Alinto

Weißbuch

E-Mail:
Das schwächste Glied in Office 365?

Zusammenfassung

Einführung

Die digitale Transformation ist mehr denn je ein zentrales Anliegen der Unternehmen. Jede Organisation setzt Projekte zur Entmaterialisierung, zur Neugestaltung von Prozessen, zum Digital Workplace, zu kollaborativen Räumen usw. um. In der Mehrheit der Unternehmen geschieht dies durch die **Einführung von Office 365, jetzt Microsoft 365 genannt**.

Aber: Die Technologie bleibt eine großartige Spielwiese für Cyberkriminelle. Zu den verschiedenen Angriffsformen gehören **Ransomware, Spam-oder Phishing-E-Mails...** Dies sind ernsthafte Bedrohungen für Unternehmen, die ernsthafte Auswirkungen auf ihr Geschäft haben können.

Häufig stammen diese Angriffe aus betrügerischen E-Mails. Auch Outlook aus der Office 365-Suite bleibt davon nicht verschont. Welche Lösungen - von Microsoft oder anderen - gibt es für eine bessere Sicherheit? Wie kann man seine E-Mails schützen? Ist es möglich, sich von einem Partner begleiten zu lassen? Wir beantworten all diese Fragen in unserem Weißbuch.

Einführung von Microsoft 365 in Unternehmen: eine Bestandsaufnahme

Microsoft 365 ist eine Suite, die von Unternehmen aufgrund ihrer zahlreichen Anwendungen, ihrer Praktikabilität und auch ihrer Marktposition massiv gewählt wird. Nach Monaten der Nutzung stellen viele Unternehmen jedoch fest, dass diese Tools kaum oder nur unzureichend genutzt werden. **Der ROI ist daher nicht unbedingt gegeben**. In diesem Artikel wollen wir Ihnen Zahlen und eine Bestandsaufnahme über die tatsächliche Akzeptanz von Office 365 und die Gründe für Misserfolge liefern.

Einführung von Office 365: die Zahlen

Die Microsoft-Suite wurde in ihrer heutigen Form mit Abonnement vor fast zehn Jahren eingeführt. Sie vereint zahlreiche Anwendungen, die den alltäglichen und geschäftlichen Bedürfnissen von Unternehmen entsprechen: die historischen Tools (Word, Excel, PowerPoint...) und neue Webdienste (OneDrive, Yammer...). Im Jahr 2019 zählte die Office 365-Suite **155 Millionen aktive Nutzer**. Sie wurde Anfang 2020 in Microsoft 365 umbenannt.

Laut einem Forrester-Bericht kann die Einführung von Office 365 innerhalb von drei Jahren einen ROI von 162 % erbringen. Vorausgesetzt, die Suite wird richtig genutzt. Der Microsoft 365 Report berichtet, dass **88 % der IT-Entscheidungsträger Microsoft 365 in ihrem Unternehmen vollständig implementiert haben**. Laut einem Artikel im JDN sind 80 % der CAC40-Unternehmen damit ausgestattet. Der Hauptgrund für diese Entscheidung ist die Flexibilität des Angebots, um der Komplexität der Organisationen gerecht zu werden.

Die Zahlen sind jedoch mit Vorsicht zu genießen. Der Microsoft-Bericht zeigt, dass die meisten Unternehmen noch nicht alle Funktionen der Software-Suite übernommen haben, insbesondere im Hinblick auf die Sicherheit. Wann gilt ein Tool als eingeführt? Ist es nur die Verbindung zu Microsoft? In diesem Fall verwenden 100 % der Nutzer das Programm, weil sie mit E-Mails verbunden sind. Die tatsächliche Einführung ist komplexer: Sie ist dann gegeben, wenn die damit einhergehenden Veränderungen real und konkret sind, z. B. durch neue Formen der Zusammenarbeit.

