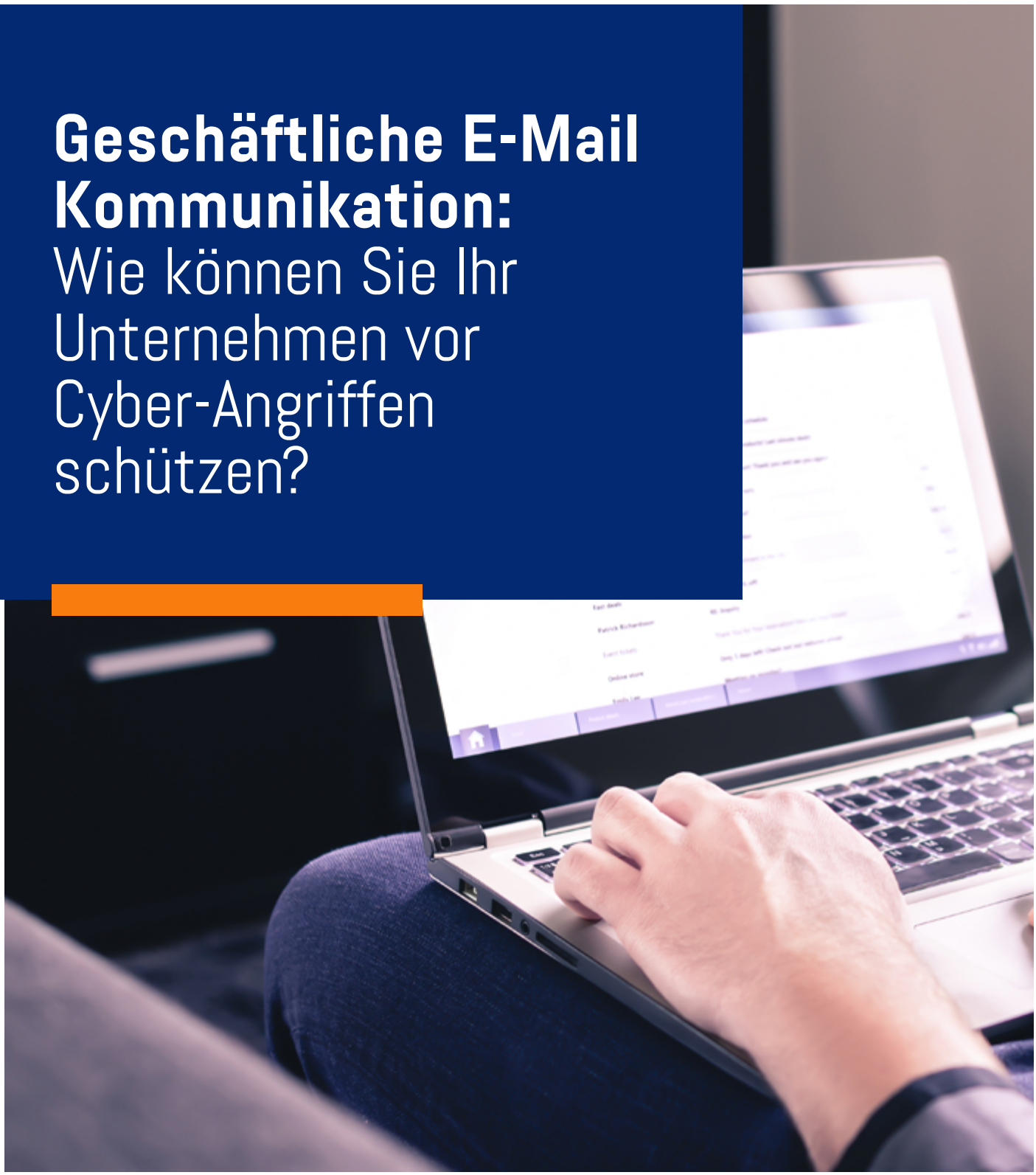
Alinto

Whitepaper

November 2021

Geschäftliche E-Mail Kommunikation: Wie können Sie Ihr Unternehmen vor Cyber-Angriffen schützen?



