techconsult
TECHNOLOGY MARKET ANALYSTS

30 YEARS ANNIVERSARY

E-Mail-Sicherheit in Unternehmen
Status, Defizite und Strategien

Branchenübergreifende repräsentative Umfrage zum Stand der E-Mail-Sicherheit in deutschen Unternehmen

Unterstützt durch

noSpam proxy®

Inhalt

Vorwort

Die Verbreitung digitaler Technologien in sämtlichen Lebensbereichen konfrontiert Unternehmen aller Art auf vielfältige Weise. Wo auf der einen Seite Potenziale wie die Beschleunigung von Prozessabläufen oder die ortsunabhängige Zusammenarbeit erkannt werden, so finden sich auf der anderen Seite auch wachsende Risiken.

Eines dieser Risiken findet sich in der wachsenden Cyberkriminalität und den damit verbundenen Schäden für die Unternehmen wieder. Dabei sind primär die E-Mail-Postfächer im Visier der Cyberkriminellen. Nahezu sämtliche interne wie externe Kommunikation wird über die E-Mail getätigt.

Doch als wie wichtig erachten Unternehmen die Absicherung der eigenen E-Mail-Postfächer? Wo sehen sie akuten Handlungsbedarf in puncto E-Mail-Sicherheit? Und wem überlassen die Unternehmen den Betrieb der E-Mail-Security?

Um diese Fragen zu beantworten, wurden im Rahmen dieser Studie 201 Entscheider oder maßgeblich am Entscheidungsprozess beteiligte Personen zu ihrer Einschätzung von E-Mail-Sicherheit, den Handlungsbedarfen aber auch den Anforderungen an cloud-basierter E-Mail-Sicherheit befragt. An der Befragung im Januar 2022 nahmen 201 Mitarbeiter aus kleinen bis großen Unternehmen aus sämtlichen Branchen teil.

Hoher Stellenwert für E-Mail-Sicherheit

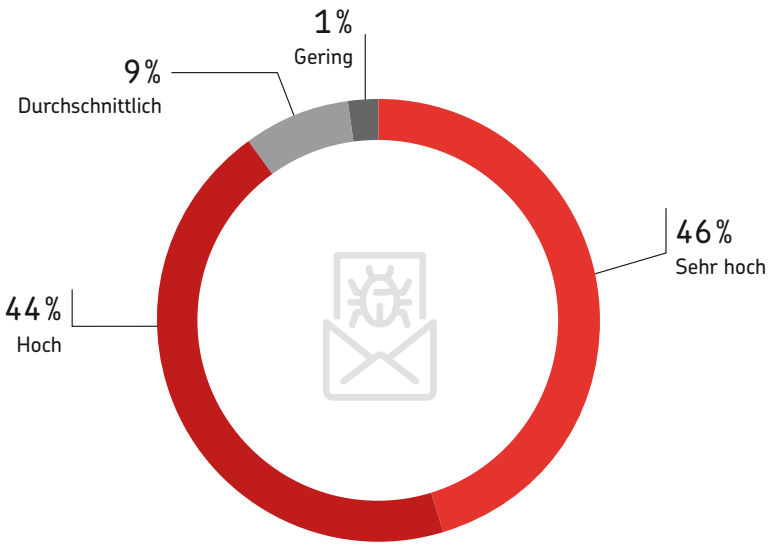
Dem Lagebericht des BSI für 2021 zu Folge gab es im Durchschnitt 394.000 neue Schadprogramm-Varianten – pro Tag. Für jeden Verantwortlichen aus der IT-Sicherheit sollten dies alarmierende Zahlen sein. Insbesondere der Schutz von E-Mail-Postfächern muss ganz oben auf der Agenda stehen. Ob Phishing, Ransomware oder Business-E-Mail Compromise, die E-Mail-Postfächer sind die primäre Methode mit der Cyberkriminelle Schadsoftware in die Unternehmensnetzwerke schleusen.

