techconsult
TECHNOLOGY MARKET ANALYSTS

EIN UNTERNEHMEN DER heise group

Sicherer Datentransfer

Daten mit sicheren Kommunikations-lösungen schützen

Unterstützt durch

FTAPI

Informationen zur Studie

Erstellung durch

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

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

Erscheinungsjahr

2024

Autor

Raphael Napieralski

techconsult
TECHNOLOGY MARKET ANALYSTS
EIN UNTERNEHMEN DER heise group

In Zusammenarbeit mit

FTAPI

Kontakt

FTAPI Software GmbH
Steinerstr. 15f
81369 München
Deutschland

Tel.: +49 (0)89 2306954 0
Mail: info@ftapi.com
Web: https://www.ftapi.com

Sonstige Informationen

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Inhalt

Einleitung

Angesichts der wachsenden Besorgnis über Cybersicherheitsbedrohungen und Datenschutzverletzungen ist die Gewährleistung der Sicherheit und Integrität von Dateiübertragungen von größter Bedeutung. Denn die nahtlose Übertragung von Dateien ist ein unverzichtbarer Bestandteil moderner Kommunikation und Zusammenarbeit geworden. Ob für private oder berufliche Zwecke, Einzelpersonen und Organisationen tauschen regelmäßig vertrauliche Informationen aus, die von Finanzdokumenten bis hin zu geheimen Daten wie Konstruktionsplänen reichen.

Doch wie ist der Stand in deutschen Unternehmen beim Thema sicherer Datentransfer? Mit welchen Herausforderungen sehen sich Unternehmen im Zuge des sicheren Datentransfers konfrontiert? Welche Gründe waren ausschlaggebend für den Einsatz? Und wie schätzen Unternehmen die Bedrohungslage in Zukunft ein?

Um diese Fragen zu beantworten, wurden im Rahmen dieser Studie 200 Personen befragt, die maßgeblich oder stark am Entscheidungsprozess bezüglich sicherem Datentransfer beteiligt waren. Befragt wurden dafür im Februar 2024 Unternehmen mit 100 bis 4.999 Mitarbeitenden aus den Branchen Industrie, Handel, Dienstleistungen, Finanzwesen, öffentliche Verwaltungen sowie Non-Profit-Organisationen.

Sicherer Datentransfer in Unternehmen bereits Realität

Digitale Konnektivität und die Abhängigkeit vom Informationsaustausch prägen nicht nur die private Welt, sondern auch maßgeblich die Geschäftswelt. Daher sollte die Sicherheit der Datenübertragung gegenüber unbefugtem Zugriff, Datenabfluss oder Manipulation ein vorrangiges Anliegen für jedes Unternehmen sein. Unter sicherer Datenübertragung versteht man den Prozess der Datenübertragung von einem Ort zu einem anderen auf eine Weise, die die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gewährleistet. Dies bedeutet, dass die Daten vertraulich bleiben und für Unbefugte nicht zugänglich sind, während der Übertragung unverändert bleiben (Integrität) und bei Bedarf für autorisierte Parteien zugänglich sind (Verfügbarkeit). Dafür stehen Unternehmen unterschiedliche Möglichkeiten zur Verfügung. Angefangen von Verschlüsselung der Daten und E-Mails über den Einsatz privater Netzwerke, strikten Zugriffskontrollen oder auch kollaborativen Plattformen zum sicheren Austausch von Daten.

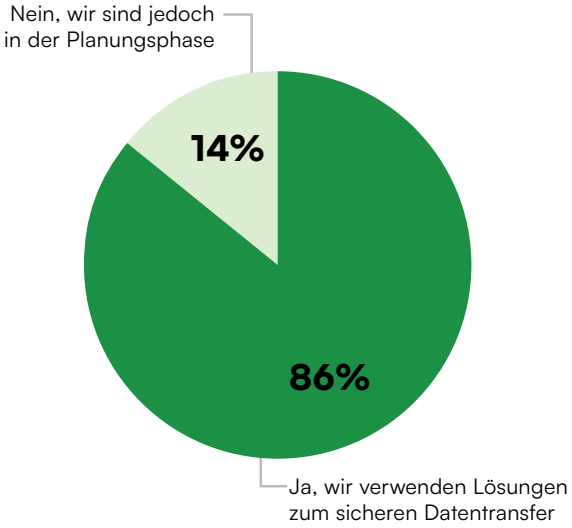
Bereits heute verwendet die überwiegende Mehrheit (86 Prozent) von Unternehmen Lösungen zum sicheren Datentransfer. Besonders Finanzdienstleister sind hier als Vorreiter hervorzuheben (92 Prozent). Traditionell sind Banken bei Sicherheitsmaßnahmen auch aufgrund der strengen Auflagen innerhalb der Branche besser ausgestattet als es bei anderen Branchen der Fall ist. Im Vergleich dazu sind es bei den Dienstleistern nur rund 74 Prozent, die bereits heute irgendeine Art von Lösung zum sicheren Datentransfer verwenden.

Aber diese Werte müssen mit Vorsicht genossen werden. Im weiteren Verlauf dieser Studie wird deutlich, dass der angestrebte Effekt des Einsatzes von sicheren Lösungen teilweise verpufft. Insbesondere wenn Mitarbeitende die Lösungen nicht oder nicht richtig nutzen. Da viele Unternehmen nicht nur in der Vergangenheit Opfer von Cyberangriffen waren, sondern auch in Zukunft mit einer Verschärfung der Situation rechnen, ist es umso wichtiger, Lösungen einzusetzen, die auch tatsächlich genutzt werden.

Abbildung 1

EINSATZGRADE SICHERER DATENTRANSFER

Basis: 200 Unternehmen



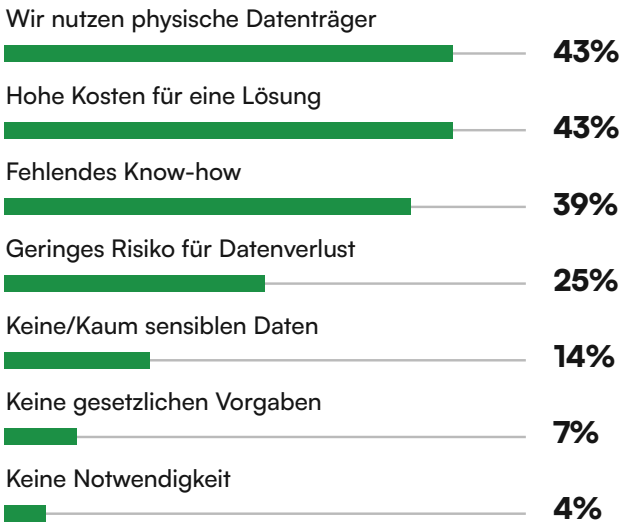
Kosten und Know-how-Mangel verhindern sichere Lösungen

Die Gründe, warum ein Teil der Unternehmen noch keine Lösungen zum sicheren Datentransfer im Einsatz hat, sind vielfältig, wobei sich drei Gründe als Hauptfaktoren anhand der Ergebnisse abbilden lassen. Knapp 43 Prozent der befragten Unternehmen nutzen primär physische Datenträger zum Austausch von Informationen. Der Einsatz physischer Datenträger wie USB-Sticks, externer Festplatten oder physischer Dokumente zur Speicherung und Übertragung von Daten kann für Unternehmen sowohl Vor- als auch Nachteile haben. Ein Vorteil davon wäre beispielweise die Verringerung von Cyber-Risiken, da die physischen Datenträger nicht an das Internet angebunden sind. Im Gegenzug entstehen aber wieder andere Risiken wie der Verlust physischer Datenträger. So lies beispielsweise im Jahr 2022 ein externer Mitarbeiter einen USB-Stick mit persönlichen Daten wie Namen, Adressen und Bankverbindungen, von 460.000 Einwohnern einer japanischen Stadt in einem Lokal liegen.[1]

Abbildung 2

GRÜNDE GEGEN DEN EINSATZ VON SICHEREM DATENTRANSFER

Basis 28 Unternehmen die keine Lösungen im Einsatz haben | Mehrfachnennungen möglich



Zudem verliert man zudem auch an Produktivität, vor allem in Bezug auf Remote-Arbeitsumgebungen. So unterstützen physische Datenträger keine kollaborative Zusammenarbeit in Echtzeit, wie es beispielsweise bei Cloud-Anwendungen möglich ist und auch der Fernzugriff ist nicht möglich.