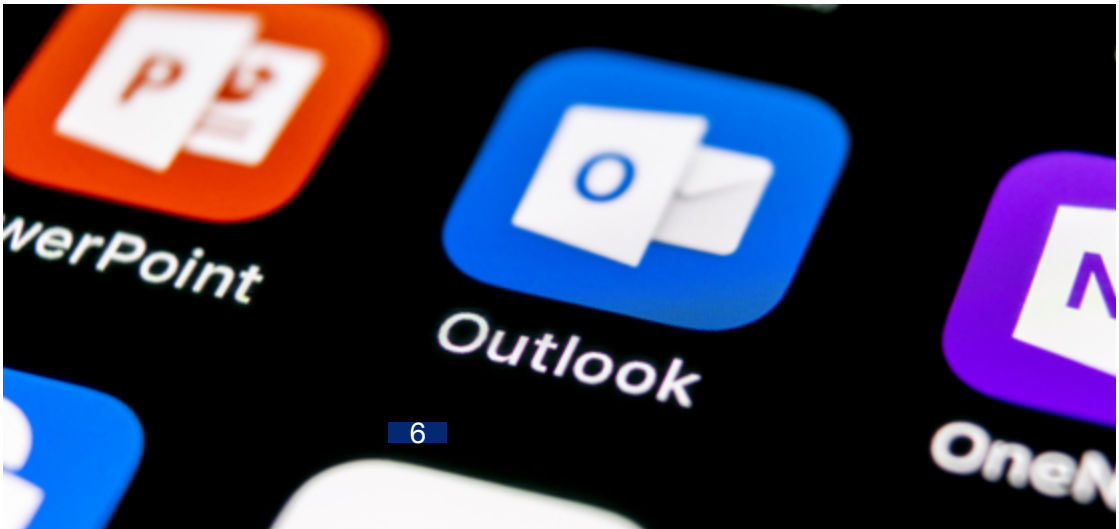
Nutzung von Office 365: Die beliebtesten Anwendungen

In Bezug auf die Nutzung muss man feststellen, dass **die Benutzer** trotz der Integration von Office in die Cloud an **den alten Praktiken** festhalten: lokale Erstellung von Dokumenten, Teilen von Dateien per E-Mail... Logischerweise sollten die Benutzer auf E-Mails verzichten, zumindest um Dokumente intern auszutauschen oder zu teilen. OneDrive bietet die Möglichkeit, sichere Freigabelinks zu generieren. Sie nutzen also die Stärken der Suite nicht wirklich aus.

Im Einzelnen sind die am häufigsten genutzten Apps im dritten Quartal 2019 :

- Outlook / Exchange: **59 %**
- Teams: **41 %**
- Skype für Unternehmen: **23 %**

Wir sehen, dass wirklich kollaborative Anwendungen nur schwer in Gang kommen. Das liegt daran, dass viele Nutzer nicht wissen, auf welche Anwendungen sie Zugriff haben (47 % laut Microsoft 365 Report) und welche Vorteile diese mit sich bringen.



ROI Office 365: Warum klemmt es?

In der Realität **ist die Annahme der Office 365-Suite nicht so selbstverständlich, wie die Anwenderunternehmen uns glauben machen wollen**.

Hier einige Zahlen, die dies belegen

- **34 %** der Nutzer sträuben sich gegen Veränderungen
- **47 %** wissen nicht, auf welche Anwendungen sie Zugriff haben
- **29 % haben zu** wenig Zeit, um sich weiterzubilden

Unternehmen müssen die Nutzung ihrer Teams ständig überwachen, um sie in die richtige Richtung zu lenken. Und genau hier liegt das Problem. Es reicht nicht aus, Leitfäden zu verteilen, die erklären, wie es geht. Sie müssen Szenarien erstellen, die Vorteile der Collaboration Suite aufzeigen und davon überzeugen. Es geht darum, **einen echten internen Transformationsprozess zu starten**, und nur wenige Unternehmen tun dies. Sie sind der Ansicht, dass es eine erfolgreiche Einführung ist, wenn sich die Nutzer ab und zu mit ihren E-Mails und einigen Anwendungen verbinden. Allerdings entspricht der ROI nicht ihren Erwartungen! Und das aus gutem Grund: Die Lizenzpreise sind 2019 um 10 % gestiegen!

Für eine bessere Akzeptanz von Office 365 gibt es folgende Möglichkeiten :

- Die Suite in den Mittelpunkt der digitalen Transformation des Unternehmens stellen
- Beziehen Sie die Direktionen durch das Setzen von Zielen mit ein
- Auch das Management muss die Lösungen nutzen, um mit gutem Beispiel voranzugehen

Während die Einführung von Microsoft 365 eine quantitative Realität ist, ist die «qualitative» Annahme durch die Benutzer in den Unternehmen noch nicht optimal. Auch wenn die Suite auf dem Papier alle Qualitäten aufweist, die für eine sichere Zusammenarbeit erforderlich sind, stößt sie auf die von den Nutzern vorgebrachten Hemmnisse, die **den Prozess der digitalen Transformation der Organisationen verlangsamen** können.

Office 365: Was ändert sich für E-Mails?

E-Mail ist ein zentrales Werkzeug für ein Unternehmen. Wenn es ausfällt, leidet die gesamte Geschäftstätigkeit! Und wenn sie keinen BCP (Business Continuity Plan) hat, ist das ein ziemliches Handicap.