Den höchsten Stellenwert genießt die E-Mail-Sicherheit in 46 Prozent der Unternehmen. Vor allem Banken und Versicherungen können hier als Vorreiter gesehen werden. Rund drei Viertel der Finanzdienstleister behandeln das Thema mit höchster Priorität. Das ist wenig verwunderlich, müssen Banken und Versicherungen mit allerhand vertraulichen Informationen über ihre Kunden umgehen. Eine unverschlüsselte E-Mail könnte beispielsweise Bankkontoinformationen oder die Sozialversicherungsnummer in die Hände von Cyberkriminellen spielen.

Einen hohen Stellenwert nimmt die E-Mail-Sicherheit in weiteren 45 Prozent der Unternehmen ein. Addiert man die Unternehmen mit hohem mit denen die einen sehr hohen Stellenwert vergeben, so sieht man, dass E-Mail-Sicherheit absolut im Fokus der Unternehmen steht. Besonders die größten Unternehmen ab 5.000 Mitarbeitenden sehen E-Mail-Sicherheit als wichtig an. Alle befragten Unternehmen in dieser Größenklasse geben der E-Mail-Sicherheit einen hohen oder sehr hohen Stellenwert.

Auf der anderen Seite hat die E-Mail-Sicherheit in kleineren Unternehmen tendenziell etwas weniger Priorität. So geben knapp 10 Prozent der Unternehmen mit weniger als 50 Mitarbeitenden an, dass sie der E-Mail-Sicherheit nur eine durchschnittliche oder gar geringe Priorität zuschreiben. In Unternehmen zwischen 50 und 199 Mitarbeitern liegt der Anteil sogar bei 14 Prozent.

Wie relevant ist E-Mail-Sicherheit?