Darüber hinaus sind auch die hohen Kosten für ebenfalls 43 Prozent der Unternehmen bislang ein großer Hinderungsgrund gegen den Einsatz von Lösungen zum sicheren Datentransfer. Die Einführung von neuen Lösungen bedeutet für Unternehmen zwar, dass diese eine größere finanzielle Belastung haben, gleichzeitig sollten Investitionen in sicheren Datentransfer auch als Chancen wahrgenommen werden. Nicht nur werden Risiken und damit potenzielle finanzielle Schäden durch Datenverluste minimiert, Investitionen in Cybersicherheit können auch als Wettbewerbsvorteil genutzt werden. Kunden zu zeigen, dass Datenschutz im eigenen Unternehmen einen hohen Stellenwert genießt, kann das Vertrauen der Kunden stärken und das Unternehmen gegenüber dem Wettbewerb besser positionieren.

Der dritte Hauptgrund ist der Mangel an Know-how bezüglich der Implementierung einer solchen Lösung innerhalb der Unternehmen. Dies stellt für 39 Prozent der Unternehmen ein größeres Problem dar. Mangelnde Kenntnisse können beispielsweise dazu führen, dass die sicheren Lösungen aufgrund von falscher Konfiguration selbst anfällig für Cyberbedrohungen werden. Außerdem kann eine falsche Implementierung dafür sorgen, dass regulatorischen Anforderungen nicht eingehalten werden, was zu rechtlichen Konsequenzen oder auch Geldstrafen führen kann. Sind Unternehmen nicht in der Lage, internes Know-how aufzubauen, so empfiehlt sich die Zusammenarbeit mit Partnern, die auf diesem Gebiet über das nötige Fachwissen verfügen.

[1]Quelle: https://www.spiegel.de/panorama/gesellschaft/amagasaki-in-west-japan-mitarbeiter-verliert-usb-stick-mit-daten-aller-460-000-einwohner-in-der-kneipe-a-95a4db8f-8d80-4a4a-9446-d4dfaf6e33cf

Datenschutzrisiken sind Treiber für Sicherheit

Eine Mehrheit derUnternehmen gibt an, bereits heute zumindest irgendeine Art von Lösung zum sicheren Datentransfer im Einsatz zu haben. Doch was genau waren die ausschlaggebenden Gründe, die Unternehmen dazu veranlasst haben, solche Lösungen zu implementieren?

Für rund zwei Drittel der befragten Unternehmen ist insbesondere die Minimierung von Datenschutzrisiken ein wichtiger Faktor. Zudem sagen weitere 58 Prozent, dass gesetzliche Vorgaben sie zum Handeln bewegt hätten.

Wenig verwunderlich, denn die Einhaltung von Datenschutzbestimmungen wie der Datenschutz-Grundverordnung (DSGVO) in Europa ist zwingend erforderlich. Verstößt man dagegen, kann dies unter anderem schwere Bußgelder oder rechtliche Konsequenzen nach sich ziehen.

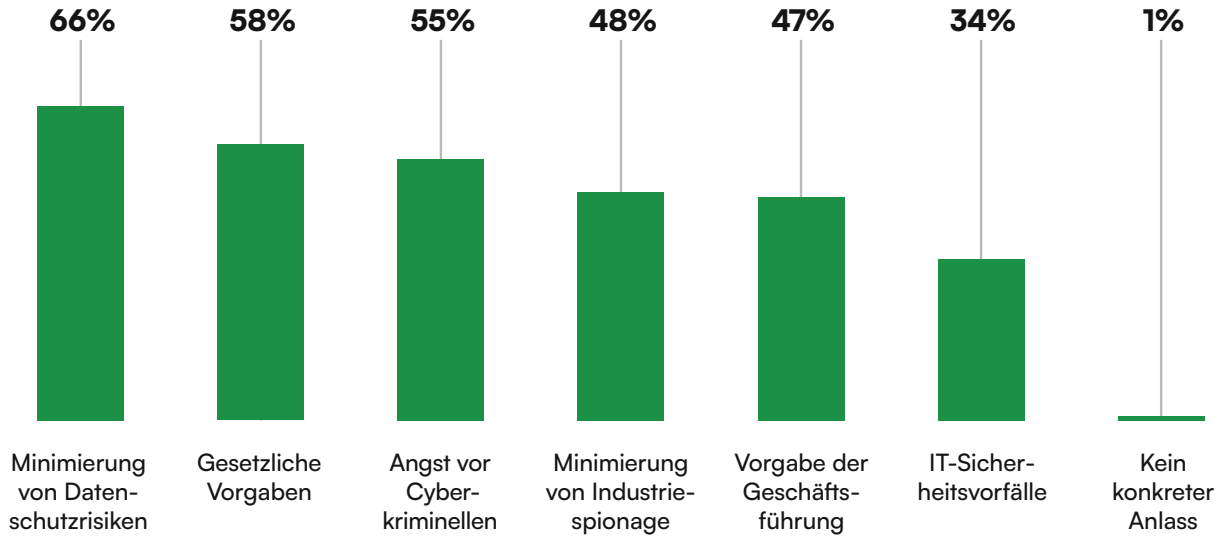
Und bei DSGVO-Verstößen kommen nicht nur finanzielle Strafen auf die Unternehmen zu, man kann sich auch das eigene Unternehmensimage zerstören, das Vertrauen der Kunden verlieren oder sogar sensible Unternehmensinformationen und Geschäftsgeheimnisse in die Hände Unbefugter abfließen lassen — mit potenziell verheerenden Auswirkungen für die eigene Marktposition.

Darüber hinaus möchten 55 Prozent der Unternehmen die Angriffsfläche für mögliche Cyberangriffe verringern. Denn jedes potenzielle Einfallstor stellt eine Schwachstelle dar. Eine Reduzierung senkt das Risiko gegenüber Cyberangriffen, schützt sensible Daten und verhindert dadurch Datenschutzverletzungen. Weist man zudem gegenüber Behörden nach, dass man durch den Einsatz von Lösungen zum sicheren Datentransfer ein potenzielles Einfallstor geschlossen hat, erfüllt man die regulatorischen Anforderungen und Compliance-Standards und vermeidet so rechtliche Konsequenzen oder auch Strafen.

Abbildung 3

TREIBER FÜR DEN EINSATZ VON LÖSUNGEN

Basis 200 Unternehmen | Mehrfachnennungen möglich



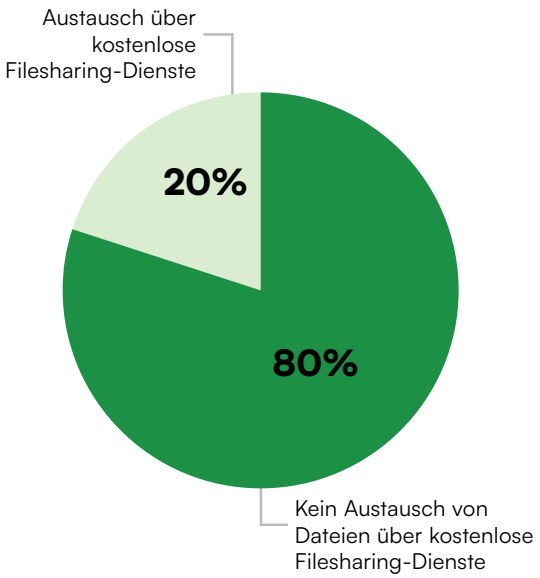
Kostenloses Filesharing noch teilweise erlaubt

Eine Möglichkeit, das firmeninterne Schutzniveau zu erhöhen, bietet das Verbot von kostenlosen Filesharing Diensten. 80 Prozent der befragten Unternehmen verbieten bereits die Nutzung kostenloser Filesharing-Dienste. Ein solches Verbot ist auch nötig, um die Datensicherheit im Unternehmen zu garantieren und muss unternehmensweit gelebt und durchgesetzt werden.

