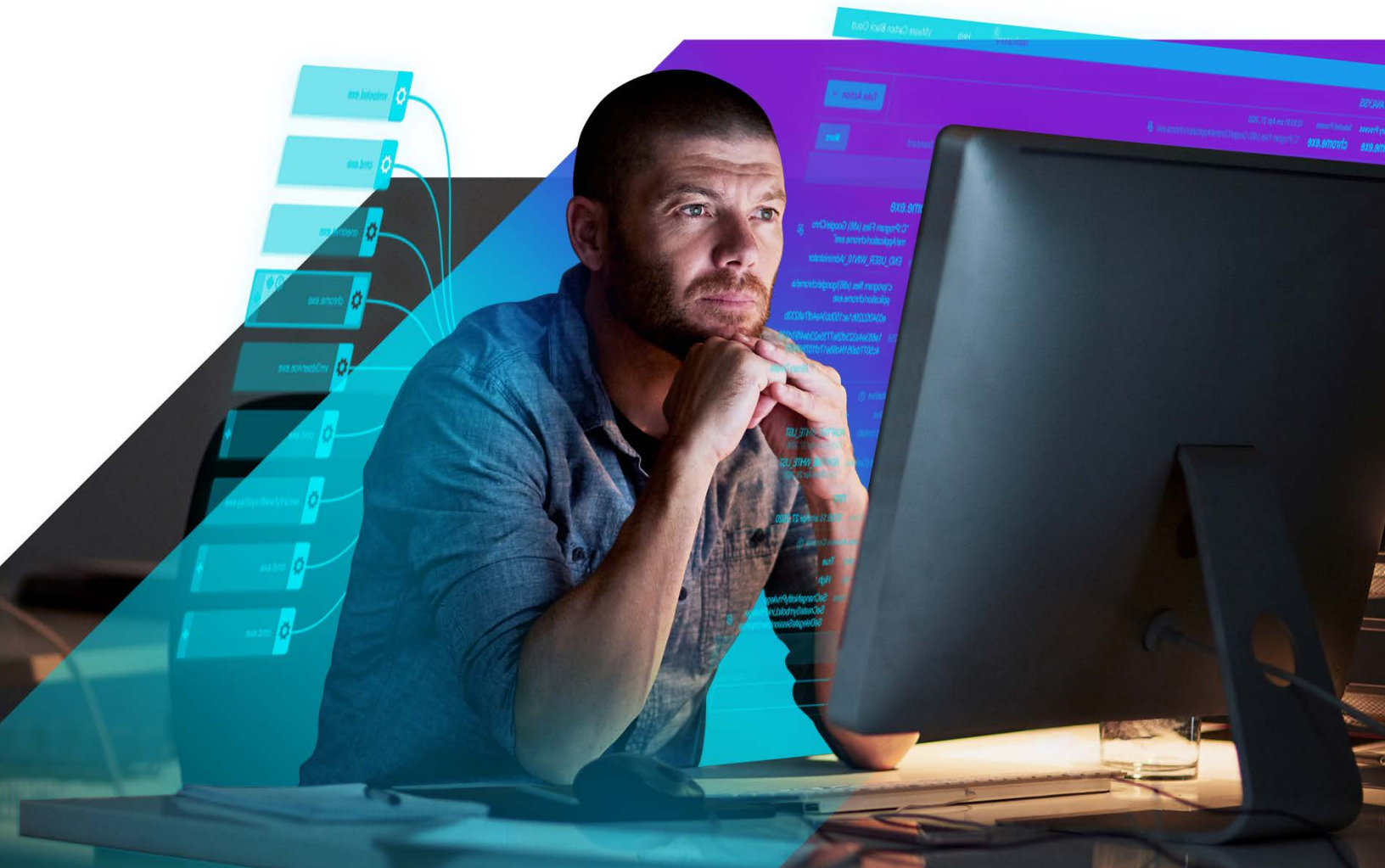
vmware®

Deutschland

VMware-Studie zur IT-Sicherheit in Deutschland

2021



Einführung

Diese Umfrage wurde durchgeführt, um die Herausforderungen und Probleme zu verstehen, mit denen deutsche Unternehmen im Zuge steigender Cyberangriffe konfrontiert sind. Sie identifiziert Trends bei Hacking- und böswilligen Angriffen und beleuchtet die finanziellen Folgen und Image-Auswirkungen, die Sicherheitsverletzungen in einem beispiellosen Jahr für Unternehmen gehabt haben. Sie untersucht die Pläne von Unternehmen in Deutschland zum Schutz neuer Technologien sowie der Einführung einer Cloud First-Sicherheitsstrategie und nimmt die Komplexität der gegenwärtigen Umgebung für die Verwaltung der Cybersicherheit unter die Lupe.

In diesem Report lesen Sie, wie Führungskräfte im Bereich der Cybersicherheit planen, sich auf die Sicherheitsherausforderungen des dezentralen Arbeitens einzustellen und Abwehrmaßnahmen zu entwickeln, um Sicherheit zum intrinsischen Bestandteil von Infrastruktur und Abläufen zu machen.

Kurzfassung:

Vorwort

ERKENNTNISSE AUS DER CYBERSICHERHEITS-LANDSCHAFT IN DEUTSCHLAND

Rick McElroy, Principal Cybersecurity Strategist des Geschäftsbereichs Security bei VMware

Alles ist anders ... und dennoch gleich.

Die Cybersicherheitsexperten, die zur vierten Ausgabe unseres Reports zur IT-Sicherheit in Deutschland beigetragen haben, sind heute in einer ganz anderen Position als bei Beantwortung der Umfrage in 2020. Nach einem Jahr, das den größten und schnellsten Wandel der Arbeitsformen in der Geschichte brachte, sind Sicherheitsteams nun für ein Ökosystem zuständig, das stärker verteilt und heterogener strukturiert ist als je zuvor.

Initiativen zur digitalen Transformation machten schnelle Fortschritte, denn die Angriffsfläche für Cyberattacken dehnte sich nun auch auf Wohnzimmer, Küchen, Heimnetzwerke und persönliche Geräte aus. Mitarbeiter im Homeoffice verhalten sich anders als Mitarbeiter im Büro und nutzen das Netzwerk zu ungewohnten Zeiten, um produktive Arbeit mit Familienaufgaben und Einhaltung der von der Regierung auferlegten Einschränkungen zu vereinbaren. Daher hat sich der Datenverkehr im Netzwerk grundlegend verändert. Zur Verteidigung müssen Überwachungssysteme und Warnschwellen den neuen Gegebenheiten angepasst werden, um Angreifern keine Gelegenheit zu bieten, die unregelmäßigen Arbeitsmuster als Deckmantel für Infiltrierungsversuche auszunutzen.

Vor diesem Hintergrund rapider Veränderung bleibt manches jedoch gleich: eine Branche, der auch COVID-19 nichts anhaben konnte, ist die Cyberkriminalität.

Angriffe erfolgen mit großer Häufigkeit und werden immer ausgefeilter: Sicherheitsverletzungen sind die unvermeidliche Folge.

Fast neun von zehn (89 %) der 252 Teilnehmer an unserer Umfrage gaben an, die Zahl der Angriffe, mit denen sie konfrontiert waren, habe im vergangenen Jahr zugenommen. 71 % von ihnen erklärten, die Angriffe hätten deshalb zugenommen, weil mehr Mitarbeiter von zu Hause arbeiten. 77 % gaben an, die Angriffe seien ausgereifter geworden.