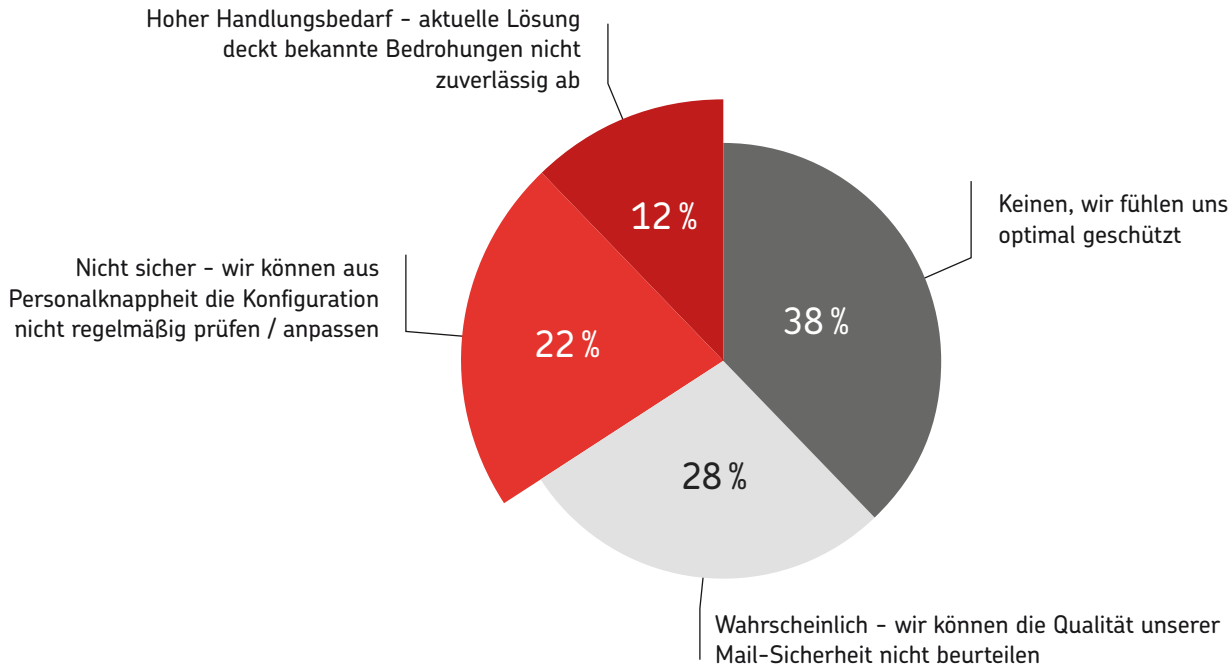
Basis: 201 Unternehmen

Unternehmen erkennen Handlungsbedarf

Unternehmen sehen sich immer größeren Bedrohungen ausgesetzt. Nicht nur ist die E-Mail die beliebteste Methode der Cyberkriminellen, um in Unternehmensnetzwerke einzudringen und Schaden anzurichten. In Zukunft ist auch damit zu rechnen, dass Angriffe immer häufiger stattfinden und auch schwerwiegender ausfallen werden. Vor allem durch die rapide ansteigende Anzahl an Mitarbeitern im Homeoffice vergrößert sich die Angriffsfläche. In den Homeoffices verliert die IT-Abteilung die Hoheit über die Sicherheit. Die alten IT-Sicherheitsstrukturen könnten unter Umständen nicht mehr ausreichen, um das eigene Unternehmen effektiv vor Bedrohungen durch E-Mails zu schützen.

So ist es auch kein Wunder, dass Banken und Versicherungen mit Abstand den größten akuten Handlungsbedarf erkennen. Fast 30 Prozent der Finanzdienstleister sind der Meinung, sofort handeln zu müssen, da ihre eingesetzten Lösungen nicht ausreichen, um die aktuellen Bedrohungen abzuwehren. Über alle Branchen hinweg sind nur 12 Prozent der Unternehmen der Meinung, dass eine sofortige Verbesserung der eigenen E-Mail-Security notwendig ist.

Welche Handlungsbedarfe sehen Unternehmen?



Basis: 201 Unternehmen, Mehrfachnennungen möglich

Tatsächlich sind nur 38 Prozent der befragten Unternehmen der Meinung, dass ihre aktuell eingesetzten Maßnahmen zur E-Mail-Sicherheit für einen optimalen Schutz sorgen. Das bedeutet, dass der überwiegende Teil – rund zwei Drittel – der Unternehmen sich darüber im Klaren ist, dass ihre E-Mail Sicherheit verbesserungswürdig ist und Handlungsbedarf besteht. Besonders Banken und Versicherungen scheinen im Fokus E-Mail-basierter Angriffe zu stehen. Nur 14 Prozent der befragten Unternehmen aus dem Finanzsektor sind mit ihrer E-Mail-Sicherheit zufrieden.

22 Prozent der Unternehmen sind der Ansicht, dass sie die Qualität ihrer E-Mail-Sicherheit nicht einschätzen können und wahrscheinlich Handlungsbedarf besteht. Wenn man keinen Überblick darüber hat, ob die eingesetzten Lösungen ausreichen, stellt sich die Frage, wie viele Angriffe unbemerkt stattgefunden haben und wie viele Daten von Cyberkriminellen abgegriffen oder manipuliert worden sind. Unternehmen, die sich der Qualität ihrer E-Mail-Sicherheit nicht bewusst sind, sollten dringlichst daran arbeiten, eine sicherere E-Mail-Infrastruktur aufzubauen. Das kann sowohl durch die Neuaufstellung der On-Premises-Sicherheitsarchitektur erfolgen oder mit Hilfe der Expertise von spezialisierten Dienstleistern.