Abbildung 4

VERBOT VON KOSTENLOSEM FILESHARING

Basis: 200 Unternehmen



Allerdings bedeutet das Ergebnis auch, das rund ein Fünftel der Unternehmen weiterhin kostenloses Filesharing erlaubt. Das hat eine Reihe von negativen Auswirkungen zur Folge. So entsteht durch die Nutzung ein weiteres potenzielles Einfallstor für Cyberangriffe, da keine Garantie besteht, dass der genutzte Dienst auch wirklich sicher ist.

Die Nutzung solcher Dienste fördert zudem die Entstehung von Schatten-IT und IT-Admins verlieren den Überblick darüber, welche Dienste im Unternehmen genutzt werden. Ohne diesen Überblick können IT-Verantwortliche auch keine Maßnahmen ergreifen, um die Cybersicherheit zu gewährleisten.

Des Weiteren sollten sensible Daten nicht auf kostenlosen Filesharing-Diensten hochgeladen werden. Das betrifft vor allem Informationen, die besonders schützenswert sind. Persönliche sowie finanzielle Daten, aber auch Geschäftsgeheimnisse sollten nie auf kostenlosen Filesharing-Diensten hochgeladen werden. Es besteht die Gefahr, dass Unbefugte Zugriff auf die hochgeladenen Daten erhalten, diese stehlen und für kriminelle Zwecke missbrauchen. Solche Datenschutzverletzungen können den Ruf des Unternehmens ernsthaft schädigen und das Vertrauen bei Partnern oder Kunden stark belasten. Darüber hinaus entstehen auch finanzielle Schäden in Form von Schadensbekämpfung beispielsweise durch externe Dienstleister, Anwaltskosten oder auch Bußgeldern.

Eine einheitliche Regelung oder ein direktes Verbot der Nutzung kostenloser Filesharing-Dienste trägt dazu bei, Sicherheitsrisiken zu vermindern und geistiges Eigentum zu schützen. Unternehmen sollten zum Teilen von Dateien professionelle Filesharing-Lösungen verwenden, bei denen Datenschutz und Compliance im Vordergrund stehen.

Komplexe Lösungen blockieren Datensicherheitsbestrebungen

Obwohl Datensicherheit einen hohen Stellenwert genießt, sehen Unternehmen bei der Einführung von sicheren Lösungen zum Teilen von Daten z. B. mit einer E-Mail-Verschlüsselung einige Schwierigkeiten.

So sind fast 47 Prozent der Unternehmen der Meinung, dass die Einführung von Lösungen für den verschlüsselten Datenverkehr sehr komplex sei. Die Implementierung erfordert von den IT-Verantwortlichen ein gewisses Maß an technischem Fachwissen sowie unter Umständen auch Spezialwissen über Verschlüsselung. Dazu müssen auch die Interoperabilität mit anderen Systemen gewährleistet sowie die potenziellen negativen Auswirkungen auf die Leistung der IT-Infrastruktur berücksichtigt werden.

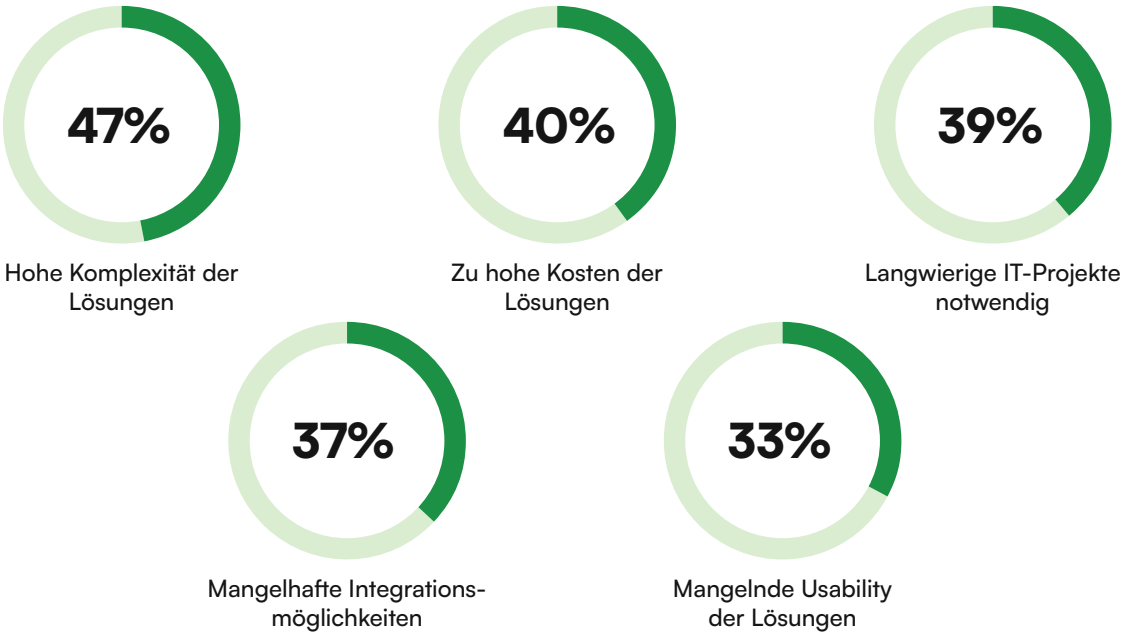
An zweiter Stelle folgen die potenziellen Kosten für die Implementierung einer sicheren Lösung. In die Überlegungen fallen unter anderem Kosten für Lizenzen sowie Wartungs- oder auch Supportkosten und möglicherweise auch Schulungskosten. Bei knappen IT-Budgets müssen Unternehmen die Kosteneffizienz im Auge behalten.

Darüber hinaus geben noch 39 Prozent der Unternehmen an, dass die Implementierung einer sicheren Lösung für die Datenübertragung mit langfristigen Projekten verbunden ist. Solche Projekte erfordern ein hohes Maß an personellen, zeitlichen und finanziellen Ressourcen. Besonders schwierig wird es vor allem dann, wenn die IT noch weitere wichtige Projekte durchführen muss und der volle Fokus dadurch nicht auf die Implementierung von sicheren Lösungen gesetzt werden kann.

Abbildung 5

HEMNISSE BEI DER EINFÜHRUNG VON SICHEREM DATENTRANSFER

Basis 200 Unternehmen | Mehrfachnennungen möglich | Top 5



Sicherheitsniveau und Bedienbarkeit als wichtigste Merkmale

Für Unternehmen, die Lösungen für den sicheren Datentransfer benutzen oder benutzen wollen, sind einige Eigenschaften bei entsprechenden Lösungen besonders wichtig. An erster Stelle steht bei 52 Prozent der Unternehmen das hohe Sicherheitsniveau der Lösung. Lösungen zum sicheren Datentransfer sollen dafür Sorge tragen, dass sensible Informationen vor unbefugtem Zugriff oder Diebstahl geschützt werden. Je höher das Sicherheitsniveau der Lösung, desto besser sind vertrauliche Daten gegen Cyber-Bedrohungen geschützt und potenzielle Datenschutzverletzungen können minimiert werden. Dazu müssen die Lösungen auch je nach Branche mehr oder weniger strenge gesetzliche Anforderungen erfüllen. Eine Nichteinhaltung kann zu Strafen und rechtlichen Konsequenzen führen.

