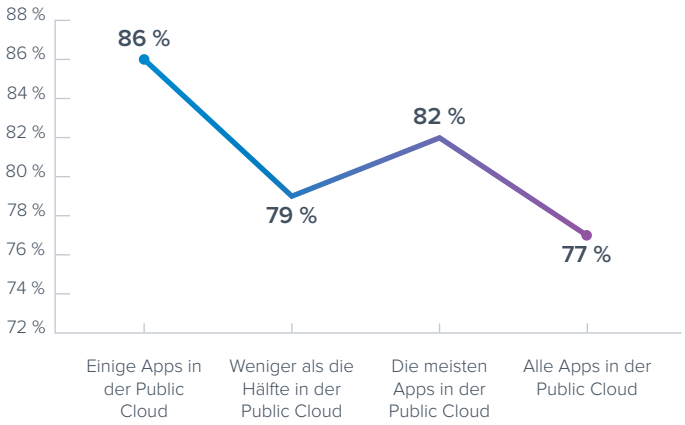
(n=750)



Die Befragten bevorzugten Drittanbieter und Drittlösungen. Die große Mehrheit (90%) erwartet, dass ein direkter Zugriff auf SaaS-Anwendungen möglich ist. 90% gaben an, dass wenn sich Anwendungen und Infrastruktur in der bevorzugten Public Cloud ihres Unternehmens befänden, sie auch WAN-, Routing- und Security-Dienste (einschließlich Firewall und Webfilterung) von diesem Cloud-Anbieter erwerben würden.

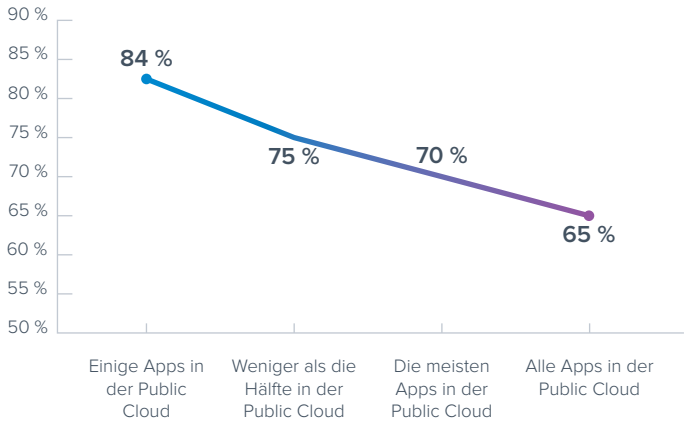
90% sagen, sie würden Azure und dem Microsoft Global Network den Vorzug gegenüber einer SASE-Lösung eines Drittanbieters geben, um den Multiprotocol-Label-Switching(MPLS)-Backbone ihres Unternehmens zu ersetzen. Unternehmen erkennen die Vorteile von cloudnativen und SaaS-Lösungen und geben an, dass sie Public-Cloud-Anbietern hinsichtlich ihrer Netzwerkinfrastrukturen eher vertrauen würden.

Haben in den letzten 12 Monaten mindestens eine Netzwerksicherheitsverletzung erlebt



Der Wechsel in die Cloud spielt auch eine Rolle bei Verletzungen der Netzwerksicherheit. Je öfter Unternehmen die Public Cloud zum Hosten ihrer Anwendungen einsetzen, desto seltener werden sie erfolgreich angegriffen.

Haben in den letzten 12 Monaten mindestens einen Ransomware-Angriff erlebt



Unternehmen, die alle ihre Anwendungen in der Public Cloud hosten, hatten in den letzten 12 Monaten seltener mit Sicherheitsverletzungen und Ransomware-Angriffen zu kämpfen.

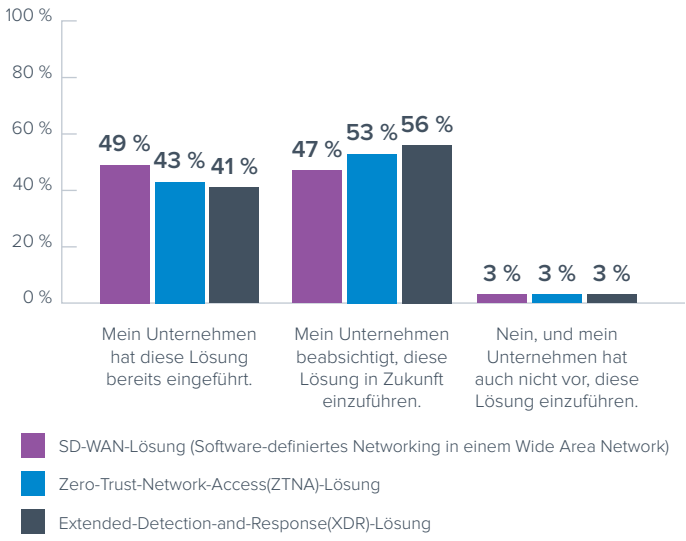
SASE: Zero Trust Network Access (ZTNA)

ERKENNTNIS Nr. 4

Unternehmen investieren in Secure-Access-Service-Edge(SASE)-Technologien.