CISOs können nicht in die Ecken sehen

Cyberangriffe haben zugenommen, aber der schnelle Umzug ins Homeoffice bedeutet, dass Unternehmen immer noch keinen Gesamtüberblick haben. Unberechenbares Mitarbeiterverhalten, persönliche Geräte und die Nutzung von Heimnetzwerken bedeuten weniger Transparenz und es kommt zu toten Winkeln und dunklen Ecken, in denen Angriffe unentdeckt bleiben. Die Folge:

71 %

erklärten, dass Angriffe aufgrund des Arbeitens von zu Hause zunehmen

2,02

Sicherheitsverletzungen im Durchschnitt je Unternehmen und Jahr

91 %

gaben an, eine erhebliche Sicherheitsverletzung erlitten zu haben

Das Ergebnis? Die Anzahl der Sicherheitsverletzungen ist signifikant. Teilnehmer, die einen Cyberangriff verzeichnet hatten, melden im Schnitt 2,02 Sicherheitsverletzungen pro Jahr. Dabei handelte es sich nicht um kleinere Zwischenfälle. In neun von zehn Fällen lag eine erhebliche Sicherheitsverletzung vor, die den Regulierungsbehörden gemeldet werden oder bei der ein Incident-Response-Team eingreifen musste.

Es ist offensichtlich, dass Sicherheitsteams unter Druck stehen, und man ist sich der Gefahr bewusst. 53 % der befragten CISOs in Deutschland fürchteten, dass ihr Unternehmen im kommenden Jahr eine erhebliche Sicherheitsverletzung verzeichnen wird.

53 % der CISOs befürchten im kommenden Jahr eine wesentliche Sicherheitsverletzung.

Ransomware, Phishing und Veraltete Sicherheitstechnologie sind die Wichtigsten Ursachen für Sicherheitsverletzungen

Auf die Frage nach den Ursachen der Sicherheitsverletzungen zeichneten die drei häufigsten Quellen ein Bild von externen Bedrohungen und internen Schwächen. Die häufigste Ursache war Ransomware, auf die 18 % der Sicherheitsverletzungen zurückzuführen waren, eng gefolgt von Phishing-Angriffen und veralteter Sicherheitstechnologie.

Die schnelle Umstellung auf das Arbeiten im Homeoffice machte Unternehmen anfällig, die ihre Sicherheitshygiene vernachlässigt und keine Mehrfaktor-Authentifizierung eingeführt hatten. Das Extended Enterprise steht ebenfalls unter zunehmender Spannung, da Drittanbieter bedeutende Sicherheitsrisiken mit sich bringen.

Wiederaufleben von Ransomware

Ransomware ist erneut zu einer der wichtigsten Ursachen von Sicherheitsverletzungen geworden, da Angreifer ausgefeilte und lukrative mehrstufige Attacken starten.

18 % **aller Sicherheitsverletzungen wurden durch Ransomware verursacht.**

Neben diesen Bedrohungen bringt die rapide Zunahme von Ransomware zusätzlich unerwünschte Anspannung. Mehrstufige Attacken, die Eindringen, Persistenz, Datendiebstahl und Erpressung umfassen, erhöhen den Druck, denn die Angreifer nutzen die Schwierigkeiten aus, mit denen Remote-Mitarbeiter konfrontiert sind. Bei den meisten Ransomware-Angriffen ist E-Mail weiterhin der am häufigsten genutzte Weg, auf dem sich die Angreifer Zugriff verschaffen.

Besorgnis um Entwicklung und Nutzung von Anwendungen

Anwendungen von Drittanbietern sind eine häufige Ursache von Sicherheitsverletzungen, so die von uns befragten CISOs. 63 % geben an, dass die Innovationsfähigkeit ihrer Unternehmen jedoch von solchen Anwendungen abhängt. Daher überrascht es nicht, dass Sicherheitsteams ein schärferes Augenmerk auf ihre Nutzung und Entwicklung richten.

Fast 63 % der Befragten stimmen zu[1], dass sie mehr Transparenz im Hinblick auf Daten und Anwendungen benötigen, um Angriffe zu verhindern, und ungefähr gleich viele sind der Meinung, dass bessere kontextbezogene Sicherheit erforderlich ist, um die Datensicherheit während des gesamten Lebenszyklus von Anwendungen zu verfolgen. Die Auswirkungen von COVID-19 werden erkannt, und 61,5 % stimmen zu, dass sie Sicherheit aufgrund der erweiterten Angriffsfläche anders betrachten müssen als in der Vergangenheit.

Anwendungen führten auch die Liste der Schwachstellen bei der Bewegung von Daten an, sind aber keineswegs der einzige Bereich, der Sorgen bereitet.

Bei der Wahrnehmung von Workloads als Schwachstelle ist ein signifikanter Anstieg zu verzeichnen.

[1] Zustimmung bezieht sich auf die Optionen „stimme voll und ganz zu“ und „stimme eher zu“ zusammen.

19 % der Befragten gaben an, dass Workloads die größte Schwachstelle bei der Bewegung von Daten in Ihrem Unternehmen seien, und merkten an, dass dies vor zwölf Monaten noch nicht der Fall war.

Weitere 3 % gaben an, dass Workloads schon seit über zwölf Monaten die größten Schwachstellen seien. Die Teams sind sich bewusst, dass herkömmlicher Virenschutz nicht in der Lage ist, Server-Workloads zu sichern, und Fehlkonfigurationen ein bedeutendes Sicherheitsrisiko darstellen. Das liegt oft an einer Wissensdifferenz zwischen Sicherheits- und Infrastrukturteams: Die Sicherheitsteams kennen das erwartete Verhalten von Produktions-Workloads nicht und die Infrastrukturteams haben keine Erfahrung darin, Angreiferverhalten zu erkennen. Dieses Jahr erwarten wir, dass Unternehmen sich mit diesen Wissenslücken befassen und die Abwehrmaßnahmen für Workloads in der Cloud stärken werden.

Zum Thema Cloud ergibt unsere Umfrage, dass sich ein unaufhaltsamer Wandel abzeichnet. Fast alle von uns befragten CISOs setzen bereits eine auf die Cloud ausgerichtete Sicherheitsstrategie um oder planen, dies demnächst zu tun. Dies ist eine beträchtliche Veränderung, die zeigt, dass Unternehmen ihre Sicherheits-Roadmap für die Cloud angesichts der Herausforderungen von COVID-19 schneller umsetzen. Auch wenn sie diesen Weg bereits eingeschlagen haben, preschen sie voran, weil sie wissen, dass umfassende Cloud First-Sicherheit in einer Cloud First-Welt unerlässlich ist.

Wir hoffen, dass unsere vierte **VMware-Studie zur IT-Sicherheit in Deutschland** für Sie aufschlussreich und informativ ist.

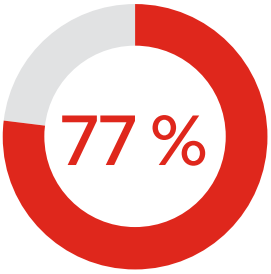
Wichtigste Ergebnisse

Häufigkeit der Angriffe und Sicherheitsrisiko sind weiterhin hoch

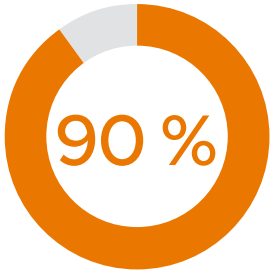
Angriffe erfolgen mit großer Häufigkeit und werden immer ausgefeilter: Sicherheitsverletzungen sind die unvermeidliche Folge.

89 % gaben an, dass die Zahl der Angriffe in den letzten zwölf Monaten zugenommen hat, und zwar um durchschnittlich 49 % in allen betroffenen Unternehmen insgesamt.

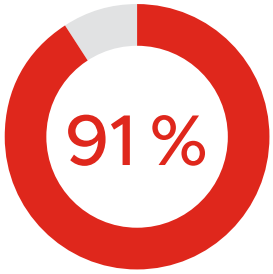
71 % derjenigen, die von einem Cyberangriff betroffen waren, erklärten die Zunahme damit, dass mehr Mitarbeiter im Homeoffice arbeiten.



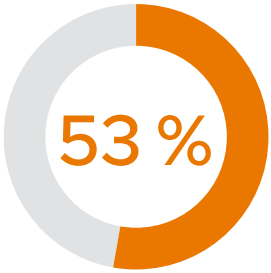
der von einem Cyberangriff Betroffenen gaben an, die Angriffe seien ausgereifter geworden.



haben in den letzten zwölf Monaten eine Sicherheitsverletzung erlitten und haben in diesem Zeitraum durchschnittlich 2,02 Vorfälle verzeichnet.



gaben an, die erlittenen Sicherheitsverletzungen seien erheblich gewesen.

