Arno Hitzges, Wolfgang Miedl, Friedemann Reim

Anwenderstudie **Collaboration-Sicherheit 2022**

Microsoft 365 und Collaboration-Risiken: Wie Unternehmen mit neuen Gefährdungs-Szenarien umgehen

Prof. Dr. Arno Hitzges
Wolfgang Miedl
Dr. Friedemann Reim

Anwenderstudie
Collaboration-Sicherheit 2022

Microsoft 365 und Collaboration-Risiken: Wie Unternehmen mit neuen Gefährdungs-Szenarien umgehen

HOCHSCHULE DER MEDIEN

sharepoint 360
Microsoft 365 • Intranet • Collaboration

GBS
Security matters

Bildnachweis

Titel: © simonkr/iStockphoto.com; S. 7: stockchairatgfx/stock.adobe.com

In diesem Buch werden geschlechterspezifische Bezeichnungen (z. B. „der Nutzer“) zur besseren Lesbarkeit nur in einer Form ausgeführt. An dieser Stelle sei angemerkt, dass sich diese in jedem Fall und ausdrücklich auf männliche, weibliche und diverse Personen beziehen. Alle dargestellten Daten, Grafiken und Auswertungen wurden mit entsprechender Sorgfalt erarbeitet. Fehler können jedoch nicht ausgeschlossen werden. Weder der Autor noch der Verlag haften für Schäden durch fehlende Angaben.

Impressum

Autoren & Herausgeber: *Arno Hitzges, Wolfgang Miedl, Friedemann Reim*
Herstellung und Verlag: *SharePoint 360 – Wolfang Miedl, Erding*
Cover Grafik und Satz: *Claudia Wolff*
Tabellen und Auswertungen: *Kardelen Dagli*

Die Autoren

Arno Hitzges
Hochschule der Medien Stuttgart

Prof. Dr. Arno Hitzges ist seit Mai 2011 als Professor für Content-Management-Systeme an der Hochschule der Medien Stuttgart (HdM) tätig. Er begann seine berufliche Laufbahn 1992 am Fraunhofer IAO, wo er den Bereich Information Engineering verantwortete. Seine Arbeiten wurden 1999 mit dem Digiglobe der Deutschen Telekom und der Zeitschrift Focus ausgezeichnet. Er war bis zu seinem Wechsel an die HdM in führenden Management-Positionen bei verschiedenen Microsoft Gold Partnern aktiv und begleitete mehr als 100 Projekte im Bereich Content Management. Er ist Mitherausgeber der SharePoint Anwenderstudien und Initiator des Stuttgarter SharePointForums, der zentralen SharePoint-Anwenderkonferenz im süddeutschen Raum.

Wolfgang Miedl
SharePoint360.de

Wolfgang Miedl ist Gründer und Betreiber des Fachportals SharePoint360.de. Er blickt auf eine langjährige berufliche Erfahrung in der IT-Medienbranche zurück. 1994 begann er als Redakteur beim Marktführer PC-Welt, weitere Stationen waren Internet World, Computerwoche und CIO Magazin. Ab 2003 arbeitete er als selbständiger Autor und Berater Event-Manager für führende Unternehmen der IT-Industrie wie Microsoft, Allianz, SAP, HP und T-Systems. Seit dem Start 2010 konnte er SharePoint360.de inzwischen zum Marktführer im Bereich SharePoint, Office 365 und Digital Workplace ausbauen – mit monatlich rund 30.000 Lesern. Seit 2016 ist er Mitautor der SharePoint Anwenderstudie.

Friedemann Reim
Hochschule der Medien Stuttgart

Dr.-Ing. Friedemann Reim ist seit Mai 2014 als Vertretungsprofessor im Studiengang Online Medien Management an der Hochschule der Medien Stuttgart (HdM) tätig. Er begann seine berufliche Laufbahn nach dem Studium der Informatik in Stuttgart und Atlanta als Software-Entwickler. Am Fraunhofer IAO verantwortete er danach den Bereich Verteilte Informationssysteme. Er war bis zu seinem Wechsel an die HdM in führenden Management-Positionen bei verschiedenen Microsoft Gold Partnern aktiv und begleitete mehr als 100 Projekte im Bereich Dokumentenmanagement und Lernsysteme.

Inhaltsverzeichnis

54 Prozent
der Unternehmen sehen in Hackerangriffen und Datenspionage das größte Cloud-Risiko.

32 Prozent befürchten beim Cloud-Ausfall eine starke geschäftliche Belastung, **22 Prozent** sehen das als unternehmenskritisch.

46 Prozent
steigern die Sicherheit mit Verschlüsselung, **32 Prozent** setzen auf automatisiertes Scannen von Dokumenten.

55 Prozent beugen gegen die „Sicherheitslücke Mensch“ mit Kommunikation vor.

1. Management Summary

Microsoft 365 und Collaboration-Risiken: Wie Unternehmen mit neuen Gefährdungs-Szenarien umgehen

Die IT-Landschaft befindet sich im Wandel, und die Pandemiesituation hat nicht unerheblich dazu beigetragen. Mit dem Home-Office sind neue Arbeitsweisen eingekehrt, welche die IT-Organisationen in den Unternehmen vor ganz neue Herausforderungen stellen. In den Fokus rückt dabei vor allem das Thema Sicherheit, denn beim mobilen und verteilten Arbeiten tauchen auch neue Gefahrenszenarien auf.

Schadsoftware sucht sich neue Wege über Collaboration und die Cloud

Die E-Mail galt bisher als wichtigstes Einfallstor für Schadsoftware in Organisationen aller Art. Doch mit der Nutzung von Collaboration-Apps und Cloud-Speicher verändern sich auch die Angriffsszenarien. Zu zweifelhafter Berühmtheit brachte es dabei in jüngster Zeit die Emotet-Schadsoftware, welche Malware und Erpressungstrojaner in Office-Dokumenten versteckt. Derart manipulierte Dokumente finden ihren Weg in geschäftliche IT-Infrastrukturen klassisch über E-Mail, aber immer öfter auch über Collaboration-Tools sowie Cloud-Speicher wie OneDrive, SharePoint Online und Google Drive.

Unternehmen und Behörden müssen bei der Abwehr von gefährlichen Inhalten neue Wege gehen. Heute verfolgt man dabei oft einen kombinierten Ansatz. Auf der einen Seite kommen ganzheitliche Sicherheitslösungen wie Gateway, E-Mail-Security und Webfilter zum Einsatz, ergänzt durch Anwendertrainings zur Sensibilisierung der Mitarbeiter.

Wie sich Organisationen im deutschsprachigen Raum derzeit beim Thema Sicherheit aufstellen, das ermittelten wir in unserer großen Anwenderbefragung, die wir im April und Mai durchführten. Der Fokus lag dabei auf Unternehmen, die bei der Arbeitsplatz-Infrastruktur auf die Microsoft-Plattform setzen.

Unternehmen fürchten Hackerangriffe und Spionage – aber auch DSGVO-Risiken

Eine zentrale Frage war dabei, welchen Bedrohungsszenarien sich die IT-Abteilungen aktuell mit ihren Cloud-Umgebungen ausgesetzt sehen. An erster Stelle liegen mit 56 Prozent Hackerangriffe und Datenspionage. Die Gefahr von Datendiebstahl folgt an zweiter Stelle mit 49 Prozent, dahinter folgen mit jeweils 39 Prozent die Angst vor Ransomware und Vireninfektionen. Als nicht unerhebliches Geschäftsrisiko sehen die Anwender auch die strengen Compliance-Regularien beim Cloud-Einsatz. 46 Prozent sehen die mögliche Verletzung von DSGVO-Vorschriften als Risiko. (Mehrfachnennungen möglich)

Cloud-Ausfälle bedrohen vielerorts den Geschäftsbetrieb

Der Umstieg auf Cloud-Infrastrukturen kam im deutschsprachigen Raum nur langsam in Fahrt. Doch spätestens mit dem Einsatz von Microsoft Teams während der Pandemiephase gehören gehostete Lösungen fast überall zum Portfolio. Mit dieser Entwicklung gehen allerdings auch neue Abhängigkeiten einher. Befragt nach den Auswirkungen eines Cloud-Ausfalls gehen 22 Prozent davon aus, dass bei einem eintägigen Ausfall erheblichen Schäden auftreten. 54 Prozent stufen das reibungslose Funktionieren der Cloud als unternehmenskritisch ein beziehungsweise rechnen bei Ausfall mit starken Belastungen. (Mehrfachnennungen möglich)

Geht man etwas tiefer ins Detail und fragt nach den Maßnahmen, mit denen sich Organisationen schützen, dann setzt fast die Hälfte der befragten Unternehmen (46 Prozent) auf Datenverschlüsselung beziehungsweise eine zentrale Verwaltung von Sicherheitsrichtlinien. Rund ein Drittel scannt die über E-Mail und andere Kanäle eingehenden Dateien mit den integrierten Tools, ein Viertel verwendet dafür zusätzliche Drittanbieter-Scanner.