Hat Ihr Unternehmen bereits eine der folgenden Lösungen eingeführt oder plant, diese in den nächsten zwei Jahren oder darüber hinaus einzuführen?

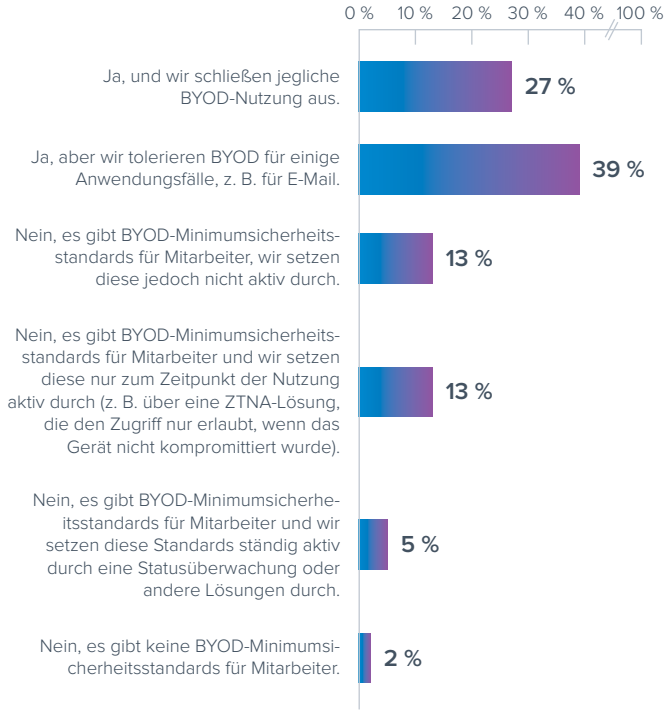
(n=750)



96% der Befragten gaben an, dass sie ZTNA bereits eingesetzt haben (43%) oder planen, dies in Zukunft zu tun (53%).

Müssen Mitarbeiter auf firmeneigenen Geräten (anstatt privaten/BYOD-Geräten) arbeiten?

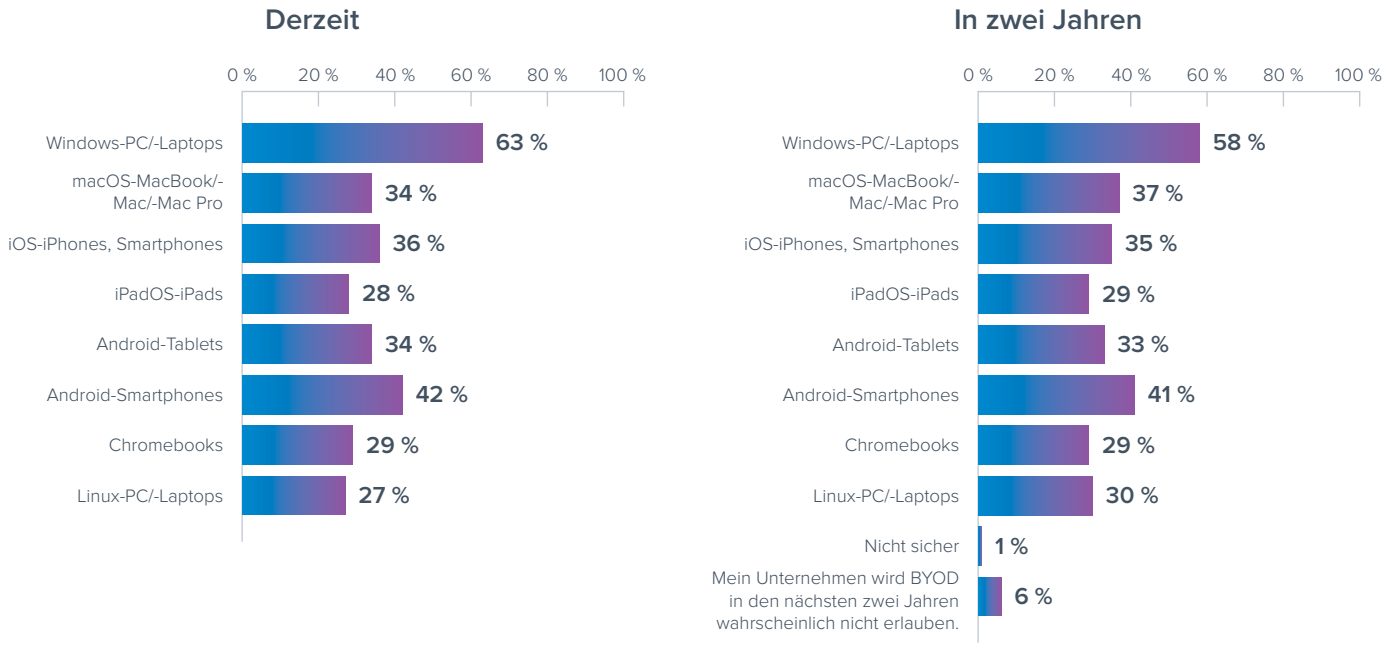
(n=750)