Inhaltsverzeichnis

Die Maschen des Netzes enger ziehen

Nur eines von zwei Unternehmen gibt an, für den Fall eines Cyberangriffs gerüstet zu sein[1]. Dies ist eine traurige Tatsache, die Unternehmen dazu veranlasst, die Sicherheit ihres IT-Netzes und vor allem ihrer geschäftlichen E-Mails zu überdenken.

Die Mehrzahl der Cyberangriffe erfolgt über betrügerische E-Mails. Und die von den Hackern eingesetzten Techniken und Technologien werden immer raffinierter. Sie zielen auf alle Unternehmen ab: von kleinen Unternehmen bis hin zu multinationalen Konzernen, wobei sie das geringe Bewusstsein der Mitarbeiter für bösartige E-Mails ausnutzen.

Die sorgfältigsten Unternehmen setzen strenge Sicherheitssysteme ein: Firewalls, Patching, Anti-Spam usw. Dennoch haben diese Schutzmaßnahmen, die häufig mit den vorhandenen Netzwerk-, System- und Messaging-Lösungen verbunden sind, ihre Grenzen. Eine E-Mail kann durch diese Sicherheitsnetze schlüpfen.

In diesem Whitepaper werfen wir einen Blick auf Cyberangriffe, stellen bewährte Verfahren zur Verbesserung der E-Mail-Sicherheit vor und geben Tipps, wie Sie Ihr Unternehmen besser schützen können.

[1] 6. Ausgabe des jährlichen CESIN-Barometers

E-Mail-Sicherheit: Eine Bestandsaufnahme

Es kann nicht genug betont werden, dass E-Mails der bevorzugte Angriffspunkt für Cyber-Attacken sind. Und dies nimmt Jahr für Jahr zu, trotz Verbesserungen in der Sicherheit von privaten und geschäftlichen E-Mails, Sensibilisierung der Nutzer und Warnungen vor Phishing und Cyberangriffen. Cyberkriminelle verwenden immer ausgefeiltere Schadenssoftware, und ihre Techniken werden immer raffinierter und technisch ausgereifter.

Ransomware, Phishing, Malware... sind allesamt Bedrohungen für Unternehmen. Diese müssen besonders vorsichtig sein und ihre Mitarbeiter ständig für diese Gefahren sensibilisieren. Dies ist heute um so wichtiger, da Cyberkriminelle auf der Coronavirus-Pandemie surfen und Angst als Klickreiz nutzen.

Um die Situation besser zu verstehen, haben wir eine Bestandsaufnahme gemacht.

Cybersicherheit: der besorgniserregende Anstieg von E-Mail-Angriffen

Bis 2020 haben sich die Cyberangriffe im Vergleich zu den Vorjahren vervierfacht[1]. Cyberkriminelle sind heute besser organisiert, verschicken zahlreiche betrügerische E-Mails und zielen auf Schwachstellen in den IT-Netzen der Unternehmen ab. Die Angriffe sind industrialisiert und geplant. Wir sind weit davon entfernt, dass eine Einzelperson allein im dunklen Kämmerlein hinter seinem Computer agiert.

Hier einige Statistiken aus Frankreich zur Veranschaulichung der aktuellen Situation und der Gefährdung im Zusammenhang mit der Email-Kommunikation:

- 11 % des Gesamtvolumens bösartiger E-Mails[2] entfallen auf Ransomware.
- 80 % aller Cyberangriffe auf französischen Unternehmen im Jahr 2020 erfolgten über Phishing-E-Mails oder Spear-Phishing[3].
- Im Jahr 2020 gab eines von fünf Unternehmen an, im Laufe des Jahres mindestens einen Ransomware-Angriff erlitten zu haben[4].
- Nur jedes zweite Unternehmen ist zuversichtlich, dass es in der Lage ist, einen Cyberangriff zu bewältigen[5].