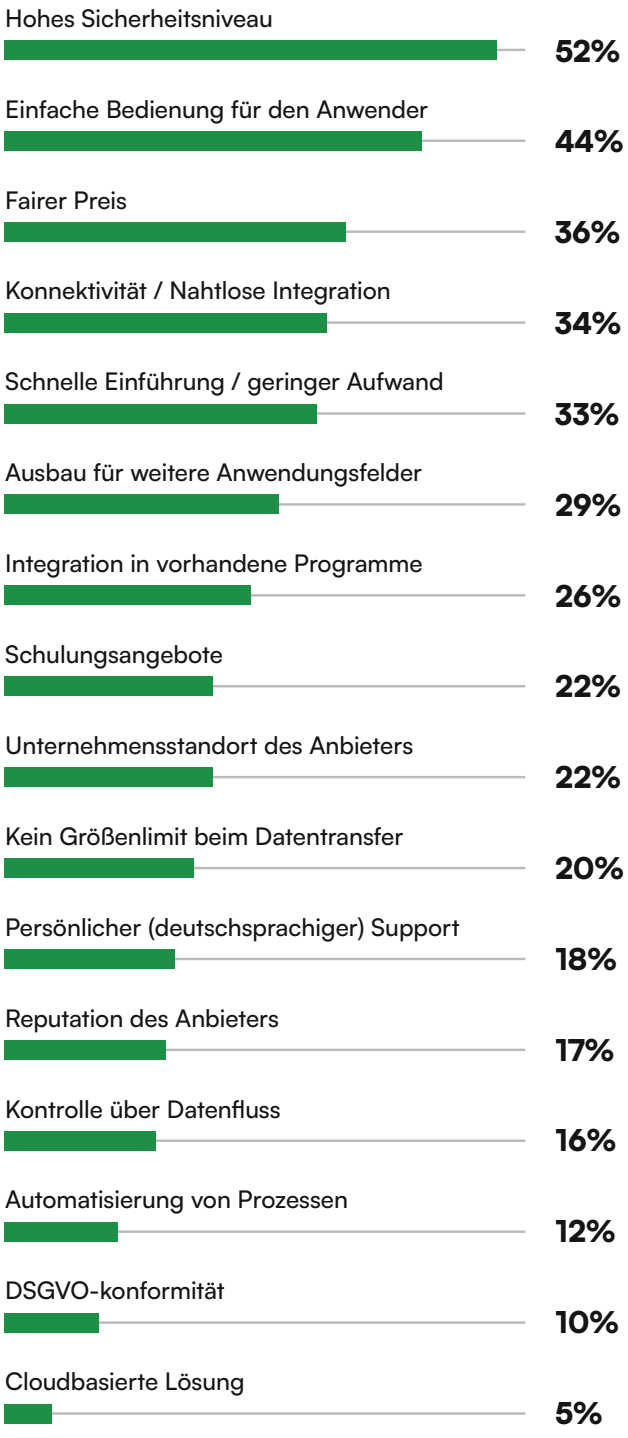
Für weitere 44 Prozent der Unternehmen ist zudem eine leichte Bedienung der Lösung von ausschlaggebender Bedeutung. Eine hohe Benutzerfreundlichkeit sorgt dafür, dass die eingesetzte Lösung für den sicheren Datentransfer eine hohe Akzeptanz bei den Benutzern fördert. Denn wenn eine Lösung komplex zu bedienen ist, kann das dazu führen, dass Nutzer sich weigern, diese Lösungen zu verwenden und sich nach leichteren und meist weniger sichereren Methoden umsehen. Bei vielen intuitiv benutzbaren Lösungen fällt der Schulungsaufwand minimal aus und interne Kosten können gespart werden.

Darüber hinaus spielen auch der Preis (36 Prozent), die Anbindung an bestehende Systeme (34 Prozent) und ein schneller Rollout (33 Prozent) größere Rollen.

Abbildung 6

WICHTIGE FAKTOREN EINER SICHEREN LÖSUNG

Basis 200 Unternehmen | Mehrfachnennungen möglich



Wunsch nach Einfachheit fördert Schatten-IT

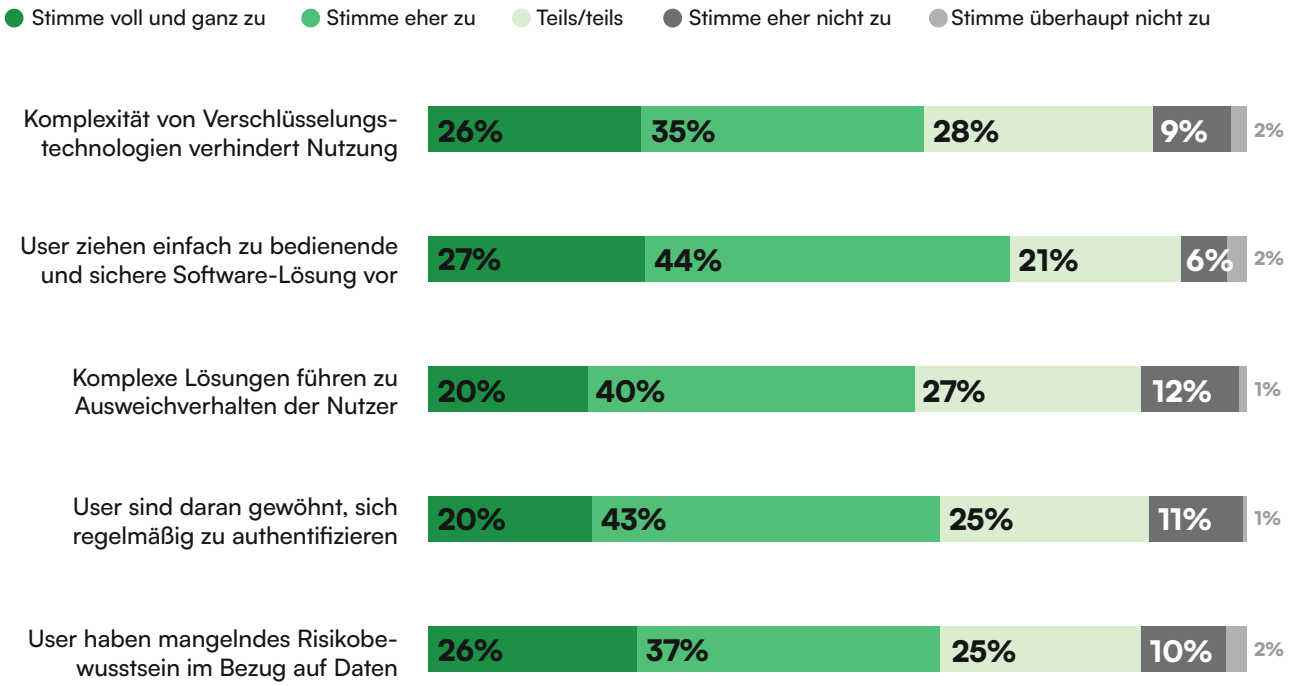
Betrachtet man das Nutzerverhalten, lässt sich feststellen, dass die Mehrheit der Befragten (71 Prozent) eine einfach zu bedienende Software-Lösung gegenüber einer komplizierten, aber dafür sichereren Lösung bevorziehen würde. Das bedeutet, dass die Balance zwischen Sicherheit und Einfachheit der Bedienung zu jeder Zeit gewährleistet sein muss. Darüber hinaus stimmen 61 Prozent der Unternehmen der Aussage zu, dass die Komplexität aktueller Verschlüsselungstechnologien eine breite Nutzung im Unternehmen verhindert. Doch ohne Akzeptanz für die Nutzung von sicheren Technologien können Unternehmen die IT-Sicherheit nicht garantieren. Daher müssen auch Verschlüsselungstechnologien einfach einsetzbar sein.