Fast sieben von zehn Befragten (67%) gaben an, dass sie vom Unternehmen zur Verfügung gestellte Geräte verwenden müssen, obwohl 39% von ihnen angaben, dass Bring Your Own Device (BYOD) in einigen Fällen erlaubt ist.

Für welche der folgenden Endgeräte ist in Ihrem Unternehmen BYOD derzeit erlaubt bzw. wird es in zwei Jahren erlaubt sein?

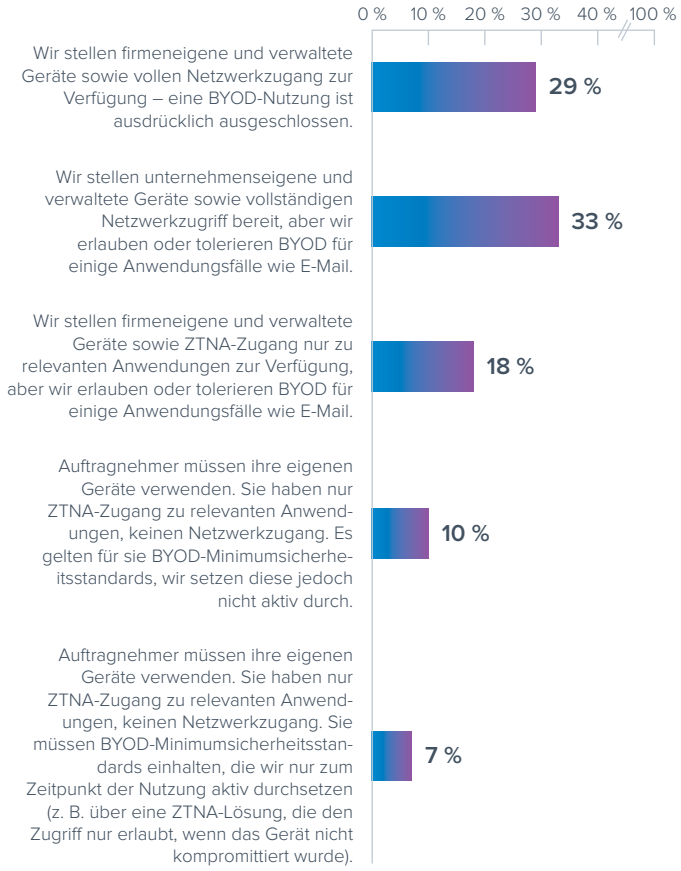
(n=543)



Unternehmen verwenden eine Vielzahl von Geräten für BYOD, darunter Geräte mit Windows, macOS, iOS, Android und Linux oder Chromebooks. In den nächsten 24 Monaten sind keine signifikanten Änderungen geplant. Um BYOD zu unterstützen, muss ZTNA für alle Gerätetypen und Betriebssysteme verfügbar sein.

Welche der folgenden Aussagen beschreibt am besten die Art und Weise, wie Ihr Unternehmen Vollzeitauftragsnehmern Zugang zu Netzwerken/ Anwendungen gewährt?