Im Jahr 2018 nutzten 56 % der Unternehmen die Office 365-Suite (heute Microsoft 365). Um E-Mails zu empfangen, müssen diese Unternehmen über den Exchange-Server gehen, was den Zugriff auf E-Mails, Kalender und Dokumente, die auf den Servern gespeichert sind, ermöglicht. Aus Gründen der Einfachheit entscheiden sich daher viele Organisationen dafür, die End-to-End-Dienste des Anbieters in Anspruch zu nehmen. Oftmals auf Kosten der Sicherheit. Das wollen wir in diesem Artikel analysieren.

Welche E-Mail-Funktionen bietet Office 365?

Outlook ist der am häufigsten genutzte Dienst für geschäftliche E-Mails. Und das aus gutem Grund, denn er weist mehrere Schlüsselfunktionen auf:

1. **Auf zusätzliche Dienste** zugreifen: Kalender, Aufgaben- und Notizverwaltung...
2. **Eigene Signaturen** erstellen
3. **Mehrere E-Mail-Postfächer** gleichzeitig abrufen
4. Erleichtern Sie die **Zusammenarbeit**
5. Eine E-Mail **von Word aus** senden
6. **Nahtlose Integration** mit anderen Office-Programmen von Microsoft
7. Die **Sicherheit von E-Mails** verbessern
8. **Mobil** auf E-Mails zugreifen
9. **Ordner und Dateien** ordnen

Es gibt jedoch immer noch Löcher im Teppich, vor allem bei der Sicherheit eingehender und ausgehender E-Mails. Die Schutzangebote von Microsoft sind kostenpflichtig, viele Unternehmen nehmen die Option nicht wahr. Viele E-Mail-Programme sind daher kaum oder gar nicht gesichert und den Händen von Hackern ausgeliefert oder zumindest anfällig. Die Gefahr wird durch die massive und schnelle Einführung von Telearbeit noch verschärft: Ohne strenge Rahmenbedingungen und **Software zur Sicherung** (Anti-Spam, Anti-Phishing) von E-Mails kann die gesamte Aktivität eines Unternehmens durch eine einfache E-Mail bedroht werden.

Welche Alternativen zu Office 365 gibt es?

CIOs würden gerne ihre **Abhängigkeit von Microsoft** verringern. Wenn sie jedoch ein Glied in der Kette wie Exchange ersetzen, könnte dies den Alltag der Benutzer schwächen. Und ein solcher Wechsel ist nicht einfach.

Einerseits, weil Microsoft in einem geschlossenen System funktioniert: Alle Anwendungen sind voneinander abhängig und Alternativen sind nicht immer leicht interoperabel. Unternehmen nehmen daher oft **das Paket «Outlook, Exchange und Active Directory»**, um zu funktionieren, ohne nach Alternativen zu suchen.

Andererseits erzeugen Änderungen von Tools Einschränkungen für die Nutzer. Organisationen möchten daher ihre Gewohnheiten nicht stören.

Es gibt jedoch Alternativen, um die E-Mails besser zu schützen. Es ist zum Beispiel möglich, Outlook beizubehalten, aber **einen anderen Postausgangsserver als Exchange zu wählen**. Dies ist für die Nutzer völlig transparent, ermöglicht aber eine bessere Absicherung der E-Mails und macht Sie nicht völlig von Microsoft abhängig.

Der Outlook-E-Mail-Dienst ist sehr praktisch, vollständig kompatibel mit allen Microsoft-Anwendungen und stärkt so die Zusammenarbeit. Es ist jedoch völlig möglich, externe Dienstleister mit der Integration von Office-Funktionen zu beauftragen und diese interoperabel zu machen.

Einsatz von Office 365: Wie kann die Sicherheit von E-Mails gewährleistet werden?

Ransomware-Angriffe werden immer häufiger und betreffen jeden, auch kleine Unternehmen. **Diese Schadprogramme dringen meist über eine E-Mail ein**. Daher sollten Sie den Aspekt der Sicherung Ihrer geschäftlichen E-Mails nicht auf die leichte Schulter nehmen. Neben der Sensibilisierung Ihrer Mitarbeiter für grundlegende Maßnahmen (keine E-Mails mit seltsamen Betreffzeilen oder Anhängen öffnen, regelmäßig das Passwort ändern und nicht überall dasselbe verwenden usw.) müssen weitere Lösungen eingeführt werden, um **Ihre IT-Sicherheit zu gewährleisten**.

In diesem Artikel geben wir einen Überblick über die Sicherheit von Exchange-E-Mails und verraten Ihnen unsere Tipps, wie Sie Ihre E-Mails gut schützen können.