Der Faktor Mensch bleibt ein großes Risikomoment

Auch die ausgefeiltesten Sicherheits-Tools helfen natürlich nicht gegen den Faktor Mensch. Um fatale Fehler auf Seiten der Mitarbeiter zu verhindern, sensibilisieren 46 Prozent der befragten Unternehmen ihre Mitarbeiter in Sachen Cyberrisiken, 55 Prozent propagieren über kommunikative Maßnahmen richtiges Verhalten. Lediglich 16 Prozent verlassen sich ausschließlich auf die technische Sicherheitsinfrastruktur. (Mehrfachnennungen möglich)

Ganz neue Herausforderungen erwachsen der IT-Sicherheit aus der Ausweitung des digitalen Arbeitsplatzes bis in die private Sphäre des Home-Office. Deutlich wird diese Problematik an der Frage nach der Nutzung privater Endgeräte. Nur noch 36 Prozent verwenden ausschließlich die vom Unternehmen bereitgestellten Geräte, 56 Prozent nutzen zumindest gelegentlich Privatgeräte für geschäftliche Aufgaben.

Microsoft-Sicherheit genießen Ansehen, doch der Bedarf an Zusatz-Tools ist hoch

Wie gut fühlen sich die Organisationen bei all diesen Herausforderungen von ihrem wichtigsten Plattformlieferanten Microsoft unterstützt? Grundsätzlich lässt sich ein hohes Vertrauensniveau feststellen. 41 Prozent vertrauen auf die integrierten Schutzmechanismen, weitere 41 Prozent erachten die Plattform grundsätzlich als sicher, sehen aber die Notwendigkeit für Drittanbieter-Ergänzungen. 18 Prozent stufen die Microsoft-Basis als nicht ausreichend sicher ein oder zweifeln gar an den eingebauten Schutzfunktionen.

Gelangen Unternehmen zu der Erkenntnis, dass offene Flanken wie Collaboration existieren, übergibt man die Zugangskontrolle in der Regel an die IT-Abteilung. Oder aber man schränken deren Nutzungsmöglichkeiten ein, wodurch aber auch die Flexibilität aus Nutzersicht leidet. Viele Unternehmen gehen aus diesem Grund dazu über, den Basisschutz von Microsoft 365 um zusätzliche Sicherheitslösungen zu ergänzen. Aus Kosten- und Komplexitätsgründen werden diese jedoch noch nicht flächendeckend eingesetzt.

2. Ausgangssituation und Zielsetzung der Studie

Digitale Arbeitsumgebungen verbunden mit Home Office und Remote Working erfordern moderne Collaboration Technologien. Kollaborations-Plattformen wie beispielsweise Microsoft 365 oder Google Workspace erleben einen Boom. Mehr und mehr Informationen werden Online über diese Plattformen verfügbar.

Mit der Verbreitung dieser Plattformen wird Cyber Security immer wichtiger. Die Zahl der sicherheitsrelevanten Vorfälle in den Unternehmen steigt. In der Presse wird regelmäßig darüber berichtet. Darüber hinaus vermutet Experten eine hohe Dunkelziffer.

Die Unternehmen haben erkannt, dass Maßnahmen zur Planung, Ausführung und Überwachung der Sicherheit hohe Priorität besitzen müssen. Zugleich handelt es sich um eine komplexe Aufgabe.

Zielsetzung der hier vorliegenden Studie ist es, die Aktivitäten und Einschätzungen der Unternehmen in diesem Themenfeld aufzunehmen. Der Fokus liegt auf dem Risk Assessment für Collaboration Plattformen und technischen Lösungsansätzen, die in den Unternehmen verfolgt werden.

3. Situationsbestimmung und Bedürfnisse der Unternehmen im Bereich Cyber Security

Die Pandemiesituation hat Unternehmen vor große Herausforderungen bei der Cyber Security gestellt. Viren, Trojaner, Ransomware, Social Engineering – die Bedrohungen sind vielfältig. Diese Gefahren gab es selbstverständlich bereits zuvor. Die Verlagerung von Arbeitsplätzen ins Home-Office hat die Dringlichkeit zur Sicherung der IT aber erhöht.

Remote Work erfordert Kollaboration und Informationsbereitstellung in vernetzten Umgebungen. Die zugrundeliegenden IT-Plattformen zeigen entsprechend große Wachstumsraten. Wie sicher sind sie? Welche Maßnahmen ergreifen die Unternehmen?

Von staatlicher Seite gibt das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de) viele Hinweise und Empfehlungen. Die vorliegende Studie untersucht die Cyber Security spezifisch bezogen auf IT-Plattformen, insbesondere Microsoft 365. Wie schätzen die Unternehmen bei diesen Plattformen die Bedrohungssituation ein? Welche Maßnahmen werden ergriffen?

3.1. Microsoft Teams ist die führende Kollaborations-Plattform, vor SharePoint und OneDrive

Welche Kollaborations-Plattformen kommen bei den Teilnehmern unserer Studie zum Einsatz? Den Löwenanteil nimmt Microsoft ein, mit Teams, das wenig überraschend mit 81 Prozent die Führungsposition einnimmt. SharePoint folgt mit 67 Prozent, gefolgt von 55 Prozent mit OneDrive-Nutzung. Mehrfachnennungen waren möglich.

Die Umfrage beansprucht an diesem Punkt allerdings keine repräsentative Aussagekraft, da ein Teil des Adressatenkreises aus Teilnehmern verschiedener Veranstaltungen zu Microsoft-Technologien besteht.

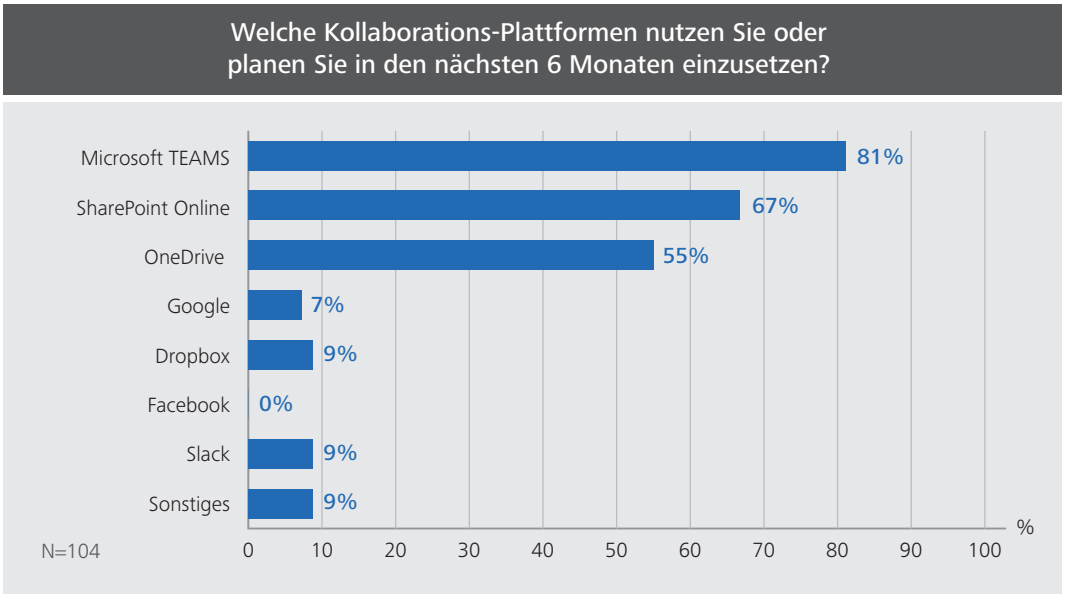

Abbildung 1: Welche Kollaborations-Plattformen nutzen Sie oder planen Sie in den nächsten 6 Monaten einzusetzen?

3.2. Die Cloud genießt heute ein hohes Vertrauen als sichere IT-Umgebung

Die Nutzung von Cloud-Systemen für geschäftliche IT-Lösungen nahm in den vergangenen Jahren stetig zu. Dabei ist ein gewisser Sonderweg im deutschsprachigen Raum zu berücksichtigen, mit einer anfänglich zögerlichen Akzeptanz für extern gehostete Anwendungen. Die Gründe dafür sind vielfältig, wobei Themen wie Sicherheit und Datenschutz eine starke Rolle spielen.