Diese Aussagen decken sich zudem auch mit der Befürchtung, dass eine komplexe Lösung Schatten-IT fördert. Knapp 60 Prozent der befragten Unternehmen stimmen dieser Aussage zu. Dazu sind sich 63 Prozent der Unternehmen darüber im Klaren, dass User über mangelndes Sicherheitsbewusstsein verfügen. Diese Ergebnisse zeigen vor allem auch, dass die Sicherheit keineswegs garantiert ist, auch dann nicht, wenn Unternehmen Lösungen zum sicheren Datentransfer implementiert haben. In Anbetracht, dass die überwiegende Mehrheit der Unternehmen behauptet, über sichere Lösungen zum Datentransfer zu verfügen, stellt das mangelnde Sicherheitsbewusstsein ein erhebliches Risiko dar.

Abbildung 7

NUTZERVERHALTEN IN UNTERNEHMEN

Basis 200 Unternehmen



Der Faktor Mensch ist immer das schwächste Glied der Sicherheitskette. Daher ist es in Anbetracht der Ergebnisse wichtig, Schatten-IT zu vermeiden, indem einfach zu bedienende Lösungen eingesetzt werden, die Anwender auch akzeptieren und die dieselbe Benutzerfreundlichkeit mitbringen, wie es ihre präferierten Lösungen tun. Darüber hinaus müssen auch die Anwender selbst regelmäßig zu IT-Sicherheitsthemen geschult werden, um die menschliche Fehlerquellen weiter zu minimieren.

Positiv lässt sich festhalten, dass rund 63 Prozent der Unternehmen der Meinung sind, dass sich die Nutzer mittlerweile an die regelmäßige Authentifizierung gewöhnt haben. Das zeigt, dass sicherheitsrelevante Maßnahmen mit der Zeit auch von den Nutzern akzeptiert werden.

63 PROZENT HABEN SICH AN AUTHENTIFIZIERUNG GEWÖHNT.

Es beweist zudem, dass Cybersicherheit nicht länger als notwendiges Übel aus der IT angesehen wird. Denn die Akzeptanz der Nutzer für Sicherheitsmaßnahmen bedeutet auch, dass Cyberbedrohungen als echte Risiken nicht nur für das Unternehmen, sondern auch für den Nutzer selbst angesehen werden.

Die Ergebnisse zeigen zudem, dass die Nutzung von sicheren Lösungen zum Datentransfer von höchster Bedeutung ist.

NUTZER VERSTEHEN DIE NOTWENDIGKEIT VON SICHERHEITSMAßNAHMEN

Dabei muss man jedoch den Spagat zwischen Sicherheit und Usability meistern, um Schatten-IT und damit erhöhte Gefahr für das Unternehmen zu verhindern. Denn grundsätzlich ist das Bewusstsein für IT-Sicherheit bei den Mitarbeitenden vorhanden. Allerdings nur bis zu einem gewissen Komplexitätsgrad. Sind Lösungen zu kompliziert in der Anwendung, so rückt die IT-Sicherheit gegenüber der Produktivität in den Hintergrund.

Keine Entspannung der Bedrohungslage in Sicht

Hinsichtlich der allgemeinen Bedrohungslage durch Cyberangriffe ist aktuell kein Rückgang zu spüren. So sagen knapp 37 Prozent der befragten Unternehmen, dass sich die Bedrohungslage in den vergangenen 12 Monaten noch einmal zugespitzt hat. Besonders größere Unternehmen zwischen 1.000 und 4.999 Mitarbeitenden konnten eine weitere Anspannung der Bedrohungslage feststellen (48 Prozent). Bei kleineren Unternehmen mit 100 bis 249 Mitarbeitenden konnten nur knapp 28 Prozent eine Vergrößerung der Bedrohungslage erkennen. Bei 39 Prozent der Unternehmen ist die Bedrohungslage in etwa gleich geblieben. Bei einem Viertel der Unternehmen gingen die Cyberangriffe sogar zurück.

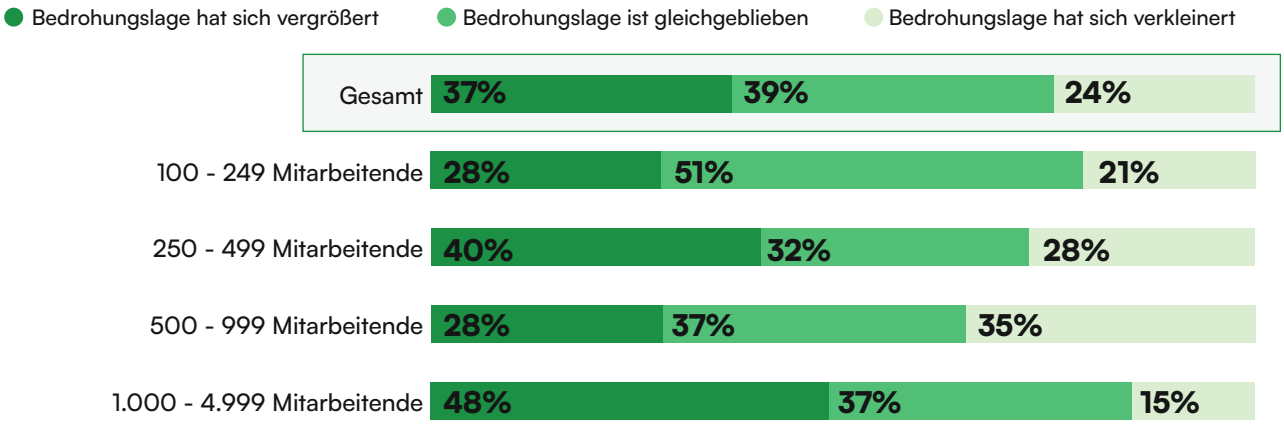
Besonders öffentliche Verwaltung und andere Non-Profit-Organisationen spüren hier eine deutliche Zuspitzung. Hier gab kein einziges Unternehmen an, eine Verringerung der Cyberangriffe erkannt zu haben. Die überwiegende Mehrheit war sogar noch stärker von Cyberangriffen betroffen, als dies im Vorjahr der Fall war.

Diese große Gefahr durch Cyberangriffe spiegelt sich auch bei der Betrachtung der erfolgreichen Cyberangriffe wider. So gab beispielsweise rund ein Viertel der Unternehmen an, dass sowohl sie als auch Wettbewerber in den vergangenen 12 Monaten Opfer eines erfolgreichen Cyberangriffs waren. Weitere 26 Prozent waren selbst Opfer, haben aber keine Auskunft darüber, ob es erfolgreiche Angriffe auf Wettbewerber gab. Auch in Zukunft erwartet man keinerlei Entspannung. So gehen 39 Prozent der Unternehmen davon aus, in den kommenden 12 Monaten Opfer von Cyberangriffen zu werden. Weitere 45 Prozent glauben auch, dass ihre Wettbewerber nicht vor Cyberangriffen verschont bleiben. Diese Zahlen sind erschreckend, denn sie sind noch ein Stück pessimistischer im Vergleich zur Betrachtung der Cyberangriffe der vergangenen 12 Monate.