Unternehmen vertrauen Cloud-Dienstleistern

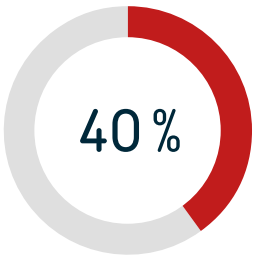
Wie bei vielen anderen Security-Themen kann auch die E-Mail-Sicherheit sowohl intern als auch extern mit Hilfe von Dienstleistern betrieben werden. Ein großer Teil der Unternehmen (40 Prozent) überlässt den Betrieb der E-Mail-Sicherheit einem Anbieter für cloudbasierte Security-Services. Die Vorteile von cloudbasierter E-Mail-Sicherheit liegen auf der Hand. Da wäre zum einen die schnellere Bereitstellung und Migration, da keinerlei Software oder Hardware installiert werden muss, zum anderen profitieren Unternehmen von den Softwareupdates, die der Betreiber der Cloud-Lösung aufspielt und dadurch zu jeder Zeit für optimalen Schutz sorgt, sowie von der Übernahme des gesamten Supports durch den Anbieter. Vor allem Unternehmen ohne eigene Sicherheitsabteilung profitieren stark von E-Mail-Sicherheit aus der Cloud. Die einfache Verwaltung und der Wegfall von Support-Leistungen entlasten die IT-Abteilungen, die sich wiederum anderen Aufgaben zuwenden können.

Mehr als ein Drittel der befragten Unternehmen betreiben ihre E-Mail-Sicherheitslösung on-premises im eigenen Unternehmen. Hier behalten Unternehmen die volle Kontrolle über die Daten, die Prozesse und damit auch über die Sicherheit selbiger.

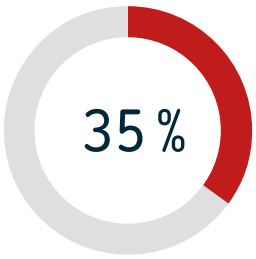
Allerdings müssen IT-Abteilungen hier selbst dafür Sorge tragen, dass die Sicherheitslösung stets auf dem neuesten Stand ist und von ihnen gewartet wird. Ein verpasstes Update kann dabei schnell zu einem Sicherheitsrisiko werden. Wie es beispielsweise im Zuge der Attacken auf Exchange-Server durch die Cybercrime Gruppe Hafnium der Fall war. Unternehmen, die nicht direkt reagiert und die Sicherheitslücken geschlossen haben, setzten ihre Netzwerke hohen Risiken aus.

Es ist zu beobachten, dass die Angreifer sowohl technisch als auch methodisch immer professioneller agieren und kontinuierlich neue Angriffsmuster entwickeln. Um im Wettlauf mit ihnen bestehen zu können, müssen interne IT-Abteilungen eine Tiefe und Breite an Know-how für Mail Security aufbauen, dass kleinere und mittlere Organisationen kaum wirtschaftlich darstellen können – von der mangelnden Verfügbarkeit entsprechender Ressourcen am Arbeitsmarkt einmal ganz abgesehen. Obwohl der Trend eindeutig in Richtung Cloud geht, ist die Nachfrage nach On-Premises-Lösungen und Managed Services weiterhin hoch. Nur wer alle Deployment-Formen beherrscht, kann die Bedürfnisse des Marktes vollends abdecken.

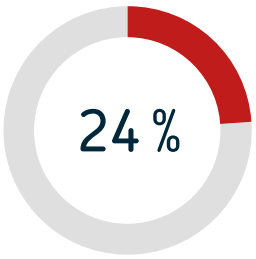
Wie wird E-Mail-Sicherheit betrieben?



Cloudbasierte E-Mail-Security



On-premises im eigenen Rechenzentrum



Managed Service bei einem lokalen Dienstleister

Basis: 201 Unternehmen

Abwehr von Schäden an höchster Stelle

Unternehmen, die auf cloudbasierte E-Mail-Sicherheit setzen oder in Zukunft bauen wollen, haben ganz gezielte Vorstellungen davon, welche Funktionen ein cloudbasierter Security-Service bieten muss.