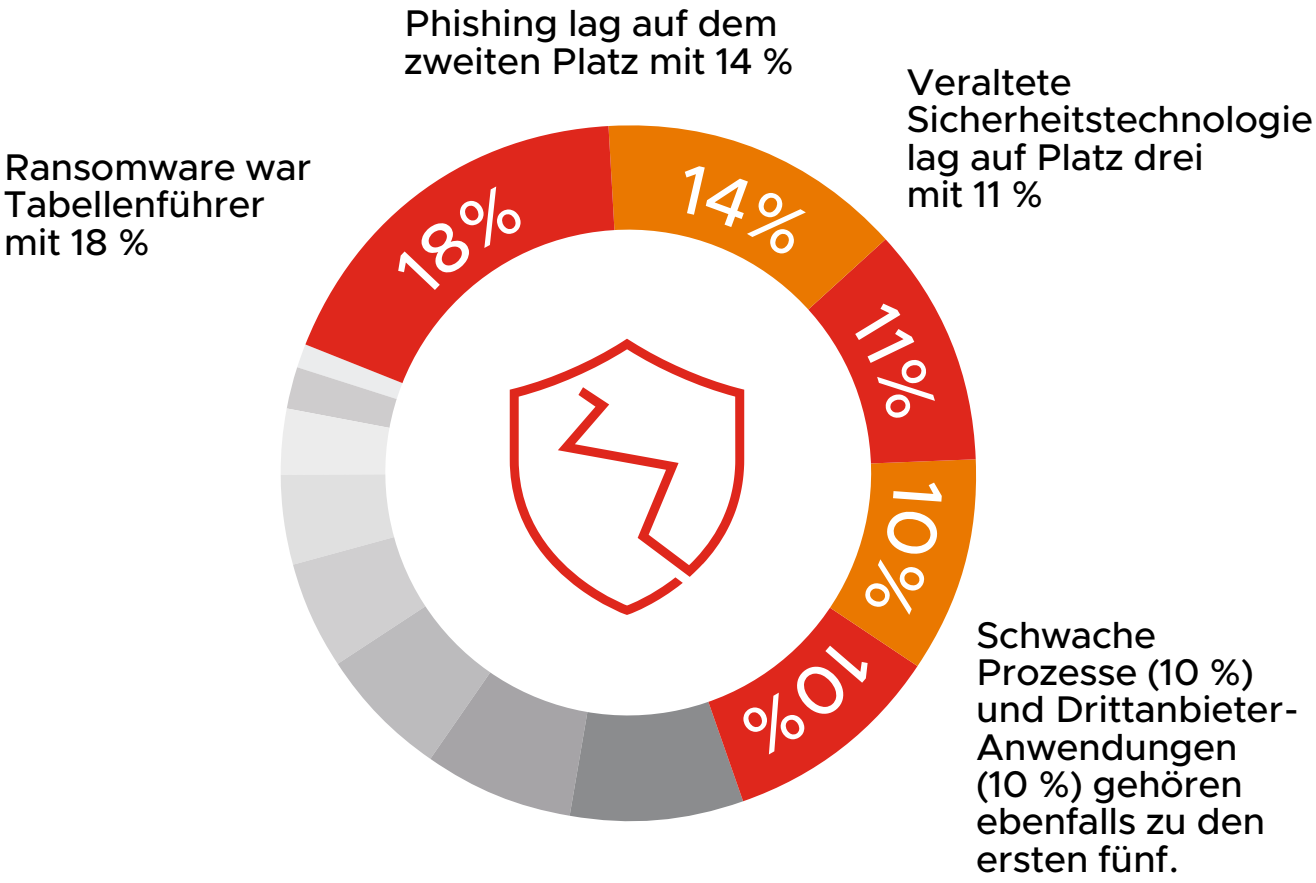


befürchten in den nächsten zwölf Monaten eine erhebliche Sicherheitsverletzung.

Ransomware, Phishing, veraltete Sicherheit, Anwendungen und Workloads führen die Liste der Befürchtungen von CISOs an

Die wichtigsten Quellen von Sicherheitsverletzungen ergeben ein Bild externer Bedrohungen und interner Schwächen.

Hauptursachen bei denjenigen, die einen Cyberangriff erlitten haben:



Anwendungen und Workloads führten die Liste der Schwachstellen bei der Bewegung von Daten an, aber sie sind keinesfalls der einzige Besorgnis erregende Bereich.

Ausdehnung der Angriffsflächen veranlasst Führungskräfte, ihren traditionellen Sicherheitsansatz zu überdenken

Erfreulicherweise wird erkannt, dass grundlegende Veränderungen in der Sicherheit für ein digitales Zeitalter erforderlich sind, das von hochgradiger Vernetzung und Unterstützung von Remote-Arbeit geprägt ist.

61,5 % Fast zwei Drittel (61,5 %) stimmen zu, dass sie Sicherheit anders betrachten müssen als in der Vergangenheit, da sich die Angriffsfläche ausgeweitet hat.

63 % stimmen zu, dass sie bessere kontextbasierte Sicherheit benötigen, um Daten während des gesamten Lebenszyklus verfolgen zu können.

63 % stimmen zu, dass sie mehr Transparenz im Hinblick auf Daten und Anwendungen benötigen, um Angriffen vorzubeugen.

Vereinfachung, Konsolidierung und Wechsel zu „Cloud First“ sind für 2021 geplant

Die befragten CISOs scheinen einen Weg der Technologiekonsolidierung und der Einführung eines stärker integrierten Sicherheitsansatzes zu gehen. 33 % geben an, dass sie ihr Sicherheitsbudget erhöhen, um diese Ziele zu erreichen.

44 % haben ihre Sicherheitstechnologie aktualisiert, um das Risiko zu mindern.

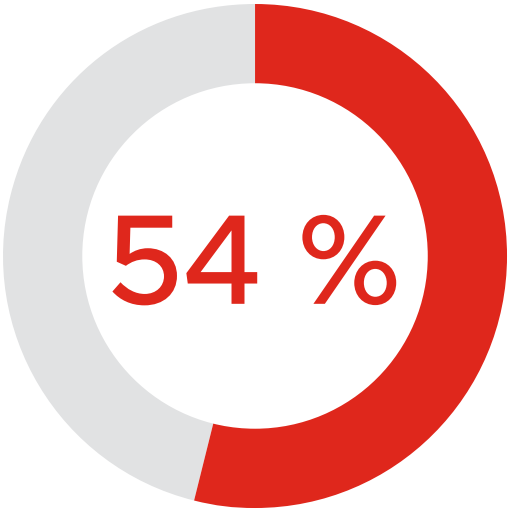
50 % integrieren mehr Sicherheit in ihre Infrastruktur und ihre Anwendungen und reduzieren die Anzahl der punktuellen Lösungen.

47 % haben ihre Sicherheitsrichtlinie und ihren Sicherheitsansatz aktualisiert, um das Risiko zu mindern.

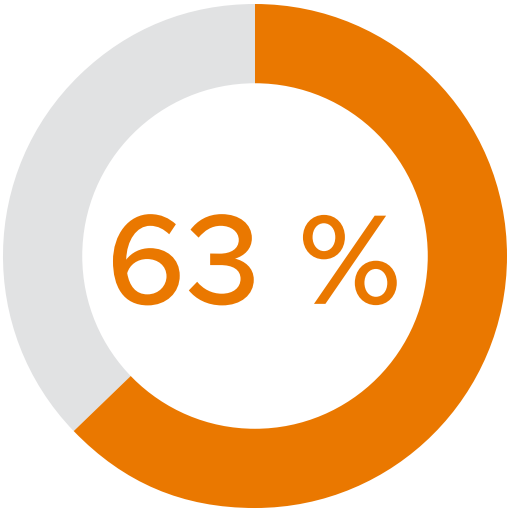
98 % haben sich auf eine Cloud First-Strategie verlegt oder planen dies.