Inzwischen ist das Vertrauen in Cloud-basierende IT-Systeme stark gewachsen, was in den Antworten zur zweiten Frage deutlich zu erkennen ist. 71 Prozent der Studienteilnehmer fühlen sich bei der Nutzung ihrer Cloud-Umgebung gut bis sehr gut geschützt, als mittelmäßig stufen es 29 Prozent ein. Eine negative Bewertung gab keiner der Teilnehmer ab.

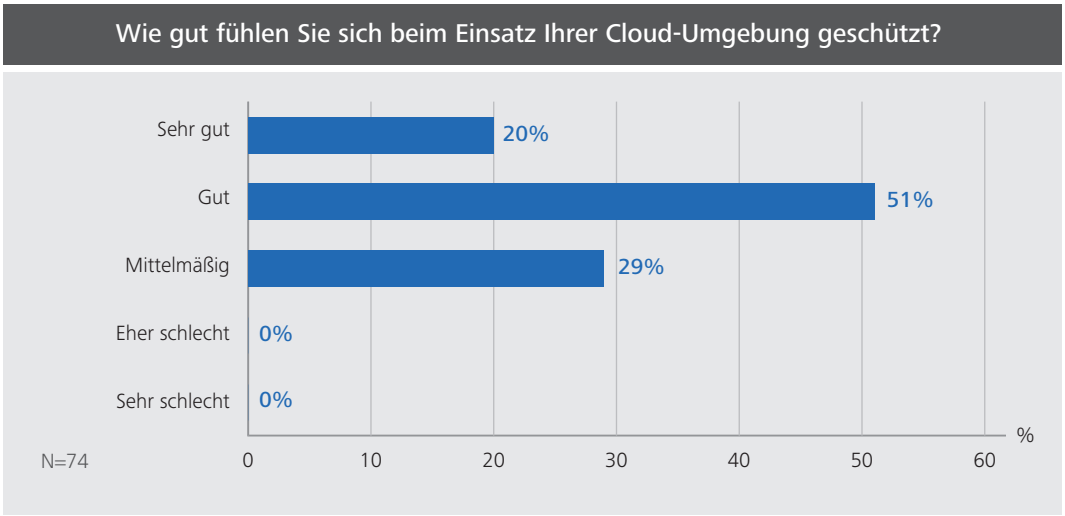

Abbildung 2: Wie gut fühlen Sie sich beim Einsatz Ihrer Cloud-Umgebung geschützt?

3.3. Komplexität von Cyber-Security-Lösungen hält Unternehmen vom Ausbau ab

In der Debatte um die Sicherheit von Cloud-Umgebungen führen die Anbieter als wichtiges Argument ihr Knowhow für Schutzmaßnahmen ins Feld. Die immer ausgefuchsteren Arten von Angriffen und Schadsoftware erschweren es vor allem kleineren Unternehmen, sich selber um den Schutz der geschäftlichen Anwendungen zu kümmern.

Wenn es um den weiteren Ausbau des Basis-Schutzes der Cloud geht, sind drei signifikante Hinderungsgründe zu verzeichnen. 22 Prozent sind zufrieden mit den Cyber-Security-Maßnahmen der Cloud-Anbieter und sehen keinen Erweiterungsbedarf. Für 40 Prozent ist die Komplexität bei der Einführung weiterer Lösungen zu hoch. Und 23 Prozent nennen als Hinderungsgrund die Kosten für zusätzliche Tools.

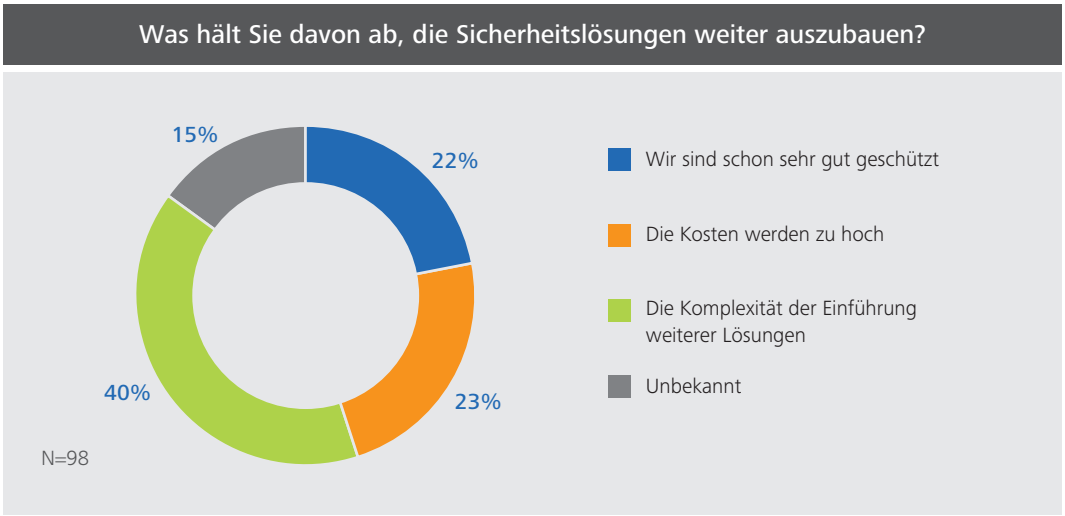

Abbildung 3: Was hält Sie davon ab, die Sicherheitslösungen weiter auszubauen?

3.4. Welche organisatorischen Maßnahmen sind notwendig, welche stören die Produktivität?

Informationssicherheit beginnt in kollaborativen Arbeitsumgebungen bei organisatorischen Vorkehrungen – noch vor allen technischen Maßnahmen. Denn bekanntlich gilt der Mensch als zentrales Sicherheitsrisiko.

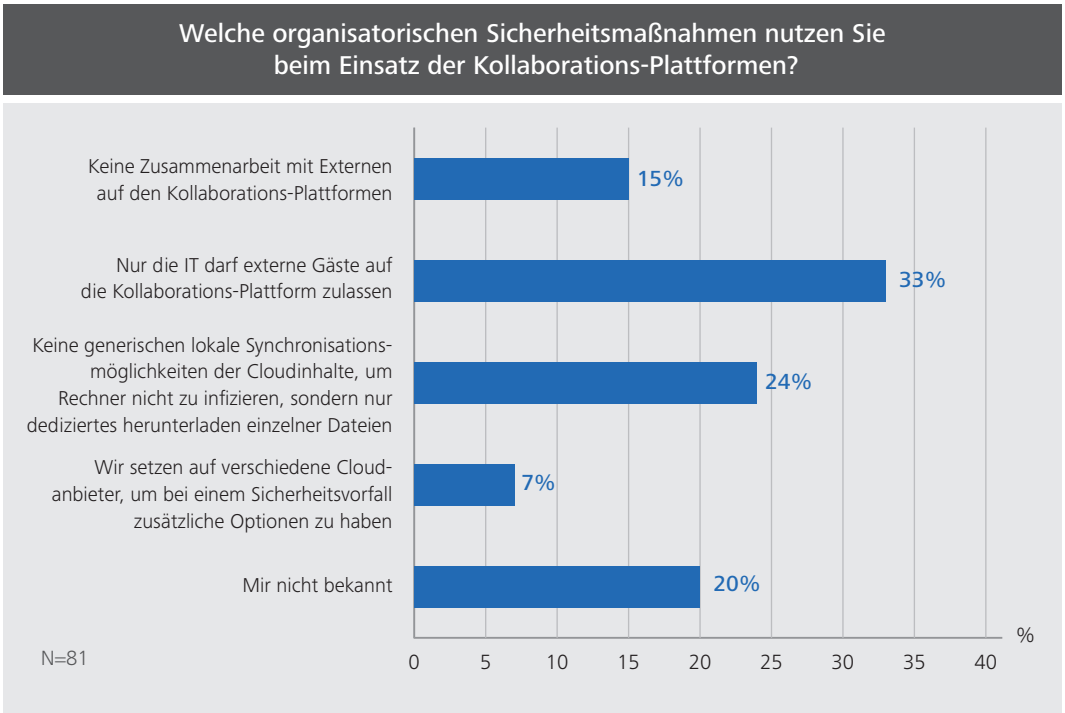

Abbildung 4: Welche organisatorischen Sicherheitsmaßnahmen nutzen Sie beim Einsatz der Kollaborations-Plattformen?

Entsprechend interessant ist die Frage, welche organisatorischen Sicherheitsmaßnahmen in den Unternehmen zum Einsatz kommen. Bei einem Drittel der Befragten ist die IT dafür zuständig, um externe Teilnehmer in kollaborative Anwendungen zuzulassen. Ein solcher administrativer Umweg steigert allerdings den Koordinationsaufwand und dürfte zu höherer Arbeitsbelastung führen.