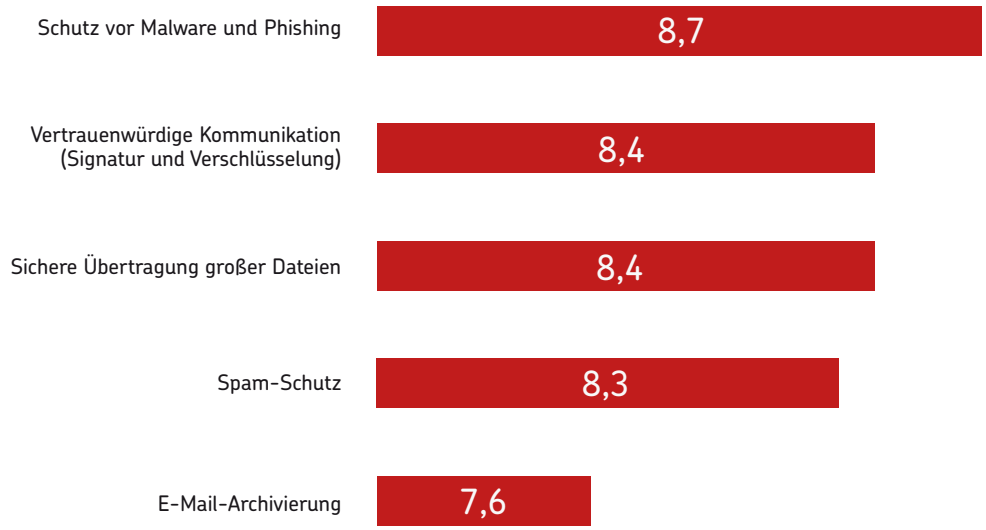
Die mit Abstand wichtigste Funktion einer cloudbasierten E-Mail-Security Lösung stellt der Schutz von Malware und Phishing dar. Das ist nicht verwunderlich, ist es doch die primäre Aufgabe einer Security-Lösung, Schadsoftware vom eigenen Unternehmen fernzuhalten. Erst im letzten Jahr wurden etliche Microsoft Exchange Dienste Opfer von Angriffen durch die Hackergruppe Hafnium. Diese nutzten Schwachstellen in on-premises Microsoft-Exchange gezielt aus. Aber auch Phishing genießt einen regelrechten „Boom". Cyberkriminelle nutzen vor allem die Zunahme von mobiler Arbeit, um sich mittels Phishing Zugang zum Unternehmensnetzwerk zu verschaffen. Gleichwohl steht Phishing auch in direktem Zusammenhang mit Malware- oder Randsomware-Angriffen. Hier werden Nutzer auf täuschend echt wirkende Webseiten geleitet, um das Unternehmensnetzwerk darüber mit Schadsoftware zu infizieren. Das Verhindern solcher Angriffe ist das A und O einer Lösung für E-Mail-Sicherheit.

Ähnlich hoch ist der Bedarf für die vertrauenswürdige Kommunikation zwischen E-Mail-Empfängern mit Signatur und Verschlüsselung. Bei der Fülle an sensiblen Informationen ist die unverschlüsselte Kommunikation heute weder zeitgemäß noch im Einklang mit der geltenden Gesetzgebung zum Datenschutz. Bei Verstößen und Lücken drohen nicht nur empfindliche Strafen, sondern auch erhebliche Reputationsverluste.

Von gleicher Wichtigkeit ist die sichere Übertragung großer Dateien. Das Senden großer E-Mails kommt oftmals nicht ohne Medienbruch aus. Outlook beispielsweise deckelt standardmäßig E-Mail-Anhänge auf 20 MB. Und die durchschnittliche Dateigröße steigt von Jahr zu Jahr. Da ist es manchmal unumgänglich, die Dateien vorher auf einen FTP-Server oder in einen Cloud-Speicher hochzuladen. Das kann unter Umständen gefährlich werden, wenn beispielsweise der Cloud-Speicher als Schatten-IT außerhalb des Blickfelds der IT-Abteilung läuft. Sensible Daten könnten so in die Hände von Cyberkriminellen gelangen.

Auch der Schutz vor Spam ist als Grundfunktion einer Mail-Security-Lösung stark nachgefragt. Die Archivierung von E-Mails liegt in der Wichtigkeit etwas zurück.

Was sind die Vorteile cloudbasierter E-Mail-Sicherheit?