KI ist das nächste Neuland für Geschäftsinnovationen – aber behindern Sicherheitsbedenken den Fortschritt?

Das nächste Neuland für Geschäftsinnovationen ist die künstliche Intelligenz, denn Unternehmen bemühen sich um einen Vorsprung bei der Entwicklung wettbewerbsfähiger Kundenservices und digitaler Erfahrungen.

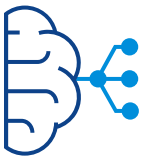


Dennoch stimmen 54 % der Teilnehmer in Deutschland zu, dass Sicherheitsbedenken sie davon abhalten, KI/ML-basierte Anwendungen zur Verbesserung dieser Services einzuführen.



Und 63 % der Befragten stimmen zu, dass ihre Innovationsfähigkeit davon abhängt, dass sie Anwendungen auf sichere Weise entwickeln und Mitarbeitern und Kunden zugänglich machen können.

KI ist das nächste Neuland für Geschäftsinnovationen – aber behindern Sicherheitsbedenken den Fortschritt?



Viele Umfrageteilnehmer sind besorgt, dass sie die digitale Chance nicht ergreifen können.

59 % stimmen zu, dass der Markt für Sicherheitslösungen zu viel Komplexität aufweist, was sie davon abhält, ihre Sicherheitsrichtlinie zu ändern, obwohl sie wissen, dass die derzeitige IT-Sicherheit nicht effektiv ist.

61 % stimmen zu, dass ihr Vorstands-/oberstes Führungsteam zunehmend besorgt ist, wenn sie Anwendungen/Services auf den Markt bringen, weil Datensicherheitsverletzungen/Angriffe eine wachsende Gefahr darstellen und zunehmend Schaden anrichten.

69 % stimmen zu, dass sie in ihren Anwendungen gern verstärkt auf KI/ML setzen würden, um Sicherheit und Services zu verbessern.

69 % stimmen zu, dass sie mehr Transparenz im Hinblick auf ihre Daten und Anwendungen benötigen, um Angriffen vorzubeugen.

Schutz von Marke und Image: Verlangt dies größere Veränderungsdringlichkeit?

Marke und Image sind nach wie vor der heilige Gral für Unternehmen und können sehr leicht Schaden nehmen. Die Auswirkungen von Sicherheitsverletzungen auf das Image sind jedoch größer als der finanzielle Schaden.

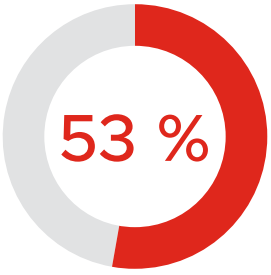
49 %

Fast die Hälfte (48,5 %) derjenigen, die einen Cyberangriff erlitten haben, gaben an, dass das Unternehmensimage auf irgendeine Weise beeinträchtigt wurde.

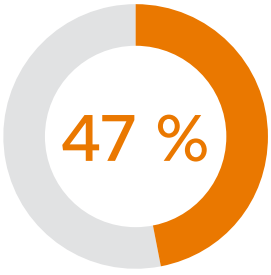
91 %

In den letzten zwölf Monaten mussten 91 % der Befragten Regierungsbehörden Meldung erstatten oder ein IR-Unternehmen beauftragen, um die Imageprobleme zu überwinden, die durch erhebliche Sicherheitsverletzungen entstanden sind.

Der Schweregrad dieser Sicherheitsverletzungen wird von den Befragten unterschiedlich bewertet und es zeigt sich trotz der wachsenden Bedrohung eine mangelnde Veränderungsdringlichkeit.



Nur 53 % befürchten, dass sie im kommenden Jahr eine erhebliche Sicherheitsverletzung erleiden werden.



Nur 47 % haben ihre Sicherheitsrichtlinie und ihren Sicherheitsansatz aktualisiert, um das Risiko zu mindern.

Vollständige Umfrageergebnisse

Haben Sie in den vergangenen zwölf Monaten eine Zunahme der Cyberangriffe auf Ihr Unternehmen festgestellt? Wenn ja, um wie viel?

89 % der befragten CISOs gaben an, sie hätten in den letzten zwölf Monaten eine zunehmende Anzahl von Cyberangriffen auf ihr Unternehmen erfahren, die im Durchschnitt 49 % betrug. Im Gesundheitswesen waren es 100 % der Befragten und hier wurden im Durchschnitt 55,5 % mehr Angriffe verzeichnet.

Teilnehmern aus dem Finanzdienstleistungssektor erging es besser als dem Durchschnitt, sie meldeten eine durchschnittliche Zunahme der Angriffe um 25 %.

Unternehmen mit 501-1.000 Mitarbeitern meldeten eine einen starken Anstieg der Angriffszahlen, die im Durchschnitt 56 % betrug.

Unternehmen mit 31- bis 40-köpfigen IT-Teams meldeten einen durchschnittlichen Anstieg der Angriffe um 56 %, während dieser im Gesamtdurschnitt 49 % betrug.

Hat sich die Anzahl der typischen Cyberangriffe auf Ihr System insgesamt verändert, seit mehr Mitarbeiter aufgrund der COVID-19-Pandemie im Homeoffice arbeiten?

71 % der Befragten, bei denen Cyberangriffe vorgekommen waren, gaben an, sie hätten eine vermehrte Häufigkeit beobachtet, weil mehr Mitarbeiter im Homeoffice arbeiten.

86 % der Befragten aus dem Gesundheitswesen beobachteten vermehrte Angriffe im Zusammenhang mit der Arbeit im Homeoffice. Die durchschnittliche Zunahme betrug hier 15,5 %. Im Finanzdienstleistungssektor verzeichneten 82 % einen Anstieg, der im Durchschnitt 17 % betrug.

Sind Cyberangriffe auf Ihr Unternehmen in den letzten zwölf Monaten ausgereifter oder weniger ausgereift geworden?

Zur Ausgereiftheit der Angriffe vermeldeten 77 % der befragten CISOs, bei denen ein Cyberangriff aufgetreten war, dass die Angriffe ausgereifter wurden. Dies ist geringfügig weniger als die 82 %, die im Report vom Juni 2020 eine wachsende Ausgereiftheit meldeten.

Bei mehr als einem Viertel (28 %) derjenigen, bei denen es einen Cyberangriff gab, sind die die Angriffe, mit denen sie konfrontiert sind, bedeutend oder mäßig ausgereifter geworden, was auf einen Kern von Akteuren hindeutet, die Angriffstechniken böswillig weiterentwickeln und verbessern.

Bei den Regierungsbehörden verzeichneten 36 % einen mäßigen oder bedeutenden Fortschritt in der Ausgereiftheit der Angriffe. Dagegen gaben im Finanzdienstleistungssektor 55 % an, die Angriffe seien nur geringfügig ausgereifter geworden.

Angreifer richten ihre ausgefeilteren Angriffe gegen größere Unternehmen, und hier behauptet ein höherer Anteil, dass die Angriffe bedeutend ausgereifter geworden sind. Das spiegelt die Tatsache wider, dass Menge und Wert von Daten mit der Größe der Unternehmen zunehmen und so bieten sich für Cyberkriminelle in größeren Unternehmen mehr Chancen, ihre Angriffe zu monetarisieren.

77 % der befragten CISOs vermeldeten, dass die Angriffe ausgereifter wurden.

Welche Art von Cyberangriff auf Ihr Unternehmen war in den letzten zwölf Monaten am häufigsten?

Die Angriffsumgebung in Deutschland ist vielfältig. Nur wenige Befragte verzeichnen die gleiche Art von Angriffen, und keine Angriffsart ragt bedeutend heraus. Das unterstreicht die Herausforderungen, vor denen CISOs in Deutschland stehen – sie müssen strategische und taktische Antworten auf einen außerordentlich vielfältigen Mix aus Angriffspunkten und -methoden entwickeln.