Weitere 15 Prozent schließen Zusammenarbeit mit Externen generell aus. Vom Sicherheitsgedanken her ist das eine konsequente Maßnahme, die jedoch mit der Idee der digitalen Zusammenarbeit kollidiert.

Eine weitere verbreitete Maßnahme betrifft das Unterbinden der Datei-Synchronisierung mit lokalen Endgeräten, die bei einem Viertel der Befragten (24 Prozent) zum Einsatz kommt. Auch hier ist ein Zielkonflikt unvermeidbar. So lässt sich zwar die Gefahr von

Angriffen über infizierte Office-Dateien stark reduzieren. Eine solche Funktionsbeschränkung erkauft man sich allerdings mit Produktivitätsverlusten. Ohne Offline-Dateien kann nämlich das mobile Arbeiten nicht überall sichergestellt werden.

In 20 Prozent der Unternehmen ist nicht bekannt, welche organisatorischen Sicherheitsmaßnahmen angewandt werden. Eventuell liegen hier einfach Defizite in der Kommunikation vor, wie das die folgende Frage thematisiert. Eine weitergehende Recherche hierzu wäre interessant.

3.5. Die Sicherheitslücke Mensch wird mit Schulungen und fortlaufender Kommunikation eingehegt

Die Sicherheitslücke Mensch ist so alt wie die IT selbst. Zwar wurden und werden immer ausgefeiltere Sicherheitstechniken entwickelt, um menschliches Fehlverhalten als schädigenden Faktor so gut wie möglich zu eliminieren. Doch stößt die Technik dabei immer wieder an ihre Grenzen.

Das begrenzte Vertrauen in die Technik spiegelt sich in der Frage nach dem Schutz gegen die menschliche Sicherheitslücke wider. Nur 16 Prozent vertrauen hier auf rein technische Maßnahmen.

Mehr als die Hälfte, nämlich 55 Prozent setzen auf eine kontinuierliche Kommunikation des richtigen Verhaltens. Fast jedes zweite Unternehmen, immerhin 46 Prozent, führt Schulungen für sicherheitsbewusstes Verhalten der Mitarbeiter durch.

Ziel von Kommunikations- und Schulungsmaßnahmen ist, das Bewusstsein für die verschiedenen Bedrohungsszenarien bei den Mitarbeitern zu schärfen. Dass dieses Ziel durchaus erreicht wird, zeigt die folgende Frage.

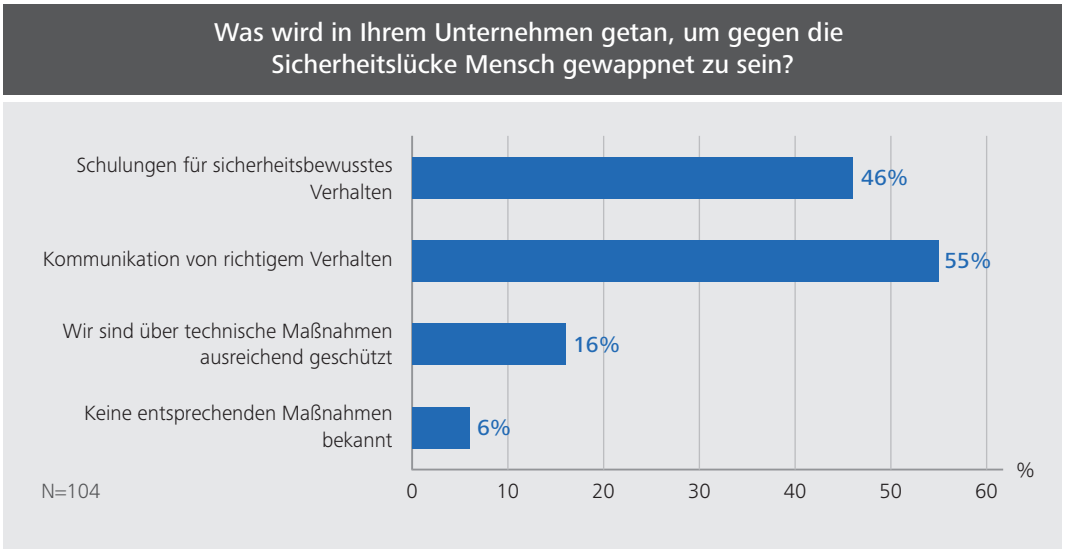

Abbildung 5: Was wird in Ihrem Unternehmen getan, um gegen die Sicherheitslücke Mensch gewappnet zu sein?

3.6. Sensibilität für vielfältige Bedrohungsszenarien ist vorhanden – vom Datenspionage bis Ransomware

Eingangs ging es bereits um die Frage der allgemeinen Sicherheitseinstufung von Cloud-Plattformen. Mit welchen konkreten Angriffspunkten und Schadensszenarien die Unternehmen tatsächlich im Geschäftsalltag konfrontiert sind, schlüsselt diese Frage auf.

An erster Stelle bei den aktuellen Risiken in Public Clouds stehen mit 54 Prozent der Nennungen Hackerangriffe und Spionage, gefolgt von Datendiebstahl mit 49 Prozent.

Beim Themenkomplex DSGVO handelt es sich um anders gelagerte Risiken, die allerdings nicht minder großem Schadenspotenziale für Unternehmen bergen. 46 Prozent sehen das als Problemfeld.

Ein enormes Risiko bilden außerdem infizierte Dateien, welche von Externen oder Internen hochgeladen oder lokal synchronisiert werden. Schließlich gelten Dokumente über E-Mail oder Collaboration-Apps als Haupteinfallstor, über die Ransomware und anderer Schadcode in die Unternehmen gelangt.

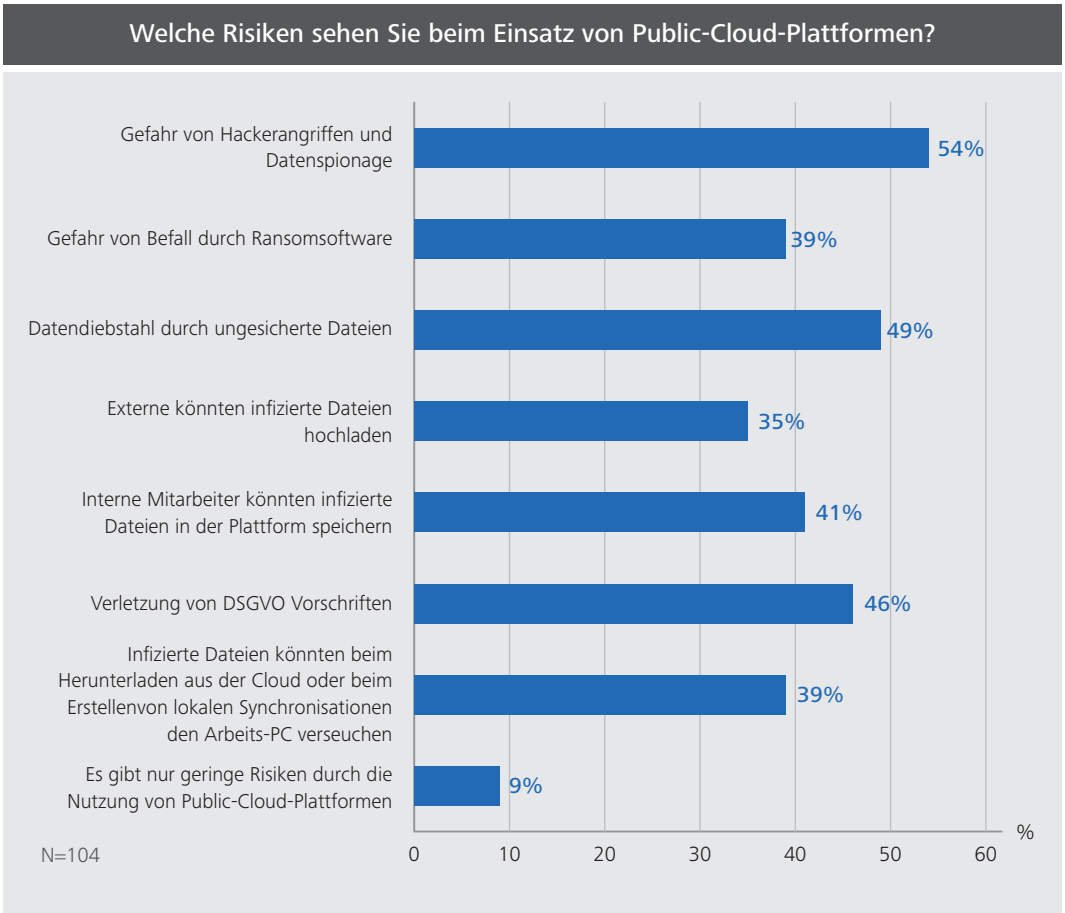

Abbildung 6: Welche Risiken sehen Sie beim Einsatz von Public-Cloud-Plattformen?