- Die Gesundheitskrise bringt neue Risiken mit sich: 35 % Anstieg der Cyberangriffe[6].
- 57 % der Unternehmen planen, ihr Budget für Cybersicherheit zu erhöhen[7].
- 85 % der Unternehmen wollen neue technische Lösungen erwerben, um ihre IT-Sicherheit zu verbessern[8].
- 75 % der empfangenen E-Mails sind unerwünscht[9].
- Die Meldungen an die Regierung über Cyberangriffe sind im Vergleich zu 2019 um 30 % gestiegen[10].

Die Entwicklung der Telearbeit, die durch die Pandemie ausgelöste Angst, die Entwicklung der Cloud und die Professionalisierung der E-Mail-Angriffe erklären diese Entwicklung. Nichts deutet auf eine Trendwende hin: Das Phänomen dürfte sich in den kommenden Jahren fortsetzen und ein echtes Problem für Unternehmen bleiben.

Cyberangriffe: erhebliche Auswirkungen für Unternehmen

Die Kosten eines Cyberangriffs lassen sich nur schwer abschätzen. Diese spiegeln nicht nur die wirtschaftlichen Folgen, sondern auch Auswirkungen auf den Ruf des Unternehmens, die Schwächung der IT-Infrastruktur oder betrieblichen Schwierigkeiten wieder.

Im Jahr 2020 hatten 58 % der Cyberangriffe nachweislich Auswirkungen auf das Geschäft, wobei in 27 % der Fälle die Produktion direkt gestört wurde[11].

Die wichtigsten Folgen der Angriffe[12] lassen sich wie folgt aufschlüsseln:

- Datendiebstahl (30%)
- Denial of Service (29%)
- Blockieren der Geschäftsaktivitäten nach Verschlüsselung der Daten durch Ransomware (24 %)
- Identitätsdiebstahl (23%)

Eine Studie der Firma Bessé zeigt, dass das Risiko des Scheiterns eines Unternehmens in den drei Monaten nach Bekanntgabe eines Cyberangriffs um 50 % steigt. In manchen Fällen kann dieses Risiko kann sogar 80 % erreichen[13].

Eine andere Studie des IBM Ponemon Institute ergab, dass 80 % der französischen Unternehmen keinen Plan für das Management von Zwischenfällen haben. Eine weitere wichtige Erkenntnis ist, dass es rund 200 Tage dauert, bis ein Unternehmen erkennt, dass es Opfer eines Cyberangriffs geworden ist. Die direkten Folgen können auch die Kunden treffen, wenn ihre persönlichen Daten gestohlen wurden.

Ein harmloser Klick auf einen Link in einer E-Mail kann daher das gesamte Unternehmen unwiederbringlich schwächen und schädigen. Deshalb ist es wichtig, das Bewusstsein der Mitarbeiter zu schärfen, aber auch die IT-Sicherheit durch spezielle E-Mail-Schutzlösungen zu stärken.

---

[1] Cyberangriffe haben sich im letzten Jahr vervierfacht, sagt ein Experte für Cybersicherheit - France TV info
[2] Intervention Devensys - Methoden zur Verbesserung Ihrer E-Mail-Sicherheit 2018
[3] Die häufigsten Cyber-Attacken gegen französische Unternehmen – Statista
[4 bis 8] 6. Ausgabe des jährlichen CESIN-Barometers
[9] Nachrichtenübermittlung: Zahlen und Bedrohungen - Sicherheitsbeauftragte
[10] Cybersicherheit: mehr Berichte im Jahr 2020 - vie-publique magazine
[11] 6 Ausgabe des jährlichen CESIN-Barometers
[12] Die häufigsten Cyber-Attacken gegen Unternehmen, CESIN und OpinionWay
[13] In einem Gremium von KMU

Einige Beispiele für Cyberangriffe und deren Auswirkungen:

- Ein Krankenhaus in New Jersey (USA) zahlte ein Lösegeld von über 600.000 Dollar (2020).