Ransomware-Angriffe stehen an der Spitze: Bei 18 % der Befragten, die Cyberangriffe erlitten hatten, waren diese am häufigsten. Dicht darauf folgen jedoch Angriffe über Google Drive (cloudbasierte Angriffe) und Anwendungen von Drittanbietern, die bei 11 % bzw. 10,5 % der Umfrageteilnehmer die häufigsten Angriffsarten waren.

Auf Angriffe mit Standard-Malware entfallen 9 % bei denjenigen, die Cyberangriffe erfahren haben. Im Bericht von Juli 2020 führten dateilose Angriffe wie Living-off-the-Land-, PowerShell und WMI-Angriffe in Deutschland die Tabelle an. Auf sie entfiel ein Fünftel (20 %) der Attacken.

Ransomware zielte überwiegend auf den Finanzdienstleistungssektor ab, hier waren solche Angriffe bei 26,5 % der Teilnehmer am häufigsten. Auch bei Befragten aus dem Gesundheitswesen (24 %) und dem öffentlichen Sektor (21 %) war ihre Zahl hoch.

Wie oft ist Ihr Unternehmen in den letzten zwölf Monaten einem Cyberangriff zum Opfer gefallen?

Neun von zehn der CISOs, die an unserer Umfrage teilnahmen, erklärten, ihr Unternehmen habe im vergangenen Jahr eine Sicherheitsverletzung infolge eines Cyberangriffs verzeichnet (90 %). Das sind mehr als die 73 %, die in der Studie vom Juni 2020 angaben, einer Sicherheitsverletzung zum Opfer gefallen zu sein.

90 % der befragten Unternehmen verzeichneten im vergangenen Jahr eine Sicherheitsverletzung.

Die durchschnittliche Anzahl der Sicherheitsverletzungen, die von jedem Unternehmen verzeichnet wurde, hat sich kaum verändert und lag im Juni 2020 sowie im April 2021 bei zwei.

In der Nahrungsmittel- und Getränkebranche ist die durchschnittliche Anzahl der Sicherheitsverletzungen mit 3,0 am höchsten, während die Vertreter des Finanzdienstleistungssektors nur 1,46 Vorfälle verzeichnen. Andere erwähnenswerte Branchen, in denen die Häufigkeit von Sicherheitsverletzungen über dem Durchschnitt liegt, sind Medien und Unterhaltung (3,67), Industrie und Technik (2,23), Behörden (2,19) und Professional Services (2,15).

Am häufigsten treten Sicherheitsverletzungen im mittelgroßen Unternehmen mit 1.001-2.000 Beschäftigten auf, wo es im Durchschnitt zu 2,97 Vorfällen pro Unternehmen kam.

Was war die häufigste Ursache von Sicherheitsverletzungen?

Für 18 % der befragten CISOs, bei denen ein Cyberangriff aufgetreten war, war Ransomware die Hauptangriffsart, gefolgt von Phishing (14 %). Die unerfreuliche Feststellung, dass ihre Sicherheitstechnologie veraltet war, hat bei 11 % ebenfalls zu Sicherheitsverletzungen geführt. Erschwerend kam hinzu, dass Prozesse nicht so wirksam waren wie erwartet (10 %) und Anwendungen von Drittanbietern Sicherheitsverletzungen verursachten (10 %). Durch die Belastung, die durch die plötzliche Umstellung auf das Homeoffice entstand, wurden eindeutig Bereiche exponiert, deren Richtlinien und Technologie nicht mit dem sich wandelnden Umfeld Schritt hielten.

Weiter unten auf der Liste standen Schwachstellen im Betriebssystem, auf die dennoch signifikante 8 % der Sicherheitsverletzungen zurückgeführt wurden. Die Verantwortung wurde jedoch nicht gänzlich dem Unternehmen zugeschrieben, denn 6 % der Vorfälle hatten ihren Ursprung in der Lieferkette und weitere 4 % waren die Folge von Island Hopping. Auch hier unterstreicht die Vielfalt der Ursachen die zahlreichen Fronten, an denen CISOs in Deutschland ihre Unternehmen verteidigen müssen.

Ransomware war insbesondere bei Finanzdienstleistern ein Problem, wo sie für mehr als ein Drittel (37 %) verantwortlich war, und auch im Gesundheitswesen, wo sie von fast einem Drittel (32 %) als primäre Ursache genannt wurde. Das Gesundheitswesen war auch besonders anfällig für Phishing-Angriffe (20 %), während Regierungsbehörden einen hohen Anteil von Angriffen über Drittanbieter-Anwendungen (21 %) verzeichneten.

Unternehmen mit 501-1.000 Beschäftigten waren besonders anfällig für Angriffe durch Ransomware. Hier wurden 25,5 % der Sicherheitsverletzungen auf diese Weise verursacht. Und Unternehmen mit 41- bis 50-köpfigen IT-Teams verzeichneten ebenfalls einen hohen Anteil an Ransomware-Angriffen (25 %).

Welcher Anteil der Sicherheitsverletzungen durch Cyberangriffe in den letzten zwölf Monaten entfiel Ihrer Meinung nach auf erhebliche Sicherheitsverletzungen, d.h. solche, die Sie Regulierungsbehörden melden oder einem Incident-Response-Team übergeben mussten o.ä.?

Sicherheitsverletzungen sind schwerwiegende Vorfälle. Die meisten (91 %) der Befragten mussten Regulierungsbehörden Meldung erstatten oder ein IR-Unternehmen beauftragen, um die von den Sicherheitsverletzungen verursachten Probleme zu überwinden.

Über ein Viertel (30 %) der Teilnehmer, die einen Cyberangriff erlitten hatten, gaben an, dass 21-30 % der Vorfälle erhebliche Sicherheitsverletzungen waren, weitere 24 % erklärten 31-40 % der Vorfälle für erheblich.

91 % der Unternehmen erlitten eine wesentliche Sicherheitsverletzung.

Im Finanzdienstleistungssektor war der mittlere Durchschnitt der erheblichen Sicherheitsverletzungen mit 17,46 % niedrig im Vergleich zum Gesamtdurchschnitt von 24,09 %, bei den Behörden lag er jedoch mit 28,33 % relativ hoch. Weitere 39 % der Befragten aus Behörden gaben an, dass 21-30 % wesentliche Sicherheitsverletzungen gewesen seien.

Umfrageteilnehmer mit 41- bis 50-köpfigen IT-Teams meldeten den höchsten Durchschnitt (26,10) aller Gruppen.

Welche finanziellen und Imagefolgen hatten diese Sicherheitsverletzungen für Ihr Unternehmen?

Knapp über ein Sechstel (18 %) der Teilnehmer, die einen Cyberangriff erlitten hatten, erklärten, ihr Unternehmen habe negative finanzielle Folgen durch eine Sicherheitsverletzung erlitten. Dies liegt unter dem globalen Durchschnitt von 24 % und stellt einen Rückgang gegenüber den 26 % dar, die laut Umfrage von Juni 2020 finanzielle Folgen erlitten haben.

Der Anteil derjenigen, die **keine** finanziellen Folgen durch eine Sicherheitsverletzung meldeten, ist ebenfalls gefallen, von 60,5 % im Juni 2020 auf 52 % in dieser Studie.

Bei Finanzdienstleistern und Organisationen im Gesundheitswesen war der Anteil derjenigen, die keine finanziellen Folgen erlitten hatten, mit 78 % bzw. 70 % am höchsten

Insgesamt waren die Imageauswirkungen geringer als zuvor. Nur 48,5 % der Befragten, bei denen ein Cyberangriff aufgetreten war, erklärten, ihr Markenimage sei dadurch beeinträchtigt worden, ein Rückgang gegenüber den 64 % im Report vom Juni 2020. 16 % erklärten, der Schaden sei schwerwiegend oder mäßig gewesen.

41 % gaben an, sie hätten durch die aufgetretenen Sicherheitsverletzungen keinen Imageschaden erlitten.

Fast die Hälfte (49 %) der Teilnehmer aus Behörden gaben an, das Image sei nicht beeinträchtigt worden.

Wie stark fürchten Sie die erheblichen Sicherheitsverletzungen, die Sie in Ihrem Unternehmen innerhalb der nächsten zwölf Monate erwarten?