3.7. Die Cloud-Verfügbarkeit gilt heute oft als unternehmenskritisch

Die Pandemiesituation hat die meisten Unternehmen vor neuartige IT-Herausforderungen gestellt. Insbesondere die Verlagerung von Büroarbeitsplätzen ins Home-Office macht sich als einschneidende Veränderung bemerkbar.

In dieser Situation spielten Kollaborations-Apps wie Microsoft Teams oder Slack eine herausragende Rolle. Daneben wirkt sich Remote Work aber auch auf weitere Anwendungsbereiche aus, von der Informationsbereitstellung bis zu betriebswirtschaftlichen Applikationen.

Dabei gilt es von der technischen Seite her, veränderte Prozesse zu unterstützen, während sich die Mitarbeiter bei ihrer Arbeitsorganisation teilweise komplett umorientieren müssen.

Entsprechend wichtig ist dabei die Verfügbarkeit der Cloud-Plattform, denn Ausfälle führen unter diesen veränderten Rahmenbedingungen zu größeren betrieblichen Beeinträchtigungen.

In der Befragung stufen 22 Prozent das Funktionieren der Cloud als unternehmenskritisch ein, 32 Prozent rechnen bei einem Ausfall mit einer starken Belastung, weitere 22 Prozent rechnen bei einem eintägigen Ausfall mit einem erheblichen Schaden.

Gelassen begegnet ein knappes Viertel (23 Prozent) dieser Problematik, weil man entweder keine kritischen Daten in der Cloud speichert oder Ausfalllösungen bereithält.

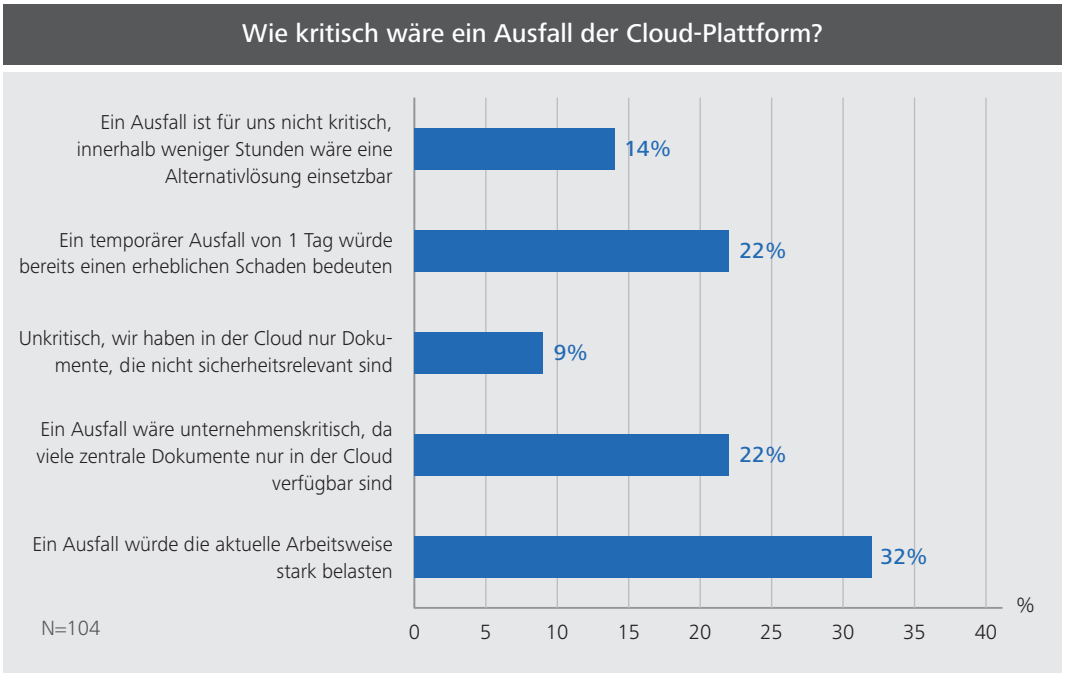

Abbildung 7: Wie kritisch wäre ein Ausfall der Cloud-Plattform?

3.8. Europäische Cloud-Anbieter werden bevorzugt

Das Thema Cloud-Bereitstellung bleibt für Anwender im deutschsprachigen Raum weiter wichtig. 86 Prozent bevorzugen eine europäische Cloud-Plattform, nur 14 Prozent erachten dieses Kriterium als unwichtig.

Der Grund dürfte vor allem in den höheren europäischen Datenschutzstandards sowie der Zugriff von US-amerikanischen Sicherheitsbehörden auf Daten im Rahmen des Cloud- und Patriot-Acts liegen.

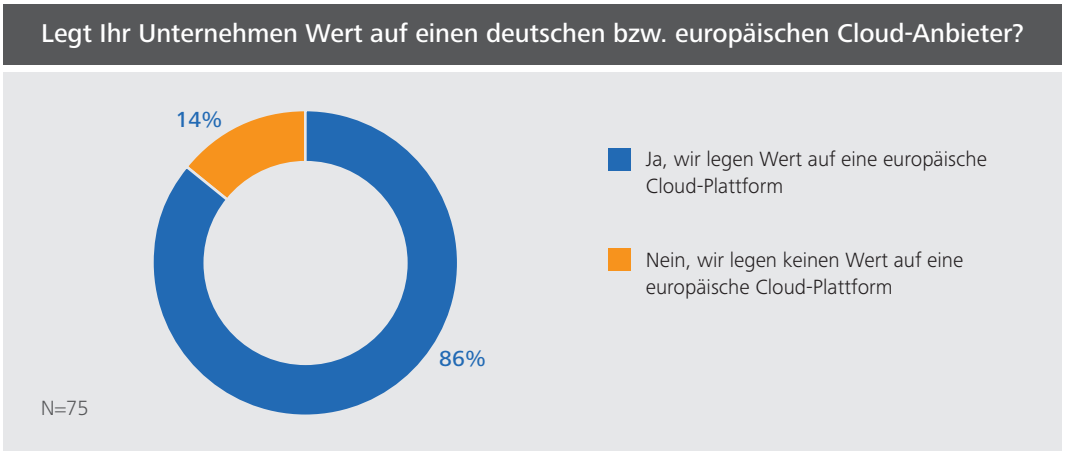

Abbildung 8: Legt Ihr Unternehmen Wert auf einen deutschen bzw. europäischen Cloud-Anbieter?

3.9. Rechtliche Rahmenbedingungen als Hauptkriterium für europäische Cloud-Anbieter

Diese Annahme bestätigt die folgende Fragestellung. Als ausschlaggebendes Risiko für die Standortwahl des Cloud-Anbieters wird Datenschutz und DSGVO-Compliance genannt. Immerhin 27 Prozent sehen auch den Umgang mit sensiblen Daten als wesentliches Auswahlkriterium.

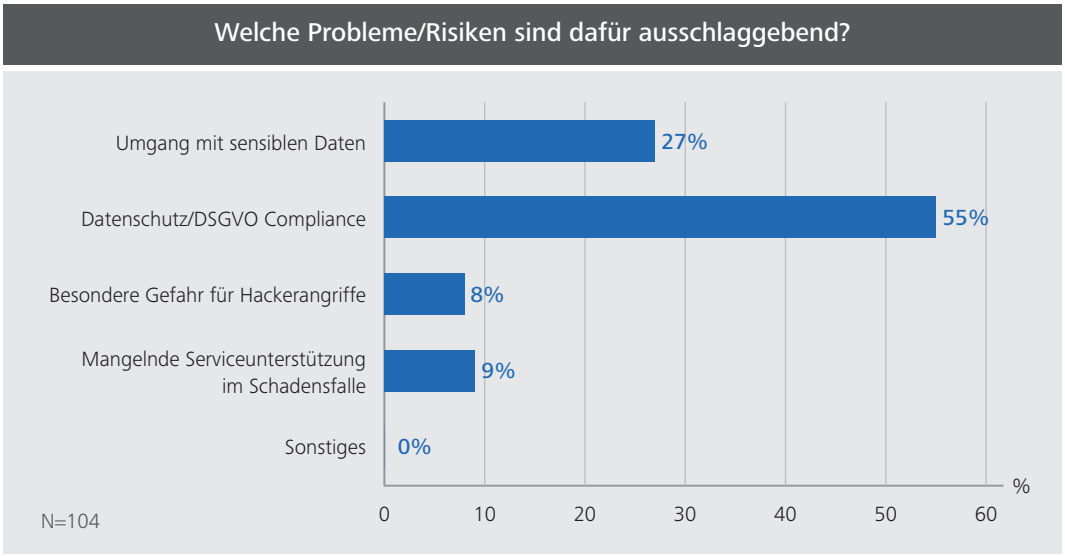

Abbildung 9: Welche Probleme/Risiken sind für die Standortwahl der Cloud-Plattform ausschlaggebend?