Sicherung von Exchange-Mailern: Welche Zahlen und welche Herausforderungen?

Die meisten Ransomware-Angriffe sind opportunistisch und nutzen die geringe digitale Reife von Organisationen aus. Seit 2018 nehmen die Angriffe zu und werden zunehmend mit anderer Malware wie Kryptoviren oder anderen Trojanern gekoppelt. Die Daten von Unternehmen und auch von Privatpersonen können daher von Hackern leicht verschlüsselt werden, die dann ein Lösegeld verlangen, um auf Ihre eigenen Daten zugreifen zu können.

Der Schaden für die Unternehmen geht oft weit über den Verlust einiger Daten hinaus:

- Produktionsstopp
- Rückgang des damit verbundenen Umsatzes
- rechtliche Risiken (z. B. mit der DSGVO)
- Rufschädigung
- Vertrauensverlust
- Die Gendarmerie berichtet auch von Fällen, in denen Mitarbeiter nach Betrügereien mit dem Präsidenten Selbstmord begangen haben.

In dem von der Regierung herausgegebenen Leitfaden «Attacken durch Ransomware, alle betroffen» berichten mehrere Unternehmen :

- Im November 2019 konnte das **Universitätsklinikum Rouen** nicht mehr auf eine Fachanwendung zugreifen. Die IT-Abteilung stellte anschließend fest, dass die Arbeitsstationen und Server verschlüsselt waren. Es handelte sich um Ransomware.
- Im Oktober 2019 wurde die **M6-Gruppe von** einem Ransomware-Angriff betroffen, der den Zugang zum Internet unterbrach, der jedoch insbesondere für Radiosendungen unerlässlich ist.
- Im April 2019 musste das **Unternehmen Fleury Michon** nach einem Ransomware-Angriff alle Internetzugänge der Mitarbeiter kappen. Der Betrieb kam drei Tage lang komplett zum Erliegen und war zwei Wochen lang beeinträchtigt.

Der Ausgangspunkt für solche Angriffe ist oft eine E-Mail. Dennoch werden Fragen der Absicherung von E-Mails, aber auch des gesamten IT-Parks, noch immer nicht ernst genug genommen. Und die Zahlen aus einer von SoftwareONE durchgeführten Umfrage belegen dies:

- **44 % der Befragten verwenden nicht Microsoft Intune** (Verwaltung mobiler Geräte und Anwendungen) ;
- **37 % verwenden nicht Microsoft Azure Advanced Threat Protection** (Identifizierung, Erkennung und Untersuchung von fortgeschrittenen Bedrohungen) ;
- **36 % nutzen Microsoft Azure Information Protection (Dokumentenschutz) nicht.**

Bei der Abwehr von Bedrohungen und der Antizipation von Angriffen sind noch weitere Fortschritte erforderlich.

Schutz von E-Mails: Unsere drei Tipps

Um die Risiken zu verringern und Ihr Geschäft zu schützen, müssen Sie mehrere Maßnahmen ergreifen. Wenn wir Ihnen jedoch unsere besten Tipps liefern sollten, würden wir die folgenden drei auswählen.

1 Sensibilisieren Sie Ihre Mitarbeiter

Angriffe mit Malware gehen sehr oft von E-Mails aus, die ein Mitarbeiter erhält. Daher ist es wichtig, sie an **gute Praktiken zu erinnern und Reflexe im Umgang mit E-Mails zu wecken**: Öffnen Sie keine verdächtigen Betreffzeilen oder Anhänge oder solche von unbekannten Empfängern, melden Sie eventuelle Probleme an die IT-Abteilung... Dies ist zwar kein absoluter Schutz, aber ein notwendiger Schritt, um das Risiko von Angriffen zu verringern.

2 Ihr IS sichern

Natürlich ist es von größter Bedeutung, Ihr Informationssystem zu sichern. Dazu gehört die Verwaltung der Zugriffsrechte auf Anwendungen, die Abschottung des IS, um das Risiko einer Ausbreitung auf alle Arbeitsplätze begrenzen zu können, die verschiedenen Anwendungen auf dem neuesten Stand zu halten, da dies ihre Sicherheit verbessert, und Ihre Daten regelmäßig zu sichern.