Abbildung 8

BEDROHUNGSLAGE NACH GRÖßENKLASSEN

Basis 200 Unternehmen



Wie schnell sich ein erfolgreicher Cyberangriff ausbreiten kann, zeigt das Beispiel der Supply Chain Attacke auf einen renommierten IT-Dienstleister. Dort erlangte eine Hackergruppe über eine ungepatchte Zero-Day-Schwachstelle Zugang zu einer Remote Management Lösung und spielte ein gefälschtes automatisches Update bei ihren Kunden auf. Über diese Kunden wiederum konnten die Cyberkriminellen dann Ransomware bei rund 1.500 Unternehmen verteilen.[2]

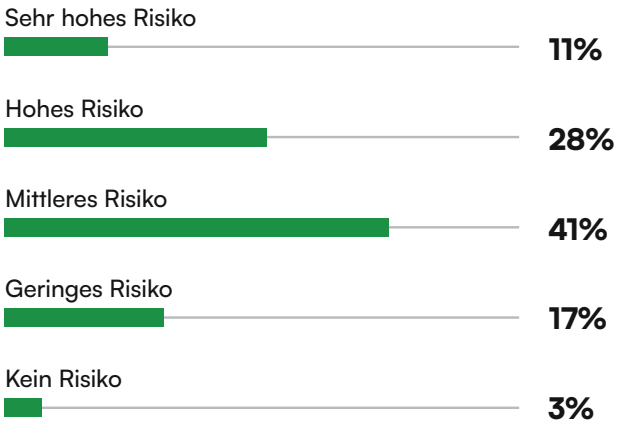
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gab im Jahresbericht zur IT-Sicherheit in Deutschland für 2023 an, dass die Bedrohung im Cyberraum so hoch wie noch nie zuvor ist. Insbesondere die Professionalisierung von Cyberkriminalität zum Beispiel mit Konzepten wie „Cybercrime-as-a-Service“ verschärfen die Situation noch einmal.

Diese Ergebnisse zeigen, dass der Einsatz von scheinbar sicheren Lösungen für den Datentransfer nicht ausreichend ist. Mögliche Gründe wie die Verbreitung von Schatten-IT oder mangelndes Sicherheitsbewusstsein der Mitarbeiter wurden bereits im Rahmen dieser Studie aufgezeigt.

Abbildung 9

RISIKOEINSCHÄTZUNG FÜR CYBERANGRIFFE

Basis 200 Unternehmen

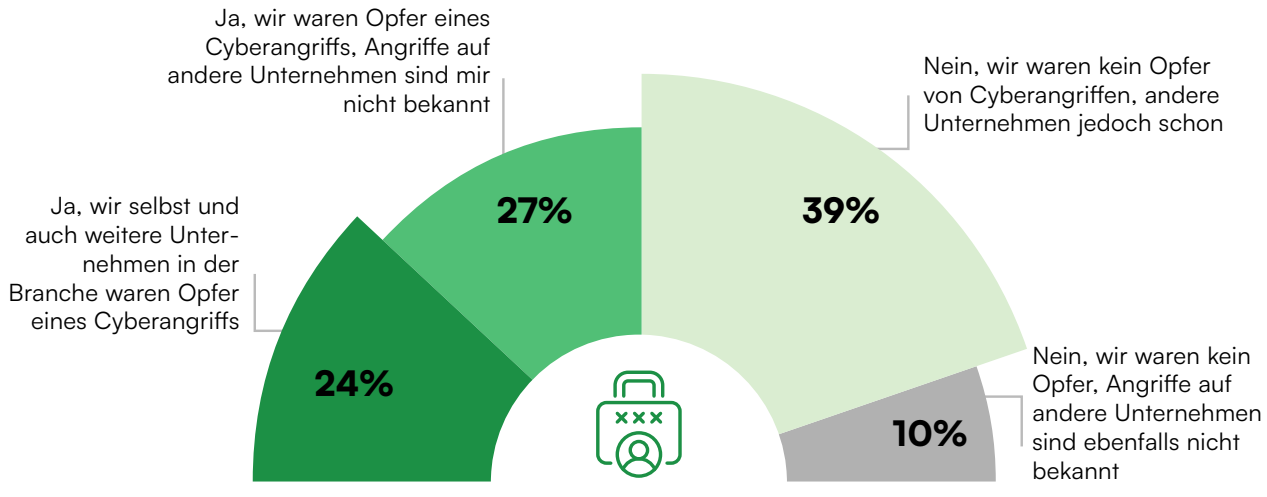


Daher ist es für Unternehmen von höchster Bedeutung die potenziellen Schwachstellen in ihrer IT-Infrastruktur zu schließen sowie die Mitarbeiter für Cybersicherheit zu sensibilisieren. Denn die Bedrohung im Cyberraum wird nicht abnehmen, sondern sich weiter verschärfen.

Abbildung 10

CYBERANGRIFFE IN DEN LETZTEN 12 MONATEN

Basis 200 Unternehmen



[2] Quelle: https://www.heise.de/news/Kaseya-Angriff-Cybercrime-Erpresser-fordern-70-Millionen-US-Dollar-6128705.html

Sicherheitsverstöße führen zu DSGVO-Vergehen

Sicherheitsverstöße führen zu DSGVO-Vergehen. So berichtet das DSGVO-Portal, dass DSGVO-Strafen in Europa kontinuierlich anwachsen. So sollen die Bußgelder im Jahr 2023 im Vergleich zum Vorjahr um 29 Prozent angestiegen sein. Hauptgrund dafür ist vor allem die Rekordstrafe von 1,2 Mrd. EUR für Meta. In Deutschland hatten nicht alle Behörden die Anzahl und Höhe der Bußgelder gemeldet. Manche Bundesländer lieferten keine Zahlen. Fakt ist jedoch, dass mindestens 169 Bußgelder in Höhe von mehr als 4 Mio. EUR verhängt wurden. Die meisten Verstöße werden derzeit bei ordnungsgemäßer Meldung und Aufzeigen adäquater Maßnahmen, die solche Vorfälle in Zukunft unterbinden, ohne Bußgeld geahndet.[3]

Abbildung 11

„DSGVO-VERSTÖßE WERDEN KONSEQUENT UND HART BESTRAFT."

22%	Stimmen voll und ganz zu
41%	Stimmen eher zu
26%	Teils teils
10%	Stimmen eher nicht zu
1%	Stimmen überhaupt nicht zu

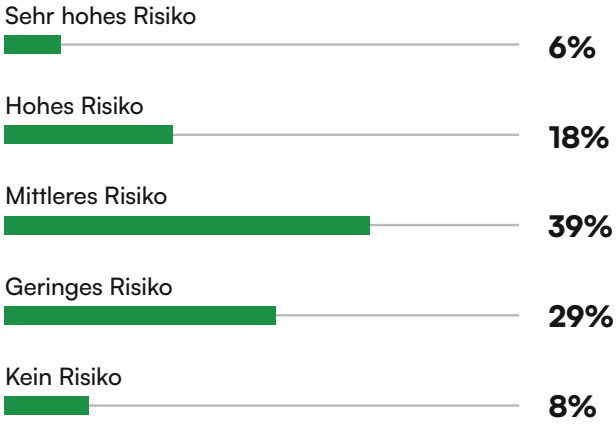
Basis 200 Unternehmen

Es ist aber davon auszugehen, dass neben den Vorfällen ohne Bußgeldbescheid auch eine gewisse Anzahl an Verstößen noch in der Schwebe sind, was mögliche Verurteilungen betrifft. Öffentliche Zahlen sind daher meist nur als Spitze des Eisbergs zu verstehen.

Abbildung 12

RISIKOEINSCHÄTZUNG DSGVO-STRAFEN

Basis 200 Unternehmen



Auch die befragten Unternehmen dieser Studie können feststellen, dass die DSGVO kein zahnloser Papiertiger zu sein scheint. So sind mehr als 60 Prozent der Unternehmen davon überzeugt, dass DSGVO-Verstöße hart und konsequent bestraft werden. Darüber hinaus sehen 63 Prozent der Unternehmen für sich selbst mindestens ein mittleres Risiko, dass sie in den kommenden 12 Monaten ein DSGVO-Bußgeld erhalten könnten. Und dass alles trotz der Tatsache, dass sich ein Großteil der Unternehmen auf die Fahne schreibt, über sichere Lösungen zum Datentransfer zu verfügen. Es liegt nahe, dass die technischen Voraussetzungen für den sicheren Datentransfer zwar grundsätzlich in den Unternehmen vorhanden sind, diese jedoch nur schlecht umgesetzt werden. Daher sollten Unternehmen, die davon ausgehen, in Zukunft mit der DSGVO Probleme zu bekommen, dringend an einer Neuausrichtung der eigenen IT-Sicherheitsstrategie arbeiten.