3.10. Hohes Vertrauen in Microsofts Sicherheitsfunktionen, aber großer Bedarf an Zusatzlösungen

Wie steht es um die Sicherheitskompetenz beim größten Anbieter für Kollaborations-Lösungen, Microsoft? Die Redmonder genießen auf diesem Gebiet einen guten Ruf und erzielen solide Vertrauenswerte.

In der Umfrage bescheinigten 41 Prozent der Microsoft-Cloud-Plattform, dass sie einen soliden Schutz bietet. Die zweite Gruppe mit ebenfalls 41 Prozent sieht Microsoft ebenfalls gut aufgestellt, hält aber die Ergänzung durch Drittanbieter-Tools für wichtig.

11 Prozent sind der Ansicht, dass Microsoft keine ausreichenden Schutzfunktionen bietet, und 7 Prozent vertrauen nicht auf die Schutzmechanismen von Microsoft.

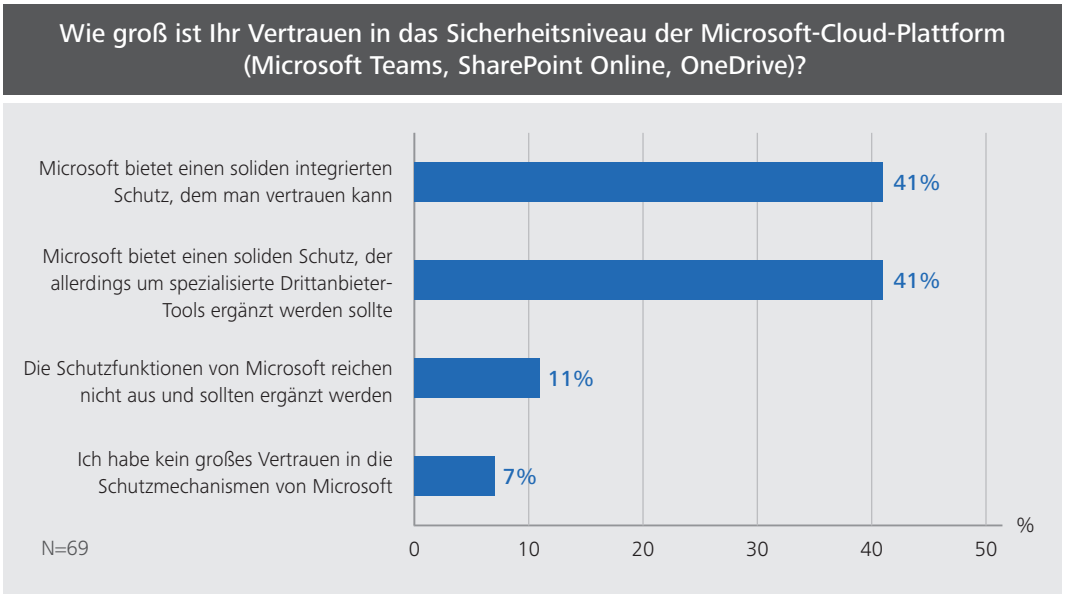

Abbildung 10: Wie groß ist Ihr Vertrauen in das Sicherheitsniveau der Microsoft-Cloud-Plattform (Microsoft Teams, SharePoint Online, OneDrive)?

3.11. Die Verwendung von Privatgeräten nimmt zu – und damit steigen die Herausforderungen an die Sicherheit

IT-Sicherheit ist auch eine Frage der verwendeten Endgeräte und deren Absicherung. Im Zuge von Remote Work und Home-Office hat sich der Trend zur Nutzung von Privatgeräten verstärkt, ebenso die Anbindung aus verschiedensten externen Netzwerken. Die Grenzen zwischen privat und dienstlich verschwimmen immer mehr, was für die IT-Administratoren ist eine wachsende Herausforderung darstellt.

Da die Nutzung von privaten Geräten zusätzliche Sicherheitsrisiken mit sich bringt, stellt sich für Unternehmen die Frage, ob und wie sie die Nutzung von Privatgeräten erlauben.

Wie die Umfrage zeigt, wird der Slogan „Bring your own device“ im Geschäftsalltag zunehmend Realität. 56 Prozent der Teilnehmer geben an, dass für die Arbeit ab und zu private Geräte verwendet werden. Nur mehr gut ein Drittel, nämlich 36 Prozent antworten, dass sie für die Arbeit nur Firmengeräte verwenden. 7 Prozent geben an, dass sie Microsoft 365 nicht verwenden.

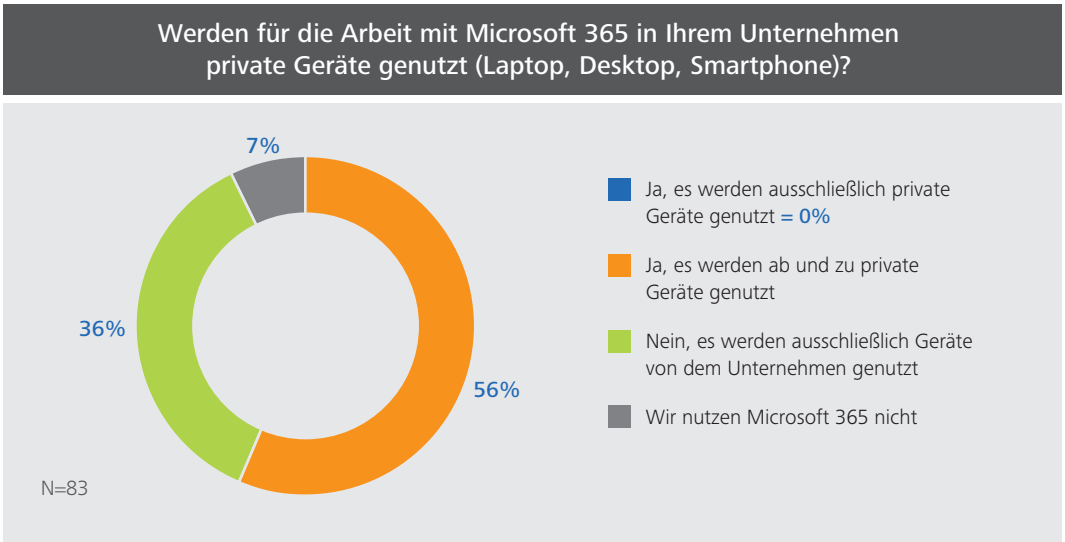

Abbildung 11: Werden für die Arbeit mit Microsoft 365 in Ihrem Unternehmen private Geräte genutzt (Laptop, Desktop, Smartphone)?

3.12. Verschlüsseln und Scannen – was Unternehmen zur Steigerung der Sicherheit unternehmen

Wie schützen sich Unternehmen gegen mögliche Angriffe und Schadsoftware in Cloud-Umgebungen? Unter Cloud wird dabei mehr verstanden als die vorgenannten Kollaborationsplattformen. Auch E-Mail-Server und Archive gehören beispielsweise dazu. Als beliebte Schutzmaßnahme kommt bei 46 Prozent eine Datenverschlüsselung zum Einsatz. Ebenfalls 46 Prozent verwalten ihre Sicherheitsrichtlinien zentral.

Knapp ein Drittel, nämlich 32 Prozent setzen auf das automatische Scannen von in die Cloud übertragenen Dateien, und zwar mit dem integrierten Virenscanner des Cloud-Anbieters. 26 Prozent setzen auf erweiterte Sicherheitsmaßnahmen, indem sie das automatische Scannen von hochgeladenen Dateien mit mehreren Virenscannern durchführen. Diese Strategie hilft, Schwachstellen einzelner Anbieter auszuschließen.

Nur eine kleine Gruppe von 16 Prozent wählte die Verlagerung sensibler Daten in die private Cloud als Lösung, und 13 Prozent setzen aus DSGVO-Gründen auf die private Cloud.