3 Entscheiden Sie sich für Lösungen zum Schutz von E-Mails

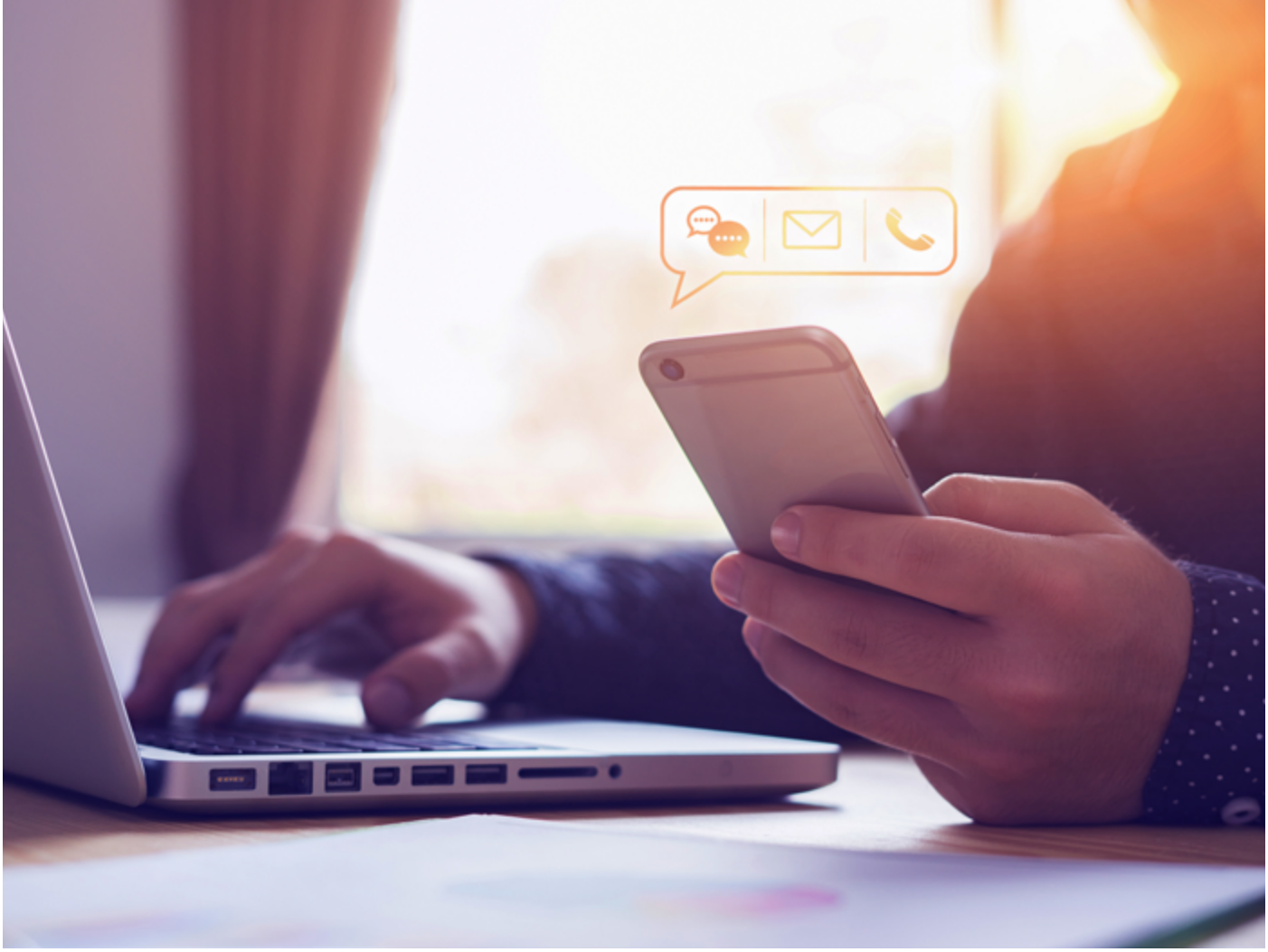
Schließlich ist es für die maximale Sicherheit Ihrer E-Mails wichtig, die Arbeitsstationen mit Antispam- und Antiviren-Software auszustatten. **Diese Tools identifizieren und blockieren bösartige E-Mails, verhindern eine Kompromittierung und verhindern, dass Ihre Daten verschlüsselt werden**. Seien Sie jedoch vorsichtig, sie reichen nicht aus. Für einen optimalen Schutz ist es wichtig, sie auf dem neuesten Stand zu halten und sicherzustellen, dass keine schädlichen Anwendungen auf Servern, Arbeitsplätzen usw. installiert sind.

E-Mail-Filterung: Warum sollten Sie sich für eine zusätzliche Lösung entscheiden?

Im Zusammenhang mit unserem letzten Tipp: Auch wenn Microsoft Lösungen zur Sicherung von E-Mails anbietet, ist die Ausstattung mit externen Lösungen ein Pluspunkt, der von der ANSSI (Agence nationale de la sécurité des systèmes d'information) als unverzichtbar angesehen wird. Zunächst einmal belegen die Zahlen, dass Unternehmen nicht immer die mit Microsoft verfügbaren Sicherheitsoptionen wählen oder sie nicht nutzen. Dadurch entsteht bereits eine Schwachstelle.