[3] Quelle: https://www.dsgvo-portal.de/news/rueckblick_dsgvo-bussgeldverfahren_und_datenpannen_2023.php

Fazit

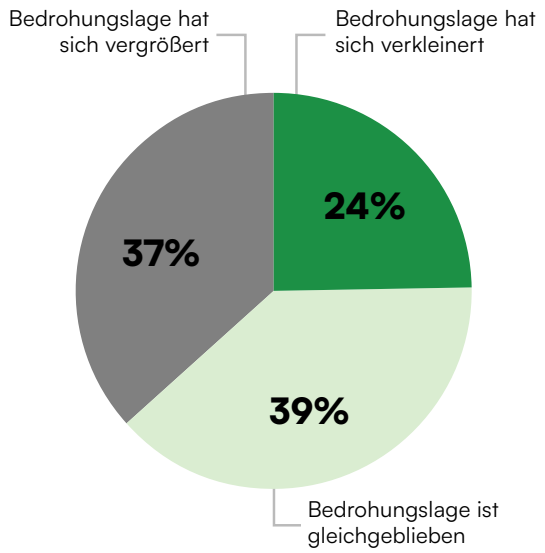
Im Zuge der sich immer weiter zuspitzenden Sicherheitslage und der Pflicht der Einhaltung von immer mehr gesetzlichen Vorschriften ist der Einsatz von Lösungen zum sicheren Datentransfer für Unternehmen unerlässlich. Denn nur mit solchen Lösungen sind Unternehmen in der Lage, Cyberbedrohungen zu minimieren und die eigenen sensiblen Daten effektiv zu schützen.

Wie wichtig die Verbesserung der eigenen IT-Sicherheit an allen potenziellen Angriffsvektoren ist, zeigen die Ergebnisse dieser Studie. Nur ein Viertel der befragten Unternehmen konnte eine Entspannung der Bedrohungslage feststellen. Für den überwiegenden Teil bleibt die Bedrohungslage gleich kritisch oder hat sich sogar vergrößert.

Abbildung 13

ENTWICKLUNG DER BEDROHUNGSLAGE DURCH CYBERANGRIFFE

Basis: 200 Unternehmen



Ein knappes Viertel war zudem selbst Opfer von Cyberangriffen und 40 Prozent sehen in den nächsten zwölf Monaten ein hohes oder sogar sehr hohes Risiko, Opfer von Cyberkriminellenzu werden.

Unternehmen können bei der schier endlos wirkenden Anzahl an unterschiedlichen Lösungen schnell den Überblick verlieren. Optimalerweise sollte eine Lösung gewählt werden, die unterschiedlichen Technologien wie Verschlüsselung, Authentifizierung oder die sichere Übertragung von Daten, in einer einzigen Suite enthält. Besonders dann, wenn Budgets und personelle Ressourcen knapp sind, eignet sich eine All-in-One-Lösung, um maximalen Schutz zu erhalten.

MITARBEITENDE ZIEHEN EINE EINFACH ZU BEDIENENDE SOFTWARE-LÖSUNG EINER KOMPLIZIERTEREN, ABER DAFÜR SICHEREREN LÖSUNG VOR.

Die Kosten für eine solche Lösung sind mit Blick auf die sich rasant zuspitzende Sicherheitslage gut investiertes Geld. Ebenfalls sollte darauf geachtet werden, dass die Lösung intuitiv nutzbar ist. Mitarbeitende präferieren einfach zu bedienende Lösungen. Sie nutzen unter Umständen unsichere Lösungen, um der Komplexität zu entgehen, was einen weiteren Gefahrenherd darstellt. Weitere Aspekte, die es bei der Wahl eines Anbieters zu betrachten gibt, sind das Vorhandensein von gängigen Zertifizierungen wie der ISO 27001 und des BSI C5. Diese garantieren, dass Cloud-Dienstleister als absolut sicher gelten und damit eine optimale Lösung für den sicheren Datentransfer darstellen.

Studiensteckbrief

Die Studie „Sicherer Datentransfer: Daten mit sicheren Kommunikationslösungen schützen“ wurde von der techconsult GmbH im Auftrag von FTAPI konzipiert und durchgeführt.

200 Personen, die maßgeblich oder stark in den Entscheidungsprozess bei der Anschaffung einer Lösung für sicheren Datentransfer involviert waren, wurden nach ihren Treibern für den Einsatz solcher Lösungen, ihren Herausforderungen damit, wichtigen Eigenschaften der Lösungen und der Bedrohungslage gegen Cyberangriffe befragt.

Abbildung 14

BRANCHENVERTEILUNG

Basis 200 Unternehmen

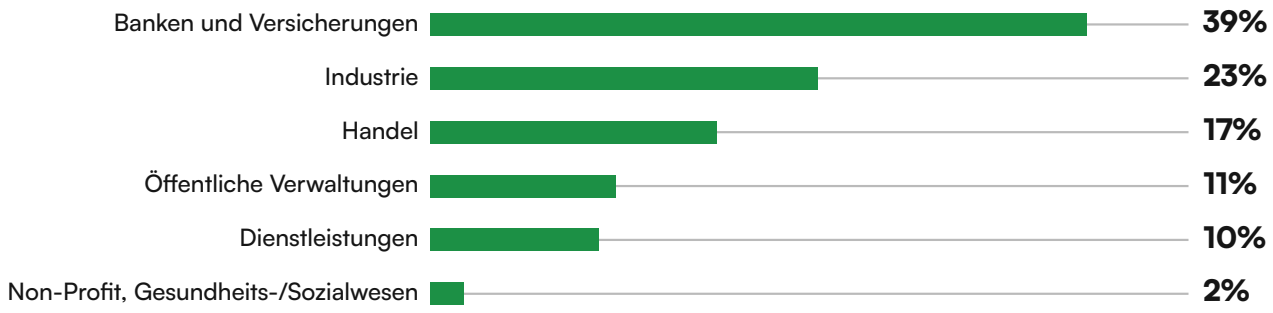


Abbildung 15

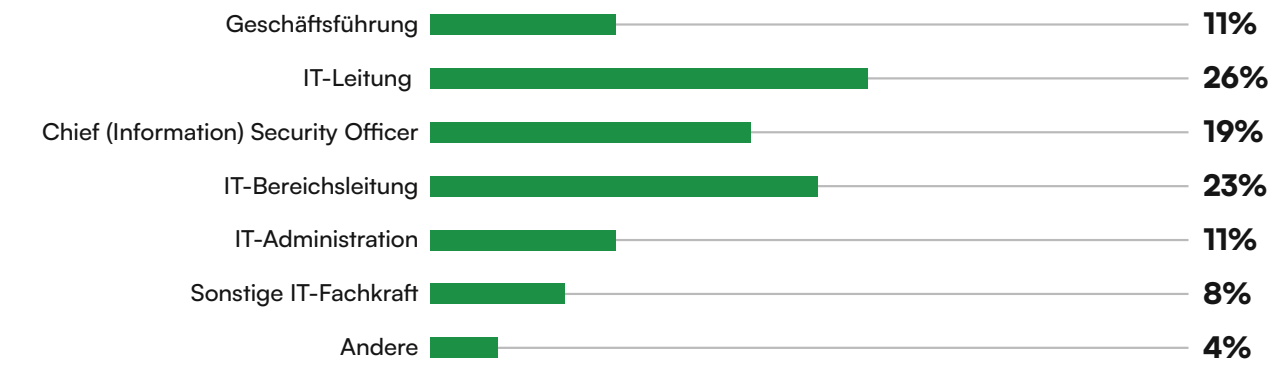
MITARBEITERGRÖßENKLASSEN

Basis 200 Unternehmen

Abbildung 16

POSITION IM UNTERNEHMEN

Basis 200 Unternehmen



Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

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

Raphael Napieralski
Analyst

Mail: raphael.napieralski@techconsult.de
Tel.: +49 (0)561 8109 181

Über die techconsult GmbH

Seit über 30 Jahren ist techconsult — als Research- und Analystenhaus — ein verlässlicher Partner für Anbieter und Nachfrager digitaler Technologien und Services. Mehr als 35.000 Interviews/Jahr mit Entscheidern, auf der Business- und Technologieebene, Lösungsanwendern sowie Technologie- und Serviceanbietern, bilden die neutrale Grundlage unserer Beratungs- und Projektaktivitäten.