Mit dem Potenzial für erhebliche Sicherheitsverletzungen im kommenden Jahr ist ein signifikanter Angstfaktor verbunden. Mehr als die Hälfte (53 %) haben große oder etwas Angst, dass ihr Unternehmen eine Sicherheitsverletzung erleiden wird.

Der Behörden- und der Finanzdienstleistungssektor waren sehr besorgt. Hier gaben 55 % bzw. 54 % der Teilnehmer an, dass sie einen Vorfall befürchteten. Dagegen machen sich nur 44 % der Befragten aus dem Gesundheitswesen Sorgen über eine Sicherheitsverletzung.

Wie begegnen Sie der Wahrscheinlichkeit von Sicherheitsverletzungen, sofern Sie überhaupt etwas unternehmen? [Die Teilnehmer konnten mehrere Optionen auswählen, gekennzeichnet durch Fettschrift]

Auf die Frage nach Ihren Plänen zur Verminderung des Risikos von Sicherheitsverletzungen lag für die Befragten die Priorität auf Vereinfachung und Konsolidierung der Sicherheitslösungen und darauf, Sicherheit zu integrieren. Ebenfalls wichtig waren die Aktualisierung von Technologie und Richtlinien sowie die Bereitstellung von Mitteln für das Problem.

> 50 % planen die Integration von mehr Sicherheit in ihre Infrastruktur und Apps und die Reduzierung der Anzahl punktueller Lösungen.

50 % der Befragten erklärten, sie planten die **Integration von mehr Sicherheit in ihre Infrastruktur und Anwendungen sowie die Reduzierung der Anzahl punktueller Lösungen**. Dies stieg auf 57 % in Industrie und Technik.

42,5 % gaben an, sie hätten **eine Anpassung der Sicherheit zur Minderung des Risikos** unter Einsatz vorhandener Ressourcen vorgenommen. Insbesondere bei Unternehmen im Gesundheitswesen ist es wahrscheinlicher als bei anderen, dass sie eine Anpassung der Technologie erwägen (58 %). 44 % gaben an, sie hätten **ihre Sicherheitstechnologie aktualisiert, um das Risiko zu mindern**.

47 % erklärten, sie **hätten ihre Sicherheitsrichtlinien aktualisiert, um das Risiko zu mindern** – eine wichtige Taktik angesichts der signifikanten Veränderungen in der Sicherheitslandschaft im vergangenen Jahr. 63 % der Unternehmen in Industrie und Technik verfolgen diesen Ansatz.

33 % haben ihr **Sicherheitsbudget erhöht**. Bei Behörden (40 %) und Finanzdienstleistern (49 %) war die Wahrscheinlichkeit geplanter Budgeterhöhungen am größten.

Interessant ist, dass Unternehmen der Strategie eine größere Bedeutung zumessen als der Behebung des Problems mit finanziellen Mitteln: Die Erhöhung des Budgets hatte insgesamt eine niedrigere Priorität als andere Bereiche.

Inwieweit stimmen Sie den folgenden Aussagen zu Entwicklung und Nutzung von Anwendungen in Ihrem Unternehmen zu oder nicht zu?

Auf die Frage nach der Veränderung der Einstellung zu Sicherheitsherausforderungen im Zusammenhang mit Anwendungsentwicklung und -nutzung in ihrem Unternehmen gaben die Befragten einen Einblick in die Probleme, vor denen sie stehen.

Transparenz ist zweifellos ein wichtiger Punkt. 63 % stimmen zu, dass sie eine **bessere Sicht auf ihre Daten und Anwendungen benötigen, um Angriffen vorzubeugen**. Im Gesundheitswesen steigt diese Zahl auf 72 %, wobei 34 % der Befragten voll und ganz zustimmen.

> 63 % benötigen eine bessere Sicht auf ihre Daten und Apps

61,5 % der Befragten in Deutschland waren der Meinung, dass die von COVID-19 geschaffene Angriffslandschaft ein Umdenken in Sicherheitsfragen erfordert, und stimmten zu, dass **sie Sicherheit anders betrachten müssen als zuvor, da sich die Angriffsfläche ausgeweitet hat**.

> 63 % stimmen zu, dass sie bessere kontextuelle Sicherheit benötigen, um Daten/ Sicherheit während des gesamten Lebenszyklus verfolgen zu können.

63 % stimmen zu, dass sie **bessere, kontextbezogene Sicherheit benötigen, um Daten/Sicherheit während des gesamten Lebenszyklus verfolgen zu können**. Dies weist auf eine aktuelle Umgebung hin, in der Sicherheit vorwiegend bedrohungszentriert und reaktiv ist. IT-Führungskräfte erkennen nun, dass dynamische Umgebungen einen kontextzentrierten Ansatz erfordern.

Die befragten CISOs in Deutschland machen sich keine Illusionen über die geschäftskritische Bedeutung der Anwendungssicherheit für ihr Unternehmen. 63 % stimmten zu, dass ihre **Innovationsfähigkeit als Unternehmen von ihrer Fähigkeit abhängt, Anwendungen sicherer zu entwickeln, zu verwalten und zu verteilen**.

67 % der Befragten **haben bei der Markteinführung neuer Anwendungen keine Bedenken, weil sie wissen, dass sie sicher sein werden**.

Auf die Frage nach ihrer Meinung zu KI bei der Entwicklung sicherer Anwendungen zeigte sich bei den Befragten ein gewisser Zwiespalt. 54 % stimmen zu, **dass Sicherheitsbedenken sie davon abhalten, auf künstlicher Intelligenz bzw. maschinellem Lernen basierende Anwendungen zur Verbesserung von Services einzuführen**, doch 69 % stimmen zu, dass sie **in ihren Anwendungen gern verstärkt auf KI und maschinelles Lernen setzen würden, um Sicherheit und Services zu verbessern**.

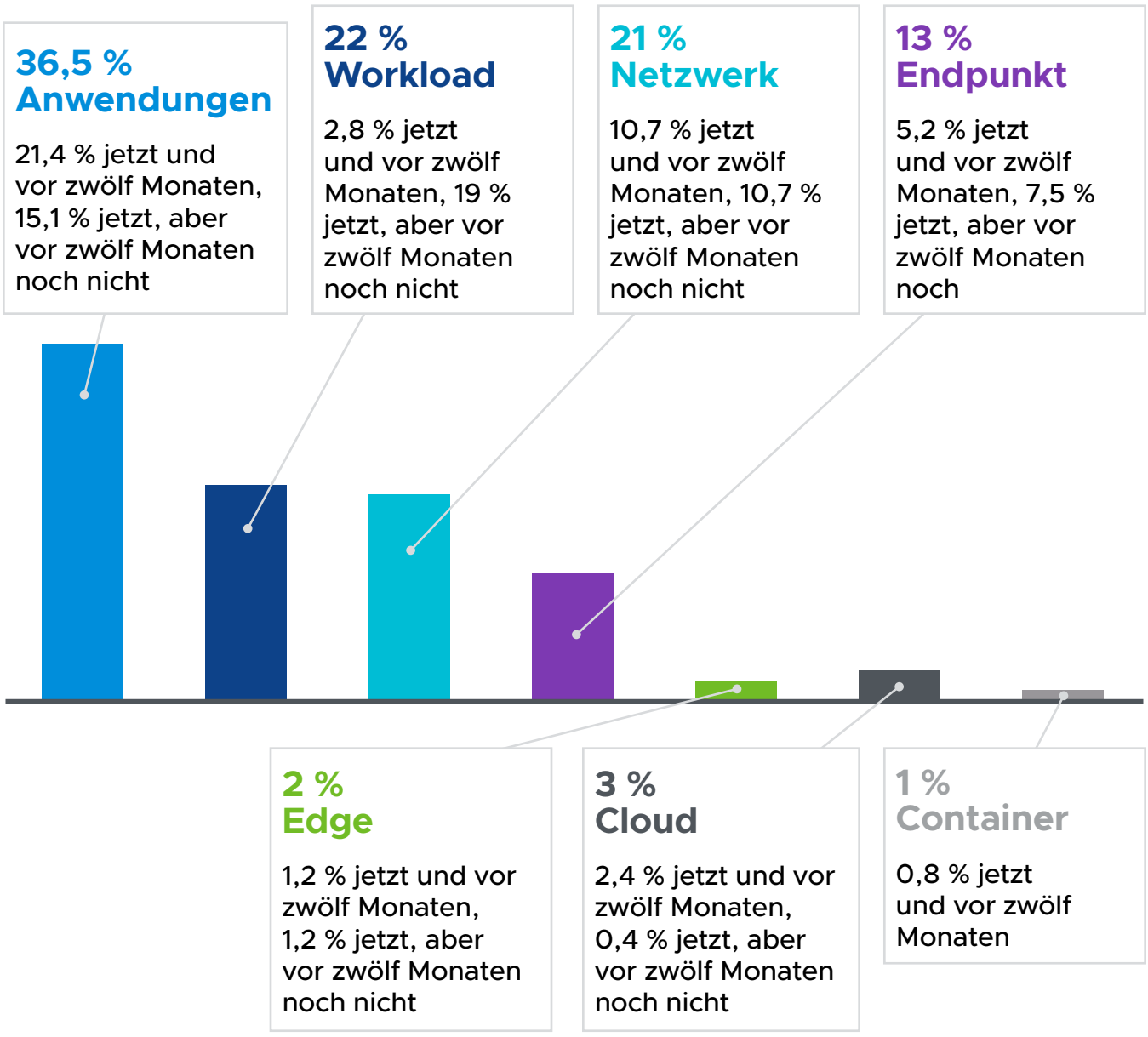
Mehr als die Hälfte der Befragten (59 %) stimmten zu, dass **der Markt für Sicherheitslösungen zu viel Komplexität aufweist, was sie davon abhält, ihre Sicherheitsrichtlinie zu ändern, obwohl sie wissen, dass die derzeitige IT-Sicherheit nicht effektiv ist**. Das legt nahe, dass Anbieter daran arbeiten müssen, ihre Angebote zu vereinheitlichen.