Zweitens ist Software, die auf die Wartung von E-Mail-Programmen spezialisiert ist, das Ergebnis kontinuierlicher Forschungs- und Entwicklungsbemühungen, die sich diesen Aspekten widmen, und bietet fortschrittliche Lösungen an. Dies hilft auch, die Grenzen der Abhängigkeit von Microsoft zu überwinden, das in dieser Hinsicht nicht unbedingt unfehlbar ist.

Bei Alinto bieten wir Produkte an, die sich an alle E-Mail-Systeme anpassen. Neben dem Spamschutz für eingehende E-Mails kümmern wir uns auch um ausgehende E-Mails, bieten einen Business Continuity Plan (BCP), Quarantäne oder Archivierungsfunktionen. Alles, was Sie brauchen, um die Sicherheit Ihrer geschäftlichen E-Mails zu verbessern. Haben Sie noch Fragen? Zögern Sie nicht, uns zu kontaktieren!



E-Mail-Verwaltung: Mehr als nur E-Mail

Die Verwaltung von E-Mails ist für ein Unternehmen von strategischer Bedeutung. Und das geht weit über das Senden und Empfangen von E-Mails hinaus. E-Mails sind ein **häufiges Einfallstor für Cyberangriffe**. Die Sicherung des E-Mail-Verkehrs erfordert daher den Einsatz von Antispam-Software, die Einrichtung eines Business Continuity Plans (BCP) und ein sicheres Hosting. Dies ist das Thema, das wir in diesem neuen Artikel behandeln werden.

#1 - Antispam und antivirus

Um die Filterung von E-Mails zu verbessern, ist es unerlässlich, sich mit einer **Antispam- und Antiviruslösung auszustatten**. Diese Tools weisen der E-Mail eine Bewertung zu, anhand derer sie als zulässig oder als Spam eingestuft oder sogar abgelehnt werden kann. Die Bewertungskriterien sind von den Administratoren parametrisierbar und können an jeden Benutzer angepasst werden. Einige Beispiele: Bild-/Textgewicht, Betreff, Absender, Inhalt... Aber auch eher technische Kriterien.

Die Sicherheitsregeln können sich mit den Bedürfnissen und Besonderheiten eines jeden Unternehmens entwickeln. Hierin liegt der Vorteil der Wahl einer **anpassungsfähigen und benutzerfreundlichen** Suite von **E-Mail-Schutzdiensten** wie Alinto Protect. Diese erhaltene Filterung ermöglicht es Ihnen auch, den Ruf Ihres Domainnamens zu schützen und von den Empfängern nicht auf die schwarze Liste gesetzt zu werden.

#2 - PCA

Wenn der E-Mail-Dienst nicht mehr erreichbar ist, wird die gesamte Geschäftstätigkeit eines Unternehmens beeinträchtigt. Ein BCP (Business Continuity Plan) ist in diesem Fall unerlässlich. Er ermöglicht es, **den Zugang zu E-Mails über ein Backup-Webmail zu gewährleisten**. Doch Vorsicht: Nicht alle E-Mail-Schutzprogramme bieten dies an. Angesichts der Zunahme von Cyberangriffen ist diese Funktion jedoch unverzichtbar.

Ein Artikel in der Zeitung Le Monde berichtet, dass nach einem Cyberangriff die ausländischen Angestellten von Bouygues construction arbeitslos wurden, da sie keinen Zugang zu ihren beruflichen E-Mails hatten. Dies ist die Art von Situation, die das sichere E-Mail-Relay Alinto Protect dank eines versicherten und rund um die Uhr überwachten BCP verhindern kann. Die Nutzer haben dann auch im Falle eines Ausfalls Zugriff auf ihre E-Mails, wodurch eine **zu große Auswirkung auf die Geschäftstätigkeit** vermieden wird.

#3 - Quarantäne

Manche E-Mails werden manchmal als Spam eingestuft, obwohl der Nutzer sie für akzeptabel hält und sie erhalten möchte. Daher ist es unerlässlich, über eine Lösung zu verfügen, die es ermöglicht, die **Kontrolle über die verschiedenen E-Mails zu behalten, die** über den Mailserver laufen.

Dies wird durch den Quarantänedienst ermöglicht. Die Benutzer erhalten eine Zusammenfassung der in Quarantäne gestellten E-Mails und können entscheiden, ob sie diese erhalten möchten oder nicht. Die Häufigkeit, mit der der Bericht gesendet wird, kann **vom Administrator angepasst werden**.