- Verne Harnish, CEO von Gazelles Inc., wurden 400.000 US-Dollar von seinem Bankkonto gestohlen, als sich Hacker Zugang zu seinem Computer verschafften und E-Mails zwischen ihm und seiner Assistentin abfangen konnten (2019).

- EasyJet hat bekannt gegeben, dass das Unternehmen Opfer eines groß angelegten Cyberangriffs geworden ist: Mehr als 9 Millionen Kundendaten (E-Mail-Adressen und Reiseinformationen), darunter 2.000 Kreditkartendaten wurden unrechtmäßig eingesehen (2020).

- Die Universität von Kalifornien in San Francisco (UCSF) war von einem Ransomware-Angriff betroffen, der den Zugang zu den Daten in ihrem Computernetzwerk lahmlegte Schließlich willigte die Universität ein, ein Lösegeld in Höhe von etwa einer Million Euro (2020) zu zahlen.

Vier bewährte Verfahren zur Vermeidung von Cyberangriffen auf E-Mails

E-Mails sind und bleiben der bevorzugte Einstiegspunkt für Hacker im Internet. Die durch die Pandemie verursachte massive Zunahme der Telearbeit hat die Zahl der Angriffe, insbesondere durch Ransomware, nach oben getrieben. In der Tat, der Experts Club für Information und digitale Sicherheit (Cesin) schätzt, dass bis 2020 57 % der Unternehmen Opfer eines Cyberangriffs geworden sind. Eine Vervierfachung innerhalb nur eines Jahres! Doch das muss nicht sein! Es gibt Lösungen, um Ihr Unternehmen vor diesen Angriffen zu schützen. Dies erfordert die Umsetzung mehrerer bewährter Praxistipps, die wir in diesem Artikel liefern.

Bewährte Praxis Nr. 1
Sensibilisierung der Mitarbeiter

Als Erstes sollten Sie Ihre Mitarbeiter über die Risiken von Cyberangriffen und die Folgen, die sie für das Unternehmen haben können, informieren. Dazu gehört, dass Sie ihnen erklären, woran sie eine verdächtige E-Mail erkennen und welche Vorkehrungen sie treffen müssen, um den Zugang zu ihren E-Mails zu sichern. Halten Sie Ihre Mitarbeiter dazu an, sichere Passwörter festzulegen, das Senden und Öffnen von Anhängen zu beschränken, nicht auf verdächtig erscheinende Links zu klicken, keine vertraulichen Informationen preiszugeben, die Identität des Absenders zu überprüfen usw.

Es ist auch wichtig zu betonen, die IT-Abteilung zu benachrichtigen, sobald ein Verdacht auf eine betrügerische E-Mail besteht. Die Reaktion muss schnell erfolgen, damit die entsprechenden Maßnahmen rechtzeitig eingeleitet werden können, bevor sich der Virus ausbreitet und erheblichen Schaden anrichten kann.

Gute Praxis #2
Schutz von sensiblen Daten

Seit der Umsetzung der DSGVO haben Fragen der Cybersicherheit für Unternehmen noch mehr an strategischer Bedeutung gewonnen. Die Sicherheit des Zugangs zu den Informationssystemen und zu personenbezogenen Daten muss gewährleistet sein.

Um Daten zu schützen, ist es unerlässlich, eine strenge Politik zur Verwaltung von Passwörtern einzuführen. Dies ist der erste Hebel, um die Computer Ihrer Mitarbeiter zu schützen. Die Passwörter müssen komplex, schwer zu erraten und vertraulich sein und sollten regelmäßig erneuert werden.

Für mehr Sicherheit sollten Sie die Computer Ihrer Mitarbeiter so einrichten, dass sie sich nach einigen Minuten der Inaktivität automatisch sperren. Außerdem ist es wichtig, Dateien mit sensiblen Daten zu schützen und den Zugriff nur befugten Personen zu gestatten.