Basis: 201 Unternehmen, Mehrfachnennungen möglich, Skala: 1 ("unwichtig") - 10 ("sehr wichtig")

Support-Qualität essenziell für Dienstleister

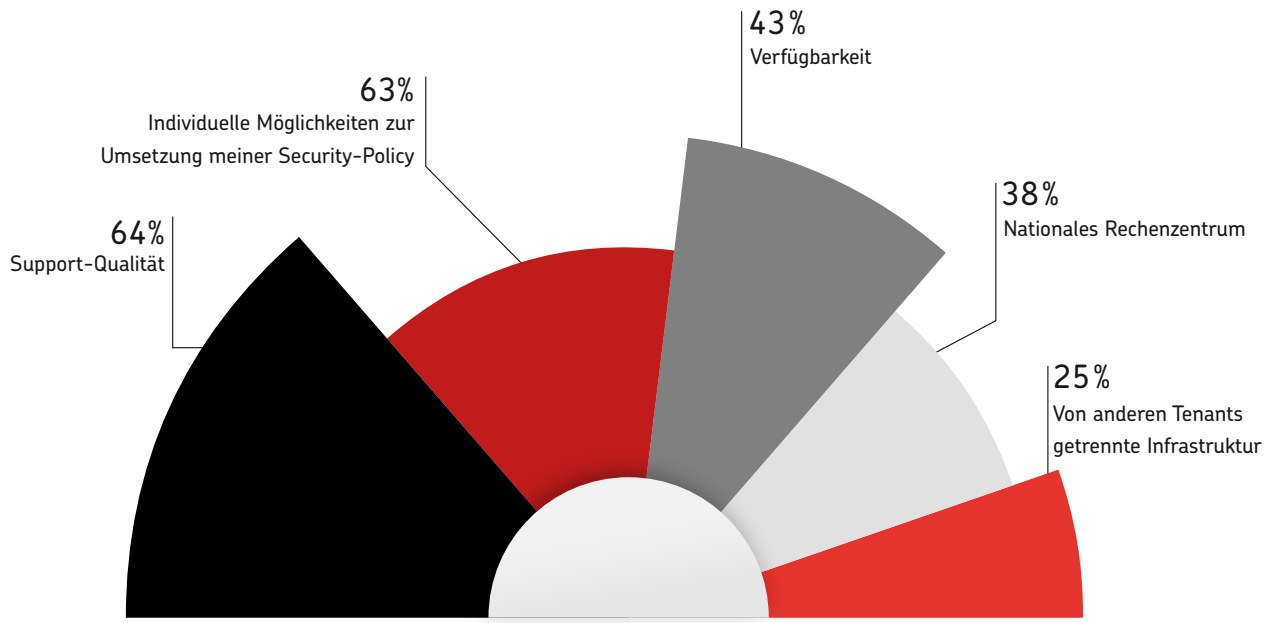
Entscheidet sich ein Unternehmen dazu die E-Mail-Sicherheit auszulagern, muss zunächst der passende Dienstleister gefunden werden, der diese Aufgaben übernimmt. Dabei haben Unternehmen klare Ansprüche daran, was Anbieter für E-Mail-Sicherheit, neben der Kernaufgabe des Schutzes, leisten müssen.

Die wichtigste Eigenschaft, die ein Anbieter für E-Mail-Sicherheit mitbringen muss, ist eine außergewöhnliche Support-Qualität. Für fast zwei Drittel der befragten Unternehmen ist dies der Kernpunkt bei der Auswahl eines Dienstleisters. Das ist nicht verwunderlich, dass Störungen in der E-Mail-Kommunikation sofort erhebliche Auswirkungen auf den Geschäftsbetrieb des gesamten Unternehmens haben können. Der Dienstleister steht in der Pflicht sämtlichen die E-Mail-Sicherheitslösung betreffenden Support schnell und effektiv zu leisten. Ist dieser beispielsweise nur schwer erreichbar oder vielleicht sogar vom Anbieter an einen anderen Dienstleister ausgelagert, kann dies schnell zu Frustration beim Kunden führen.