Mit Alinto Protect werden die in Quarantäne gestellten E-Mails 30 Tage lang aufbewahrt, sodass die Benutzer die Kontrolle über ihre Mailbox behalten können.

#4 - Archivierung

Um über die einfache Verwaltung von E-Mails hinauszugehen, wünschen sich manche Unternehmen ein System zur Archivierung ihrer E-Mails, oft **um gesetzliche Auflagen zu** erfüllen. Auch die Speicherung wird optimiert, indem das E-Mail-Volumen direkt auf dem Server reduziert wird, wodurch dieser manchmal nicht mehr leistungsfähig ist.

Der Archivierungsdienst von Alinto bewahrt eine unveränderbare Kopie aller Nachrichten für den eingestellten Zeitraum auf. Auch hier kann der Administrator Regeln für Domänen und/oder Benutzer festlegen und ändern.

#5 - Unterkunft

Der Standort des Hostings ist auch für Unternehmen ein sensibles Thema. Und diese Problematik wird seit der **Umsetzung der GDPR** (General Data Protection Regulation) noch verstärkt. Bei den Webgiganten ist es schwierig zu wissen, wo die Daten gehostet werden. Indem sie einen sicheren Relay-Service wie den von Alinto nutzen, haben Unternehmen die Möglichkeit, ihr Hosting selbst zu wählen, sei es in Frankreich oder in Europa.

Die Alinto-Dienste werden in privaten Clouds in Rechenzentren in Frankreich, der Schweiz, Deutschland oder Spanien gehostet. Die Kunden können sich auch dafür entscheiden, ihre Daten selbst zu hosten. **Ein ganzjähriger 24/7-Support und Wartung sind verfügbar**.

Für eine effizientere Wartung der geschäftlichen E-Mails empfiehlt sich die Anschaffung einer Software, die die in diesem Artikel aufgeführten Funktionen aufweist. Alinto bietet dies durch eine übergreifende und agile Lösung. Um mehr zu erfahren, geht es hier entlang!

Microsoft 365 Begleitung: Warum sollten Sie sich für Alinto entscheiden?

Um zu verhindern, dass die Einführung der Office 365-Suite nicht hält, was sie verspricht, und dass die Sicherheit in den Mittelpunkt Ihrer Nutzung gestellt wird, vor allem im Hinblick auf Ihre E-Mails, haben Sie sich für einen Partner entschieden.

Es ist jedoch schwierig, sich in der Fülle von Angeboten und Anbietern zurechtzufinden. In diesem Artikel geben wir Ihnen fünf Kriterien an die Hand, die Ihnen bei Ihrer Wahl helfen sollen.

#1 - Entscheiden Sie sich für Nähe

Microsoft ist ein bedeutender Softwarehersteller, der **80 % der CAC40-Unternehmen** ausstattet. Dieser Indikator sagt viel über die Stärke des Unternehmens aus, aber auch über die Anzahl der Mitarbeiter und die Fluktuation. Wenn Sie ein kleines oder mittleres Unternehmen sind und eine spezielle Betreuung benötigen, sollten Sie sich an einen Partner mit überschaubarer Größe wie Alinto wenden.

So profitieren Sie von einer persönlichen Begleitung und Betreuung durch ein Team, das Ihre Probleme kennt und **Sie bei der Einführung anleiten kann**.

#2 - Sich für Sicherheitsexpertise entscheiden

Die Beauftragung eines überschaubaren Partners bedeutet jedoch nicht, dass man sein **Fachwissen im Bereich der Sicherheit** vernachlässigen sollte. Dies ist eine große Herausforderung für Unternehmen, insbesondere mit dem Aufkommen von Telearbeit und der Digitalisierung der Unternehmen.

Mit Alinto vertrauen Sie einem Partner, der seit 20 Jahren Experte für E-Mail-Sicherheit ist. Die Gruppe deckt alle Probleme im Zusammenhang mit E-Mails ab und investiert Jahr für Jahr in Forschung und Entwicklung, um Trends in der Sicherheit und im Kampf gegen Hacker vorwegzunehmen.

#3 - Reaktivität bevorzugen

Im Zusammenhang mit der Kundennähe garantiert Ihnen die Zusammenarbeit mit einem überschaubaren Partner, dass die Supportteams schneller auf Ihre Bedürfnisse **reagieren können**. Dies ist bei größeren Partnern nicht immer der Fall, die manchmal einen Level-2-Support in Rechnung stellen, während der Level 1-Support nur von einem szenariobasierten Callcenter verwaltet wird.