Und schließlich stimmten 61 % zu, dass der Anwendungssicherheit auf Geschäftsleitungsebene Aufmerksamkeit zukommt, und dass ihr **Vorstands-/oberstes Führungsteam zunehmend besorgt ist, wenn sie neue Anwendungen auf den Markt bringen, weil die Bedrohungen zunehmen und Datensicherheitsverletzungen immer größeren Schaden anrichten**.

> 61 % stimmen zu, dass ihre Geschäftsleitung zunehmend um die Sicherheitsrisiken bei der Markteinführung neuer Apps besorgt ist.

Welches ist Ihrer Meinung nach die größte Schwachstelle bei der Bewegung von Daten in Ihrer Sicherheitsinfrastruktur und hat sich das in den letzten zwölf Monaten verändert?

Anwendungen wurden als größte Schwachstelle bei der Datenbewegung genannt und es wird deutlich, dass dieser Aspekt schon seit einiger Zeit Besorgnis erregt. Besonders interessant ist die signifikante Zunahme der Einschätzung, dass Workloads eine Quelle von Schwachstellen sind. Es ist wahrscheinlich, dass Unternehmen sich im kommenden Jahr stärker darauf konzentrieren werden, dieses Risiko einzudämmen.



Wie haben Unternehmen die Umstellung auf das Homeoffice bewältigt?

Wir haben die teilnehmenden CISOs gebeten, ihren Erfolg bei der Umstellung der Belegschaft auf die Arbeit vorwiegend im Homeoffice zu bewerten, und gefragt, ob ein Ansatz mit Sicherheit als oberster Priorität zu einer effektiveren Umstellung beigetragen hätte.

71 % stimmen zu, dass sie in der Lage sind, ihren Mitarbeitern die Arbeit im Homeoffice zu ermöglichen, und dass Sicherheit kein Hindernis ist. Das unterstreicht die Arbeit der Sicherheitsteams, die mehr denn je eine zentrale Rolle in den Betrieben spielen. Gesundheitswesen und Finanzdienstleistungssektor haben sich gut geschlagen. Hier stimmten 80 % bzw. 78 % der Befragten zu, dass es bei der Ermöglichung der Arbeit im Homeoffice keinerlei Sicherheitsbarrieren gab. Dagegen meldete in Behörden ein höherer Anteil der CISOs Schwierigkeiten und 22 % waren nicht der Meinung, dass sie ihren Mitarbeitern die Arbeit im Homeoffice problemlos ermöglichen konnten.

Die Befragten räumen ein, dass es immer Verbesserungsmöglichkeiten gibt, und 70 % stimmen zu, dass es ihnen mit einem sicherheitszentrierten Ansatz besser gelungen wäre, Mitarbeitern die Arbeit an alternativen Orten ohne Beeinträchtigung der Produktivität zu ermöglichen. Das stimmte mit den Ergebnissen einer vorangegangenen VMware-Studie überein, die ergab, dass für IT-Fachkräfte das größte Problem bei der Umstellung auf Homeoffice darin lag, dass sie keine Multi-Faktor-Authentifizierung implementieren konnten. Inzwischen sind Sicherheitsfragen stärker in den Vordergrund getreten und es dürfte für CISOs einfacher sein, die Unterstützung der Geschäftsleitung für einen Ansatz zu gewinnen, bei dem Sicherheit an erster Stelle steht.

Verfolgen oder planen Sie eine Cloud First-Strategie?

Fast alle Befragten gaben an, dass sie den Wechsel zu einer Cloud First-Strategie planen – und wo er nicht sofort erfolgt, ist er fest eingeplant.

Insgesamt 58 % geben an, dass sie schon seit über einem Jahr eine Cloud First-Strategie verfolgen, 29 % seit weniger als zwölf Monaten. Weitere 12 % planen die Einführung einer Cloud First-Strategie innerhalb des kommenden Jahres oder zu einem späteren Zeitpunkt.

98 % verfolgen bereits einen Cloud First-Ansatz zum Schutz des Unternehmens oder planen dies.

Weit verbreitet ist Cloud First bei den Finanzdienstleistern, bei denen 71 % seit mehr als zwölf Monaten und 22 % seit weniger als zwölf Monaten den Cloud First-Grundsatz verfolgen. Auch im Gesundheitswesen verfolgen 70 % ähnlich lange einen Cloud First-Ansatz. Dagegen setzen 40 % der Befragten aus Behörden seit weniger als einem Jahr eine Cloud First-Sicherheitsstrategie um.

Wichtige Erkenntnisse Und Maßnahmen

Unsere vierte Studie zur IT-Sicherheit in Deutschland hat ergeben, dass leitende Cybersicherheits-Fachleute und die Unternehmen, für die sie arbeiten, weiterhin mit einer großen Anzahl von ausgefeilten Bedrohungen konfrontiert sind. Diese Situation wird durch die Umstellung auf dezentrales Arbeiten noch erschwert. Zwar haben die meisten Unternehmen den Übergang zum Homeoffice erfolgreich vollzogen, CISOs räumen jedoch ein, dass dies mit einem Ansatz, bei dem Sicherheit an erster Stelle steht, einfacher gewesen wäre.

Zweifellos hat COVID-19 eine signifikante Veränderung des Cybersicherheits-Umfelds mit sich gebracht und wird auch weiterhin Einfluss auf die Sicherheitsstrategie haben. So muss sich die Cybersicherheitsbranche darauf konzentrieren, Lösungen anzubieten, welche die betriebliche Komplexität reduzieren und dabei belastbaren Schutz für verteilte Arbeitsumgebungen bieten, die für die meisten Unternehmen in der Zukunft die Standardsituation darstellen werden.