Ein weiteres wichtiges Merkmal stellt die Konfigurierbarkeit zur Umsetzung der eigenen Security-Policies dar. Dass die Konfigurierbarkeit einer Software nach den eigenen Vorstellungen äußerst wünschenswert ist, verwundert wenig.

Aber das setzt auch große Kenntnisse im Unternehmen voraus. Denn jede Konfiguration birgt die Gefahr, dass man Fehler begeht und eine vormals sichere Lösung für Cyberkriminelle öffnet. Fehlt dieses Wissen jedoch, sollte man sowohl auf die Expertise der Anbieter, als auch die best practices der Hersteller vertrauen und die bereitgestellte Lösung so nehmen wie sie ist. Denn nur so ist auch der sichere Betrieb gewährleistet.

Was muss ein externer Dienstleister leisten?



Basis: 201 Unternehmen, Mehrfachnennungen möglich

Fazit

E-Mail-Sicherheit stellt eine zentrale Disziplin im Kontext der IT-Sicherheit dar. Unternehmen sehen grundsätzlich, dass sie großen Handlungsbedarf bezüglich ihrer E-Mail-Sicherheit haben. Rund 2/3 der Unternehmen sind der Meinung, die E-Mail-Sicherheit bedarf Anpassungen, um sich an die veränderten Rahmenbedingungen einzustellen und die E-Mail-Postfächer auch nachhaltig sicher zu betreiben.

Lösungen für E-Mail-Sicherheit werden sowohl in der Cloud, on-premises und als Managed Service von jeweils signifikanten Anteilen der befragten Unternehmen gefordert. Da sich diese Anteile in Zukunft sicher weiter verschieben werden, sollten auch Wechsel einfach möglich sein. Hier bieten Lösungen, die alle Einsatzszenarien gleichwertig unterstützen, klare Vorteile.

Lösungen, die flexible und detaillierte Konfigurationsmöglichkeiten und deren Hersteller beste Supportqualität bietet, decken die an E-Mail-Security gestellten Anforderungen optimal ab. Eine optimal aufgestellte E-Mail-Sicherheit ist für Unternehmen jeder Größe von höchster Bedeutung. Denn Cyberkriminelle attackieren E-Mail-Postfächer in hoher Frequenz und eine Entspannung der Bedrohungslage ist nicht zu erwarten. Eher noch werden Cyberbedrohungen ist Zukunft noch gehäufter auftreten.

Nur mit einer optimal aufgestellten E-Mail-Sicherheit lassen sich nicht nur Schäden durch Malware und Phishing verringern. Eine ganzheitliche Lösung ermöglicht Unternehmen auch sichere E-Mail-basierte Kommunikation sowohl im eigenen Unternehmen als auch mit Kunden und Partnern.

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

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

Kontakt

Raphael Napieralski
Analyst

E-Mail: **raphael.napieralski@techconsult.de**
Tel.: +49 561 8109 181

Über die techconsult GmbH

Als Research und Analystenhaus ist techconsult seit 30 Jahren der Partner für Anbieter und Nachfrager digitaler Technologien und Services. Die techconsult GmbH wird vom geschäftsführenden Gesellschafter und Gründer Peter Burghardt am Standort Kassel mit einer Niederlassung in München geleitet.

Über Net at Work

Net at Work unterstützt als IT-Unternehmen seine Kunden mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit. Der Geschäftsbereich Softwarehaus entwickelt und vermarktet mit NoSpamProxy ein innovatives Secure E-Mail-Gateway mit erstklassigen Funktionen für Anti-Spam, Anti-Malware und E-Mail-Verschlüsselung, dem weltweit mehr als 4.000 Kunden die Sicherheit ihrer E-Mail-Kommunikation anvertrauen. Die mehrfach ausgezeichnete Lösung – unter anderem 5-facher Champion im unabhängigen techconsult Professional User Ranking – wird als Softwareprodukt und Cloud-Service, sowie von Partnern auch als Managed Service angeboten. Mehr zum Produkt unter: www.nospamproxy.de

noSpamproxy®

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

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

Erscheinungsdatum: 03/2022