Bei Alinto haben Sie sofort Zugang zu Spezialisten und wir legen Wert darauf, einen **rund um die Uhr überwachten Service** anzubieten, um die Sicherheit Ihres Unternehmens jederzeit zu gewährleisten. Darüber hinaus bieten wir einen Business Continuity Plan (BCP) für den Fall, dass Ihr E-Mail-Dienst nicht verfügbar ist. All dies in einem leistungsstarken Servicepaket ohne zusätzliche Kosten.

#4 - Vertrauen Sie auf Objektivität

Warum vertrauen Sie bei der Bereitstellung von Office 365 nicht einfach auf Microsoft? Das ist oft der erste Gedanke, der auf der Hand liegt. Wenn Sie sich jedoch für einen externen Partner entscheiden, erhalten Sie eine **objektive Begleitung, die ganz auf Ihre Bedürfnisse und nicht auf kommerzielle Ziele ausgerichtet ist**.

Wir bei Alinto kennen alle wichtigen E-Mail-Dienste und unsere Schutzlösung passt sich an jeden einzelnen an. Wir haben daher kein Interesse daran, Ihnen einen bestimmten Messenger zu empfehlen. Wir basieren auf Ihren Bedürfnissen und Besonderheiten, um **Ihnen die beste Lösung anzubieten**.

#5 - Hosting in Frankreich wählen

Wenn Sie Ihre Daten in Europa oder sogar in Frankreich hosten möchten, sich aber nicht selbst darum kümmern wollen, können Sie Ihren Partner mit dem Hosting beauftragen. Stellen Sie die **Souveränität Ihrer Daten** sicher, denn sie sind wertvoll, lesen Sie das Kleingedruckte!

Unsere Alinto-Dienste befinden sich in Frankreich, der Schweiz, Deutschland und Spanien. Wir entwickeln unsere Infrastrukturen kontinuierlich weiter, um ein **Höchstmaß an Ausfallsicherheit und Sicherheit zu** bieten. Es liegt uns am Herzen, einen souveränen Service zu gewährleisten, der eine sehr hohe Verfügbarkeit bietet.

Sie haben nun alle Karten in der Hand, um Ihren Partner auszuwählen und sich bei der Einrichtung Ihres sicheren E-Mail-Systems und der Office 365-Suite begleiten zu lassen. Wie wäre es mit einem Gespräch?

Schlussfolgerung

Es gibt keinen Grund, warum E-Mail das schwächste Glied in Office 365 sein sollte, solange es gut geschützt ist. Und dafür gibt es dedizierte Lösungen: sowohl durch das Verhalten der Nutzer als auch durch die Verwendung der richtigen Sicherheitssoftware...

Über

Alinto wurde im Jahr 2000 gegründet und ist ein Unternehmen, das sich auf E-Mail-Berufe spezialisiert hat: E-Mail-Dienst im SaaS-Modus, Anti-Spam, E-Mail-Server... über mehrere Produkte :

- **Alinto Protect**: Das sichere E-Mail-Relais, das gegen die Risiken des Internets immun macht, indem es einen ständigen Zugriff auf E-Mails gewährleistet.
- **Alinto Gateway**: Das SMTP-Mail-Relay ermöglicht es Servern oder Anwendungen, E-Mails zu versenden, um einen sogenannten «sauberen» Datenverkehr zu gewährleisten.

Alinto ist in Frankreich, der Schweiz und Spanien vertreten, hat mehr als 30 Mitarbeiter und bietet mehr als drei Millionen Nutzern einen qualitativ hochwertigen Service. Über 15 Millionen E-Mails werden täglich über seine Messaging-Dienste versendet.

Die Alinto-Gruppe vereint seit 2016 mehrere Einheiten, um sich als wichtiger Akteur im Bereich E-Mail zu positionieren. Sie besteht aus den folgenden Unternehmen:

- **Cleanmail**: Schweizer Unternehmen, das seit 2002 auf Spam-Filter in der Cloud spezialisiert ist.
- **SerenaMail**: spanischer Spezialist für E-Mail-Sicherheit (Spam-Filter).
- **Alinto**: Sichere E-Mail-Dienste.

Dies ermöglicht es der Gruppe, ihre Marktposition zu stärken und ihre internationale Entwicklung auszubauen.

Lyon (siège)
15 quai Tilsitt
69002 Lyon
+33 481 09 01 10

Paris
31 rue de Reuilly
75012 Paris
+33 141 58 15 33

Madrid
Calle Aniceto Marinas, 48
28008 Madrid
+34 91 005 29 64

Barcelone
Avda. Diagonal, 434
08037 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Alinto

www.alinto.com