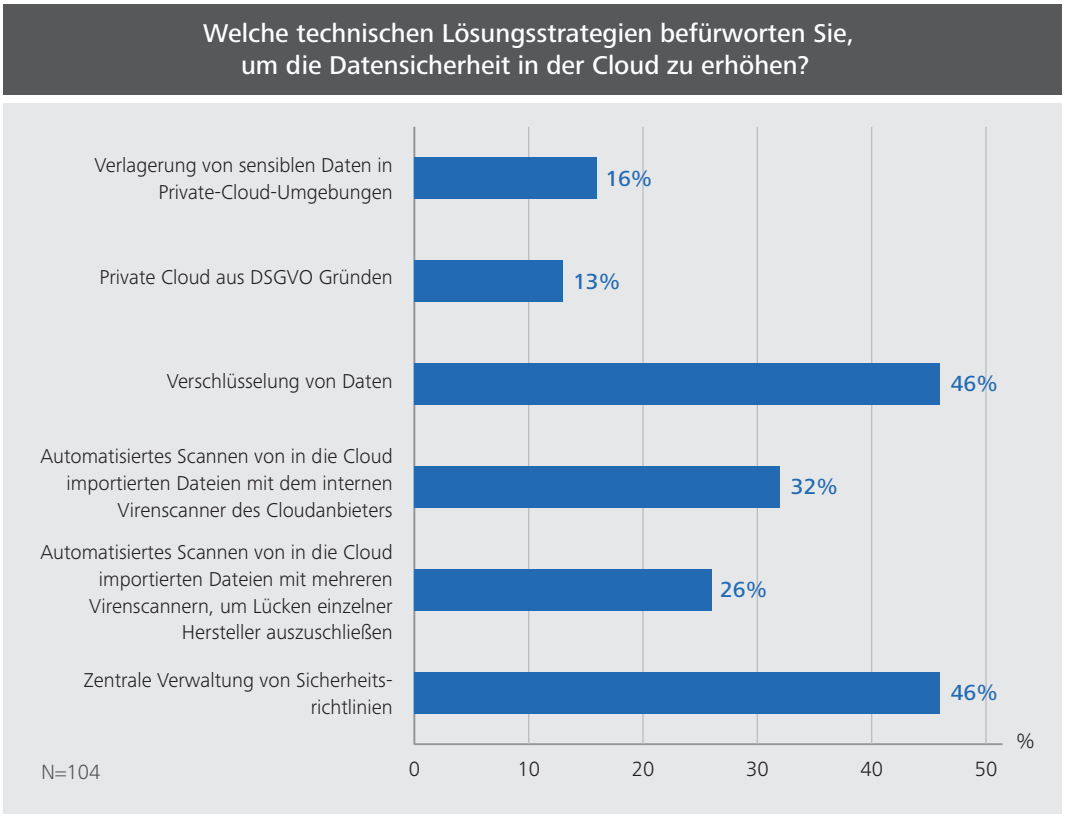

Abbildung 12: Welche technischen Lösungsstrategien befürworten Sie, um die Datensicherheit in der Cloud zu erhöhen?

3.13. Microsofts Sicherheits-Tools sind vielen entweder zu komplex oder zu teuer

Microsoft bietet inzwischen ein breites Portfolio an Sicherheitswerkzeugen an. Wem der integrierte Basisschutz hier nicht ausreicht, der kann vielzählige zusätzliche Angebote dazubuchen. Dennoch wollen sich viele Unternehmen nicht allein auf Microsoft verlassen, und zwar aus unterschiedlichen Gründen.

So beurteilen in unserer Umfrage 29 Prozent die Microsoft-Lösung als zu komplex bei der Einrichtung. Weitere 29 Prozent nennen hohe Kosten als Hinderungsgrund.

Fehlende Lizenzierungspläne halten 23 Prozent davon ab, auf Microsoft zu setzen. Vielfach dürfte man diese Stimmen dem Kostenthema zuschlagen können, da erweiterte Lizenzen auch eine Steigerung der Kosten bedeuten.

Nicht zu vernachlässigen ist auch der Anteil von 17 Prozent, der potenzielle DSGVO-Konflikte mit amerikanischen Anbietern als Show-Stopper nennt. Trotz europäischer Standorte bleibt Microsoft in vielen geschäftlichen Bereichen ein US-Anbieter, dem manche mit Vorsicht begegnen.

Lediglich bei drei Prozent spricht eine Multi-Cloud-Strategie gegen den Einsatz von Microsoft-Sicherheits-Tools.

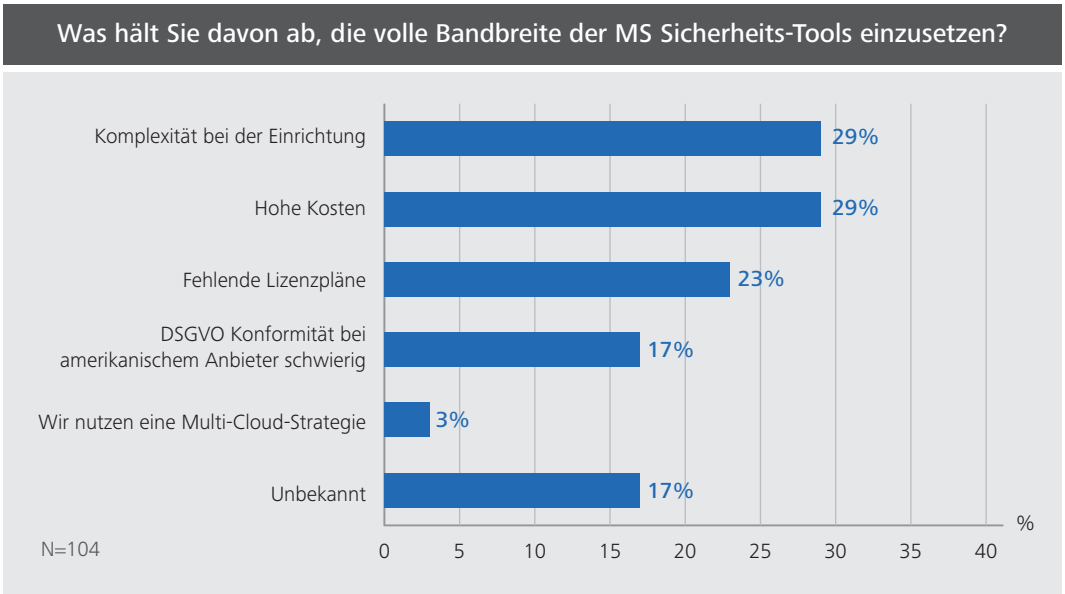

Abbildung 13: Was hält Sie davon ab, die volle Bandbreite der MS Sicherheits-Tools einzusetzen?

4. Methodik und Herkunft der Teilnehmer

Die vorliegende Studie zeigt die aufbereiteten Ergebnisse einer explorativen Umfrage zum Thema Cyber Security.

Die Teilnehmer kommen aus dem deutschsprachigen Raum (DACH-Region). Sie wurden über E-Mail-Newsletter, Blog-Posts und Mailings von Anwendergruppen und Beratungsunternehmen auf diese Umfrage aufmerksam gemacht.

Die Ergebnisse geben einen Überblick über die aktuelle Situation, sind aber nicht repräsentativ für die untersuchte Region.

Der Fragebogen wurde im gesamten Umfragezeitraum (Mitte Mai 2022 – Mitte Juni 2022) 132 Mal aufgerufen. Für Online-Fragebögen typisch ist unter der Gesamtzahl der Befragten eine Teilmenge, die die Fragen unvollständig oder gar nicht beantwortet haben. Unvollständige Antworten oder übersprungene Fragen werden aus der Grundgesamtheit herausgefiltert, was die Lesbarkeit der Statistiken verbessert. Die Grundgesamtheit bezogen auf die jeweilige Frage wird in den Diagrammen gesondert ausgewiesen. Der Großteil der Fragen gehört zur Gruppe der Pflichtfragen, nur ein kleiner Teil der Fragen ist freiwillig. Insgesamt haben 104 Teilnehmer alle Pflichtfragen vollständig beantwortet.

Zunächst gilt es die gewählte Stichprobe der Befragung zu ermitteln. Dazu wurden folgende Fragen gestellt:

1. Wie viele Mitarbeiter sind aktuell in Ihrem Unternehmen beschäftigt?
2. In welcher Branche ist Ihr Unternehmen tätig?
3. Welche Position bzw. welches Aufgabengebiet haben Sie in Ihrem Unternehmen inne?

Es kann nicht ausgeschlossen werden, dass mehrere Teilnehmer desselben Unternehmens an der Befragung teilgenommen haben. Allerdings gehen wir – aufgrund der ursprünglichen Datenbasis, der per E-Mail verteilten Fragebögen davon aus, dass dies nur in sehr seltenen Fällen geschehen ist.

4.1. Unternehmensgröße und Branchenzugehörigkeit

Die meisten der 104 Teilnehmer arbeiten in Unternehmen mit bis zu 500 Beschäftigten. 38 Prozent arbeiten in Unternehmen mit 1 bis 249 Beschäftigten, 6 Prozent in Unternehmen mit mehr als 5000 Beschäftigten.