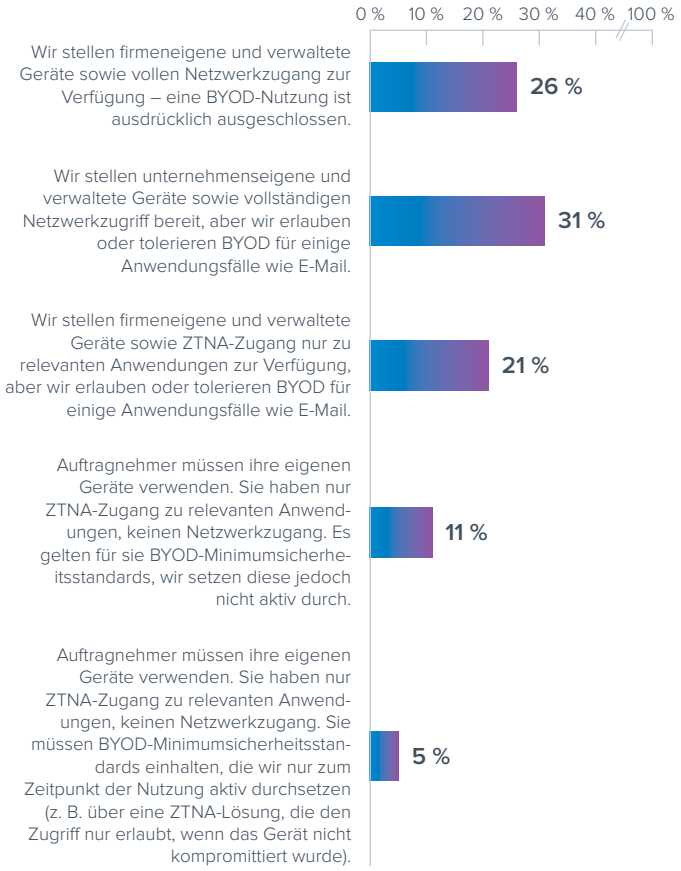
(n=750)



Knapp zwei Drittel (60%) der Befragten, die über einen erfolgreichen Ransomware-Angriff berichteten, geben unternehmenseigene Geräte mit vollem Netzwerkzugang an Auftragnehmer aus. 20% der Befragten, die von einem erfolgreichen Ransomware-Angriff berichten, geben unternehmenseigene Geräte an Auftragnehmer mit ZTNA-Zugang aus.

Wie gewährt Ihr Unternehmen temporären Auftragnehmern Zugang zu Netzwerken/Anwendungen?

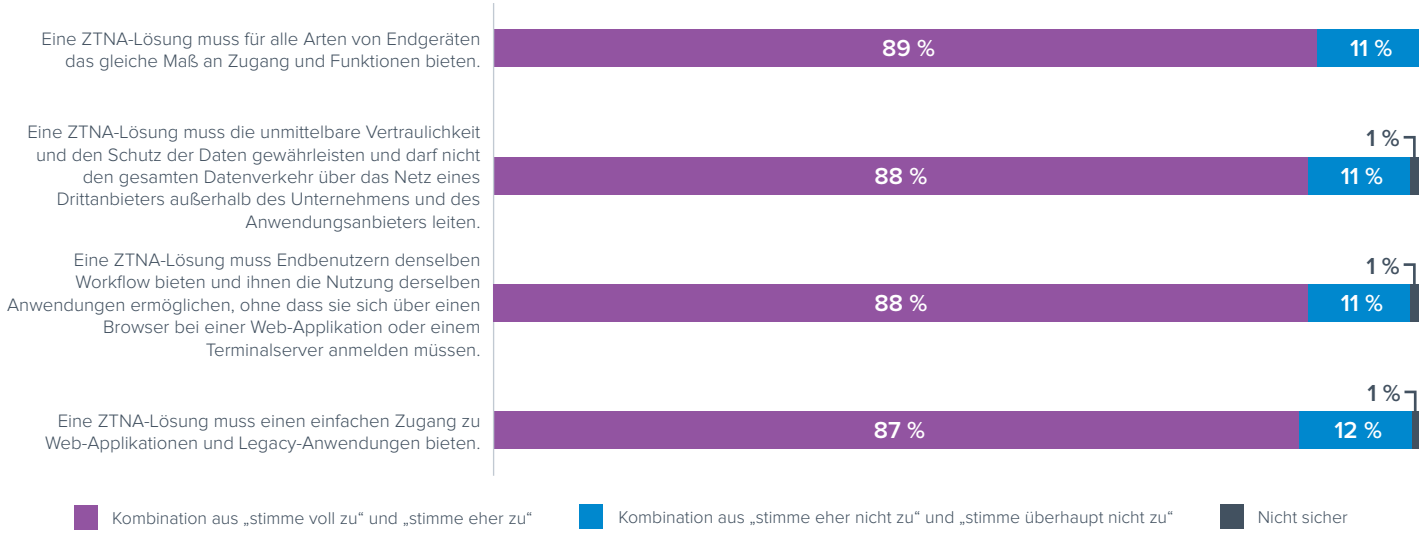
(n=750)



Die Mehrheit der befragten Unternehmen (78%) stellt firmeneigene Geräte für vorübergehende Auftragnehmer zur Verfügung, die vollen Netzwerkzugang benötigen. Eine gewisse Anzahl von Unternehmen verlangt ZTNA mit BYOD für den direkten Anwendungszugang. 21% geben firmeneigene Geräte aus und erlauben nur ZTNA-Zugang.