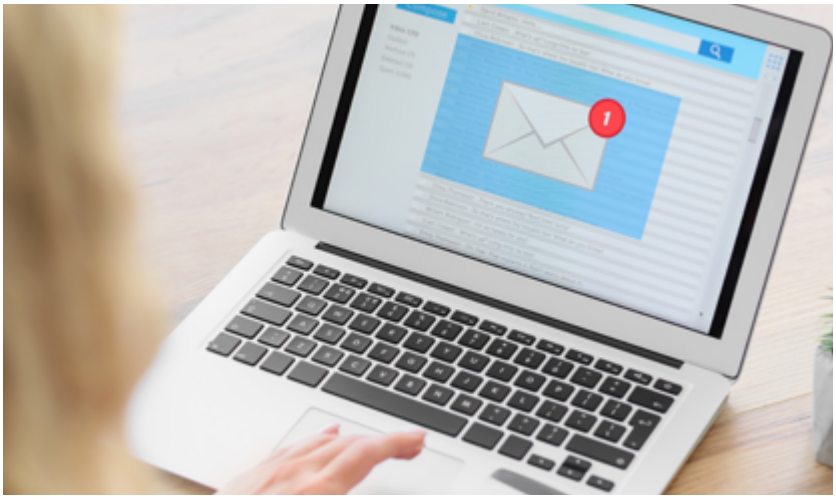
Um die Informationssysteme zu sichern, ist es außerdem wichtig, sensible Daten wie zB Gesundheitsdaten, Zahlungsinformationen usw. zu verschlüsseln. All diese Präventivmaßnahmen gehen Hand in Hand mit dem Schutz der Netzinfrastruktur durch die Installation von Firewalls, Filter-Routern, Anti-Intrusion-Probes, Lastausgleichssystemen und der Erkennung von DDoS-Angriffen usw.

Gute Praxis #3
Kontrolle über den E-Mail-Verkehr

Die E-Mail ist nach wie vor der meistgenutzte Kommunikationskanal der Welt. Die Nutzer erhalten täglich Hunderte von E-Mails. Das ist nicht nur anstrengend und ineffizient, sondern hat auch erhebliche Auswirkungen auf das Risiko von Cyberangriffen. Wie unser Bericht zur E-Mail-Sicherheit zeigt, sind mehr als 75 % der E-Mails unerwünscht.

Aus diesem Grund ist die Kontrolle des E-Mail-Verkehrs von größter Bedeutung: Es muss sichergestellt werden, dass betrügerische E-Mails vor den Toren des Informationssystems (IS) des Unternehmens bleiben. Die Filterung muss jedoch fein und präzise sein, damit gültige E-Mails, die für die Mitarbeiter relevant sind, nicht unnötig aussortiert werden.

Deshalb ist es wichtig, Filterregeln einzurichten und ständig anzupassen, White- und Blacklists zu führen und E-Mails, die nicht betrügerisch sind, aber im Verdacht stehen, kommerziell zu sein, in eine Quarantänezone zu stellen. Die Nutzer können darauf zugreifen, damit sie keine wichtigen Informationen zu verpassen.



Gute Praxis #4
Einsatz einer E-Mail-Sicherheitslösung

Um die Sicherheit Ihrer geschäftlichen E-Mails zu erhöhen, ist es unerlässlich, eine E-Mail-Schutzsoftware (z. B. Antispam oder Antivirus) einzusetzen. Diese Lösungen werden regelmäßig aktualisiert, wenn neue Cyberangriffe bekannt werden. Sie passen sich perfekt an die verschiedenen professionellen E-Mail-Lösungen an, angefangen bei Microsoft 365 Exchange. Diese Tools filtern Spam anhand mehrerer Kriterien, setzen bestimmte Absender automatisch auf eine schwarze Liste und schützen den Ruf Ihrer Emaildomäne (beim Versand von Massen-E-Mails usw.).