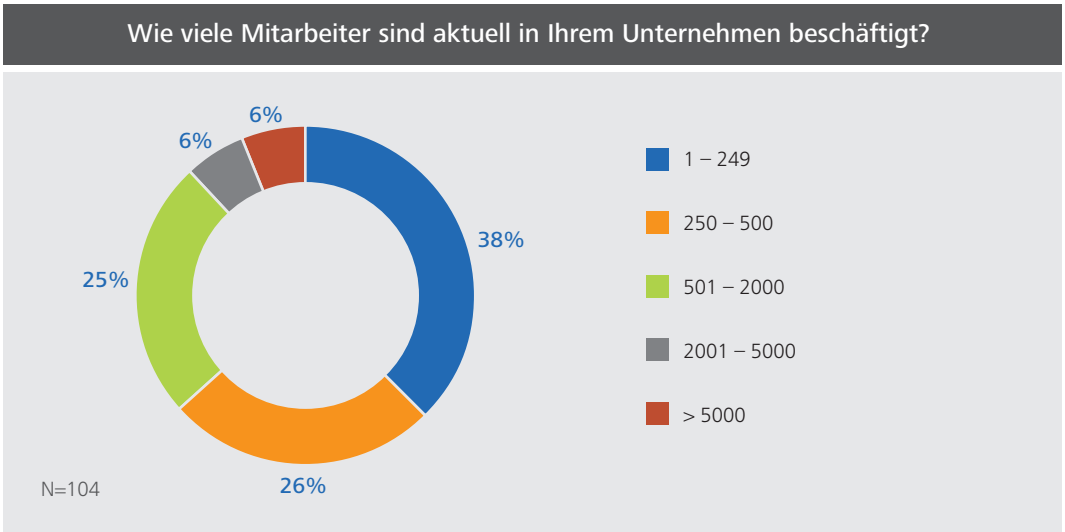

Abbildung 14: Teilnehmer – Unternehmensgröße

Bezüglich der Branchen kommen 28 Prozent der Teilnehmer aus dem IT-Umfeld, 29 Prozent aus der Industrie. Banken und Versicherungen stellen mit 12 Prozent eine signifikante Teilgruppe der Befragten. Dienstleistungen sind mit 7 Prozent, Medizin und Pharma mit 3 Prozent und Handel mit 2 Prozent vertreten.

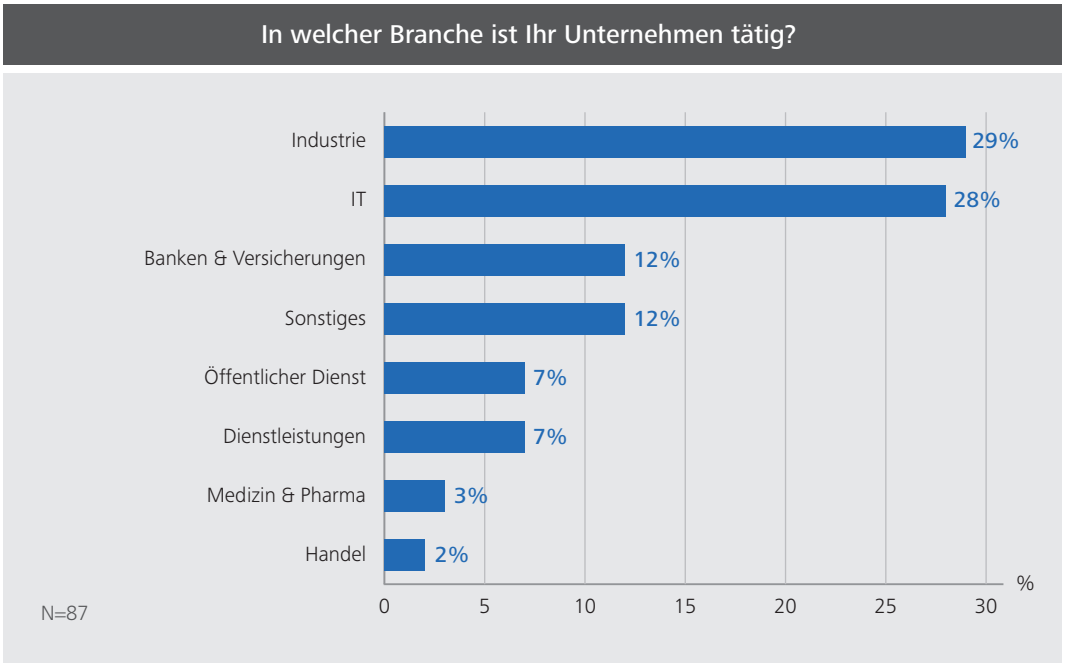

Abbildung 15: Teilnehmer – Branchenzugehörigkeit

Betrachtet man die Positionen und Abteilungen der Teilnehmer, so sind 44 Prozent im IT-Bereich ihres Unternehmens tätig, 23 Prozent bezeichnen sich als IT-Führungskraft. Im Bereich Geschäftsführung arbeiten 15 Prozent, 17 Prozent kommen aus Fachbereichen.

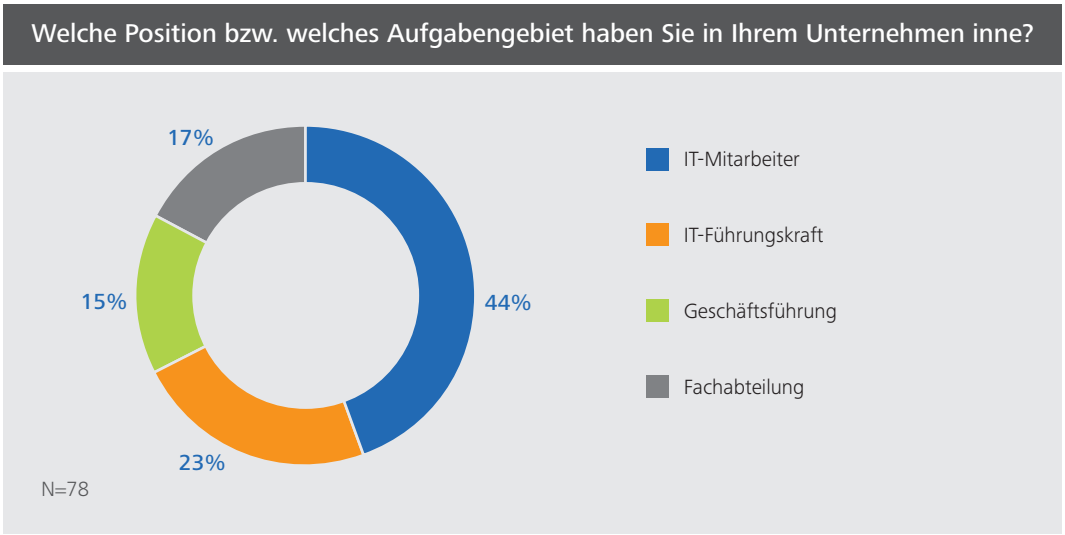

Abbildung 16: Teilnehmer – Aufgabenbereich im Unternehmen

Gegenüber früheren Umfragen ist besonders der hohe Anteil an IT-Fachkräften inklusive der Führungskräfte auffallend. Cyber Security ist ein Expertenthema.

Abbildungsverzeichnis

Partner

GBS

GBS ist ein anerkannter Anbieter von E-Mail- und Collaboration-Sicherheitslösungen in Deutschland, mit fast 30 Jahren Erfahrung in den Bereichen Datenschutz, Produktivität und Compliance. Das Unternehmen wird von namhaften Marktforschern in Deutschland und von seinen Partnern als führendes Unternehmen für Cybersicherheitslösungen anerkannt, mit Schwerpunkt in den Bereichen Data Loss Prevention und Collaboration Sicherheit.

GBS bietet umfangreiche Lösungen der nächsten Generation für E-Mail-Produktivität, Compliance sowie einen mehrstufigen Schutz bei der E-Mail-Kommunikation und Datenaustausch über verschiedene Collaboration-Plattformen gegen alle Arten von Sicherheitsbedrohungen. Die Lösungen für Microsoft 365, Exchange und HCL Domino sind einfach zu bedienen, flexibel und decken Schlüsselbereiche wie Malware-Schutz, Verschlüsselung, E-Mail-Produktivität, Datenverluste, Workflow und Compliance ab.

Die Lösungen von GBS schützen mehr als 2 Millionen Endbenutzer weltweit. Das Unternehmen hat langjährige Beziehungen zu über 2.000 Kunden aufgebaut.

Kontakt:
GBS Europa GmbH
expert@gbs.com
www.gbs.com