Eine Analyse der Antworten zeigt wichtige Bereiche auf, denen sich Cybersicherheitsteams im kommenden Jahr zuwenden müssen:

Bessere Transparenz priorisieren

Der schnelle Wechsel zum Homeoffice hat für Unternehmen zu einem Transparenzproblem geführt. Das wahre Ausmaß der Angriffe lässt sich nur schwer feststellen, denn die Abwehr kann nicht in alle Ecken sehen, in denen persönliche mobile Geräte und Heimnetzwerke auf das Ökosystem des Unternehmens aufgepfropft werden. Rechnet man die Herausforderungen hinzu, die sich durch Drittanbieter-Anwendungen und unternehmensfremde Anbieter stellen, erhöht sich die Zahl der toten Winkel.

Denn Abwehrteams wissen einfach nicht, was sie nicht wissen, und folglich sind Unternehmen anfällig. Diese begrenzte Sichtbarkeit der Risiken in einem komplexen Gefüge macht es Sicherheitsteams sehr schwer, die erweiterte Angriffsfläche zu schützen. Unternehmen müssen der Verbesserung der Sichtbarkeit aller Endpunkte und Workloads hohe Priorität zumessen, um die Remote-Arbeitsumgebung zu schützen. Robuste situationsbezogene Erkenntnisse, die es erlauben, Bedrohungen im Zusammenhang zu sehen, helfen Abwehrteams, Risiken richtig zu erkennen und ihnen zu begegnen.

Das Wiederaufleben von Ransomware bekämpfen

Cyberangriffe werden immer ausgereifter und das gilt auch für Ransomware. Angreifer verschaffen sich unbemerkt Zugang zu Netzwerken, exfiltrieren Daten und finden Hintertüren, bevor sie Lösegeldforderungen stellen und/oder gestohlene Daten direkt monetarisieren. Um nicht Opfer wiederholter Angriffe zu werden, müssen Unternehmen hochentwickelten Schutz vor Ransomware mit robusten Gegenmaßnahmen nach Angriffen kombinieren, damit sie erkennen, ob weiterhin Gegenspieler in ihrer Umgebung präsent sind.

Ineffektiver, veralteter Sicherheitstechnologie und Prozessschwäche weiterhin entgegenwirken

Durch veraltete Sicherheitstechnologie und -prozesse bedingte Schwachstellen stellen weiterhin ein signifikantes Risiko für Unternehmen dar und durch die Umstellung auf Homeoffice sind sie noch anfälliger geworden. Beim Übergang von der Sofortreaktionsphase zur Betrachtung der längerfristigen Zukunft müssen Unternehmen die wichtigen Veränderungen an Prozessen und Technologie ermitteln, die erforderlich sind, um Remote- und Hybrid-Mitarbeitern sicheres Arbeiten zu ermöglichen und Risiken zu reduzieren.

Sicherheit als verteilten Service bereitstellen

Die Zeit ist vorbei, in der Sicherheitsteams Desktop-Computer des Unternehmens für Mitarbeiter in Firmenräumen schützten, die mit Unternehmensanwendungen auf Servern in einem unternehmenseigenen Rechenzentrum verbunden waren. Heute ist die Lage komplexer. Remote-Mitarbeiter verbinden sich mit Anwendungen auf einer Infrastruktur, die nicht unbedingt im Besitz des Unternehmens ist oder von ihm verwaltet und kontrolliert wird. Angesichts der neuen Oberflächen und unterschiedlichen Umgebungen, die es zu verteidigen gilt, kann Sicherheit nicht mehr in einer Abfolge von punktuellen Produkten und Drosselstellen im Netzwerk bestehen. Stattdessen müssen Endpunkt- und Netzwerkkontrollen als verteilter Service umgesetzt werden. Das heißt, die Sicherheit muss den zu schützenden Assets folgen, ganz unabhängig von der Art der vorhandenen Umgebung.

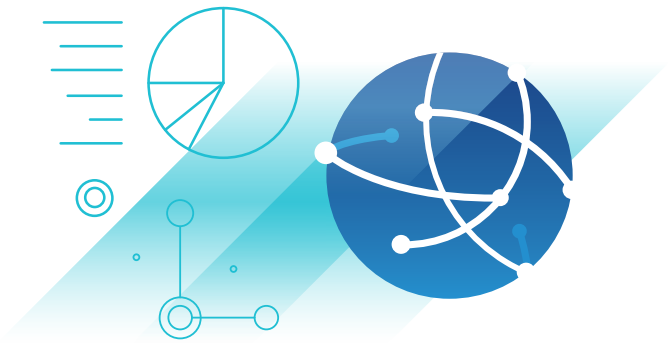
Integrierten Ansatz der Cloud First-Sicherheit verfolgen

Die größte Veränderung, die wir in unserer Studie aufgedeckt haben, ist der Übergang zu einer Cloud First-Sicherheitsstrategie. Das Ausmaß dieser Veränderung, die in so kurzer Zeit vonstatten ging, ist kaum zu überschätzen. Vor 2020 beschrieben nur wenige CISOs ihre Sicherheitsstrategie als „Cloud First“. Die Veränderung ist eine logische Folge davon, dass Unternehmen auf die aufgrund von COVID-19 plötzlich stark verteilte Arbeitsweise reagieren müssen.

Aber der Umstieg in die Cloud ist kein Allheilmittel für die Sicherheit. Nicht alle Clouds sind gleich und Kontrollen müssen von den Nutzerorganisationen überprüft werden, denn für groß angelegte Angriffe ist die Cloud ideal. Angesichts dieser dynamischen Veränderung sind Investitionen in die Sicherheit der Public Cloud von kritischer Bedeutung. Der Umstieg in eine Public Cloud ist ein Umstieg in eine sehr raue Umgebung, wo die Sicherheit nicht nur von Ihren eigenen Maßnahmen, sondern auch von denen Ihrer Nachbarn abhängt. Auch wenn Sie Ihre eigenen Ressourcen schützen können, haben Sie keine Kontrolle über die anderen, die diese Umgebung mit Ihnen teilen. Und solange die große Wanderung in die Cloud anhält, müssen Unternehmen dem Schutz von Cloud-Workloads an jedem Punkt des Sicherheits-Lebenszyklus höchste Priorität einräumen.

Die VMware-Studie zur IT-Sicherheit in Deutschland 2021 zeigt eine Branche, die sich darauf konzentriert, auf den Erfolgen des vergangenen Jahres aufzubauen und sich auf die sich wandelnde Bedrohungslandschaft einzustellen. CISOs haben eine recht genaue Vorstellung davon, welchen Kurs sie einschlagen und welche Tools sie einsetzen müssen, um Angreifern immer einen Schritt voraus zu sein.

Methodik



VMware beauftragte das unabhängige Marktforschungsunternehmen Opinion Matters mit einer Umfrage, die im Dezember 2020 durchgeführt wurde. Befragt wurden **252 CIOs, CTOs und CISOs** in Unternehmen aus verschiedenen Branchen in Deutschland, darunter Finanzdienstleistungen, Gesundheitswesen, Regierungs- und Kommunalbehörden, Einzelhandel, Industrie und Technik, Nahrungsmittel und Getränke, Versorgungsunternehmen, Professional Services sowie Medien und Unterhaltung. Diese vierte Studie von VMware zur IT-Sicherheit in Deutschland baut auf der vorangegangenen Umfrage vom Juni 2020 auf. Sie ist Bestandteil eines globalen Marktforschungsprojekts, das 14 Länder und Regionen umfasst: Australien, Kanada, Saudi-Arabien, Naher Osten, Vereinigtes Königreich, Frankreich, Deutschland, Spanien, Niederlande, Nordische Länder, Italien, Japan, Singapur und die Vereinigten Staaten.

Über VMware

VMware-Software bildet die Grundlage von komplexen digitalen Infrastrukturen weltweit. Mit einem vielfältigen Angebot in den Bereichen Cloud, Anwendungsmodernisierung, Networking, Sicherheit und digitaler Arbeitsplatz unterstützt das Unternehmen Kunden dabei, beliebige Anwendungen in jeder Cloud und auf jedem Gerät bereitzustellen. VMware hat seinen Hauptsitz in Palo Alto (Kalifornien) und setzt sich konsequent dafür ein, Gutes zu bewirken – mit wegweisenden technologischen Innovationen und globaler Reichweite. Weitere Informationen finden Sie auf vmware.com/de/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com