Stimmen Sie diesen Aussagen zu oder nicht zu?

(n=750)



Fast 90% der Befragten erwarten von ihrer ZTNA-Lösung:

- einen einfachen Zugang zu Web- und Legacy-Anwendungen (87%)
- die gleichen Funktionen für alle Endgeräte (88%)
- Unterstützung bestehender Workflows (88%
- vollständige Datenvertraulichkeit (88%)

Die Befragten mit Zero-Trust-Network-Access(ZTNA)-Technologie waren im Vergleich zu Unternehmen, die ZTNA noch nicht eingeführt haben, deutlich weniger von Netzwerksicherheitsverletzungen betroffen.
Von den Unternehmen, die im letzten Jahr von einer Netzwerksicherheitsverletzung betroffen waren, setzen 43 % ZTNA ein und 57 % nicht.

Fazit

Viele Unternehmen erleben aktuell eine hohe Anzahl an Netzwerkverletzungen und ihre Security-Risiken nehmen aufgrund ständig zunehmender Ransomware-Angriffe ein immer größeres Ausmaß an. Dass sich eine solche Situation entwickeln konnte, ist angesichts des pandemiebedingten Wechsels hin zum externen Arbeiten und der damit einhergehenden raschen Technologietransformation nicht überraschend.

Doch Unternehmen möchten auch zukünftig ihren Mitarbeitern die Arbeit im Homeoffice ermöglichen. Daher müssen IT-Abteilungen eine hybride Umgebung unterstützen, wenn sie sowohl für Mitarbeiter im Homeoffice als auch für die Kollegen im Büro optimale Arbeitsbedingungen ermöglichen möchten. Leider sind externe Mitarbeiter trotz Breitbandverbindungen und firmeneigener Geräte weiterhin mit IT-Problemen wie langsamen Anwendungen, abgebrochenen Telefonaten und schlechter Videoqualität konfrontiert. Diese Probleme der Benutzerfreundlichkeit sind eng mit dem Aspekt der Security verbunden: Unternehmen, die sich um die Lösung ihrer Security-Probleme bemühen, verbessern in der Regel auch die Benutzerfreundlichkeit ihrer Bereitstellungen.

Unternehmen werden sich daher heute zunehmend bewusst, dass sie durch die Migration ihrer SaaS-Anwendungen in die Public Cloud die Benutzerfreundlichkeit für ihre Mitarbeiter optimieren können. Um diese Cloud-Präsenz zu unterstützen und die Security zu verbessern, stehen ihnen neue Technologien zur Verfügung. Diese Secure-Access-Service-Edge(SASE)-Technologien umfassen Networking- und Security-Komponenten. Unternehmen berichten in diesem Sinne nun von bestehenden oder geplanten Investitionen in SD-WAN und Zero Trust Network Access, und um die Vorteile solcher SASE-Implementierungen voll auszuschöpfen, entscheiden sie sich für cloudnative SASE-Lösungen. Es gibt immer mehr Belege dafür, dass diese Investitionen Unternehmen helfen werden, sich besser an das neue Arbeitsmodell anzupassen.

Leider sind externe Mitarbeiter trotz Breitbandverbindungen und firmeneigener Geräte weiterhin mit IT-Problemen wie langsamen Anwendungen, abgebrochenen Telefonaten und schlechter Videoqualität konfrontiert. Diese Probleme der Benutzerfreundlichkeit sind eng mit dem Aspekt der Security verbunden: Unternehmen, die sich um die Lösung ihrer Security-Probleme bemühen, verbessern in der Regel auch die Benutzerfreundlichkeit ihrer Bereitstellungen.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Überzeugung, dass jedes Unternehmen Zugang zu Cloud-fähigen Sicherheitslösungen auf höchstem Niveau verdient, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen und anpassungsfähigen Lösungen, die mit den Unternehmen unserer Kunden wachsen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Somit können sie sich darauf konzentrieren, ihr Geschäft auf die nächste Stufe zu bringen.

Weitere Informationen finden Sie unter barracuda.com.

Barracuda®
Your journey, secured.