So werden Nachfrager in ihrer digitalen Standortbestimmung und strategischen Planung ebenso unterstützt, wie in konkreten Sourcing-Prozessen, um fundierte Entscheidungen auf Basis datengestützter Fakten zu treffen. In der Entwicklung und Umsetzung individueller Go-to-Market-Strategien profitieren Anbieter sowohl strategisch als auch taktisch von der marktorientierten Unterstützung unserer Analysten und des tc-Partnernetzwerks.

Über die FTAPI Software GmbH

Das Münchener Software-Unternehmen FTAPI bietet eine umfassende Plattform für einfache und sichere Daten-Workflows und Automatisierung. Damit verbindet FTAPI Menschen, Daten und Systeme sicher, schnell und einfach. Seit 2010 vertrauen über 2.000 Unternehmen und mehr als eine Million aktive Nutzer*innen auf die Produkte SecuMails, SecuRooms, SecuForms und SecuFlows — egal ob es um das Senden oder Empfangen von Daten, den strukturierten Dateneingang, das Teilen von vertraulichen Informationen oder die sichere Automatisierung von Daten-Workflows geht: mit der Secure Data Workflow Plattform von FTAPI sind sensible Daten jederzeit geschützt. www.ftapi.com

Kontakt

FTAPI Software GmbH
Steinerstr. 15f
81369 München
Deutschland

Tel.: +49 (0)89 2306954 0
Mail: info@ftapi.com

Entscheidende Kriterien für eine sichere Datenaustausch-Lösung

Maximaler Nutzerkomfort
Eine intuitive Bedienbarkeit sowie ein minimaler Einführungsaufwand erhöhen die Akzeptanz gegenüber der neuen Lösung.

Höchste Sicherheit
Eine durchgehende Ende-zu-Ende-Verschlüsselung schützt Ihre Daten vor dem Zugriff Dritter und gewährleistet Ihnen höchste Sicherheit bei der digitalen Kommunikation.

Kein Größenlimit
Dateien jeglicher Art und Größe müssen sicher aus einer Lösung übertragen werden können.

Nahtlose Integration in bestehende Systeme
Fügt sich die Lösung problemlos in bestehende Systeme ein, können die Mitarbeitenden direkt in ihrer gewohnten Umgebung weiterarbeiten.

Datensouveränität und Nachvollziehbarkeit
Jederzeit die Kontrolle über den Datenfluss im eigenen Unternehmen zu behalten und die Souveränität der Daten zu gewährleisten, ist heute essentiell für den Unternehmenserfolg.

Geringer Verwaltungsaufwand
Eine schnelle Implementierung vermeidet zusätzlichen Admin-Aufwand und schont personelle Ressourcen in Ihrer IT-Abteilung.

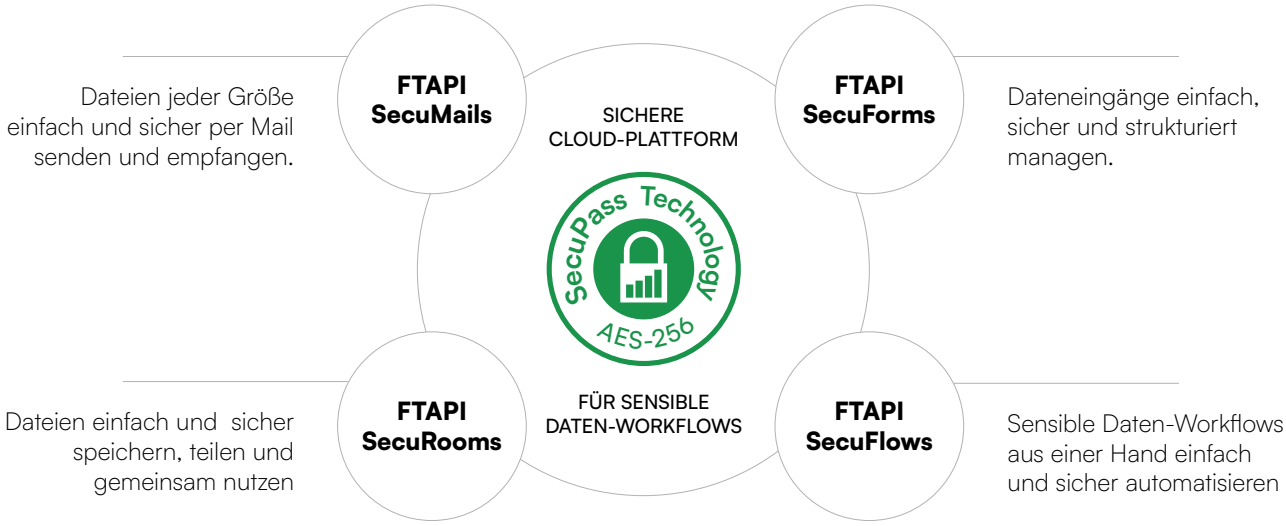
Kosten
Anfallende Kosten müssen transparent und leicht nachvollziehbar sein. Für externen Empfänger:innen dürfen keine Extrakosten oder zusätzlicher Aufwand enstehen.

Compliance
Maximale Compliance und Einhaltung rechtlicher Vorgaben durch Verschlüsselung in mehreren Sicherheitsstufen.

Transparenz durch Zertifizierungen
Zertifizierungen nach ISO beispielsweise zeigen wie hoch der Sicherheitsaspekt gewichtet wird und wie viel Wert das Unternehmen darauf legt den eigenen Anspruch an die Sicherheit auch nach außen zu demonstrieren.

Deutscher Lösungsanbieter
Entwicklung, Support und Hosting in Deutschland sowie ein einsehbarer Kundenstamm sind Grundvoraussetzung für einen glaubwürdige Lösungsanbieter.

Die FTAPI Plattform:
Ein umfangreiches Angebotsspektrum für Ihre Bedürfnisse



Vorteile von FTAPI

Sicherheit und Compliance
Vom sicheren Downloadlink bis hin zur durchgehenden Ende-zu-Ende-Verschlüsselung.

DSGVO-konform
Versenden und empfangen Sie personenbezogene Daten datenschutzkonform und sicher.

Personalisierbarkeit
Passen Sie Farben, Logos und Texte der CI Ihres Unternehmens an und schaffen Sie so Vertrauen.

Einfache Bedienung
Die Nutzung aller unsere Produkte ist leicht verständlich und intuitiv.

Zertifizierungen und Pentest
FTAPI ist ISO-zertifiziert und unterzieht sich jährlich einem unabhängigen Pentest.

Zentrale Administration
Verwalten Sie SecuMails, SecuRooms, SecuForms bzw. SecuFlows inkl. Add-Ons an einer zentralen Stelle

Große Datenmengen
Tauschen Sie auch besonders große Datenmengen sicher und verschlüsselt aus.

Transparenz
Empfangs- und Downlaodbestätigungen machen Ihre Datenaustauschprozesse transparent.

Automatisierungen
Mit FTAPI SecuFlows automatisieren Sie aufwendig manuelle, wiederkehrende Prozesse in Ihrem Untenehmen.