Die Anbieter von E-Mail-Lösungen bieten integrierte Anti-Spam-Lösungen an, die jedoch nicht immer (oder nur selten) ausreichend sind. Es ist daher unerlässlich, einen verstärkten Schutz durch spezielle Tools wie Alinto Protect / Cleanmail zu gewährleisten. Die Vorteile sind zahlreich: E-Mail-Schutz, sauberer E-Mail-Posteingang, feine Filterung, Quarantäneverwaltung, Zeitersparnis bei der E-Mail-Verwaltung ...

Schreiben Sie alle bewährten Praxis-Tipps in einem Dokument nieder, das Ihren Mitarbeitern zur Verfügung steht, um sie an diese vier wesentlichen Empfehlungen zu erinnern. Die Kommunikation und die Sensibilisierung des Teams sind für einen optimalen Schutz Ihrer geschäftlichen E-Mails ebenfalls unerlässlich.

Warum reicht der eingebaute Antispamfilter von E-Mail-Lösungen nicht aus?

Viele Unternehmen verwenden die mit ihren E-Mail-Lösungen angebotene Antispam-Software. Sie sehen keine Notwendigkeit, eine weitere Lösung hinzuzufügen. Manche verwenden nicht einmal eine solche Software! Dies ist jedoch ein echtes Problem für Unternehmen, da E-Mails der Haupteinstiegspunkt für Cyberangriffe sind.

Neben der Sensibilisierung der Mitarbeiter für die richtigen Vorgehensweisen, um betrügerische E-Mails zu erkennen, ist es wichtig, die Sicherheit Ihres professionellen E-Mail-Systems zu erhöhen. In vielen Fällen reicht die von Ihrem Provider angebotene Antispam-Software nicht aus. Wir sagen Ihnen, warum.

Integrierter Spam-Schutz ist nicht effizient genug

In E-Mail-Systeme integrierte Anti-Spam-Software filtert unerwünschte E-Mails anhand allgemeiner, vordefinierter Filterregeln heraus. Diese Regeln sind schwer zu verwalten und lassen sich nicht ohne Weiteres an die Bedürfnisse der Benutzer und an das plötzliche Auftreten neuer Bedrohungen anpassen. Es handelt sich daher um einen unvollständigen Schutz des E-Mail-Systems, der E-Mails blockiert, die von Spamlisten kommen, fragwürdige Betreffzeilen oder Anhänge haben.

Der Beweis: 2016 versandte AV Comparatives 127.800 Spam-Nachrichten an Konten, die bei E-Mail-Dienstleistern geführt wurden. Die Erkennungsraten waren sehr niedrig: 89,87 % des Spams kamen bei einem der Anbieter an. Dies zeigt, wie wichtig es ist, sich nicht mit den Basisversionen - die scheinbar kostenlos sind, zumindest ohne zusätzlichen Kosten – zufriedenzugeben, sondern eine leistungsfähigere Zusatzlösung anzuschaffen.

Die leistungsstarken Plus-Versionen sind sehr teuer

Natürlich bieten E-Mail-Anbieter erweiterte, kostenpflichtige Versionen ihrer Anti-Spam-Software an (z. B. Microsoft Advanced Threat Protection / Microsoft 365 Defender). Diese bieten weitergehende Funktionen. Sie können zum Beispiel von den Administratoren konfiguriert werden (Anzeige, Änderung, Konfiguration). Es ist auch möglich, benutzerdefinierte Regeln für jeden Benutzer zu erstellen, die immer Vorrang vor den generellen Einstellungen haben.

Diese Versionen bieten auch automatisierte Prozesse mithilfe von künstlicher Intelligenz. Sie gehen noch einen Schritt weiter und identifizieren Werbekampagnen, die der Filterung der ersten Stufe entgehen. Es sind auch Dashboards verfügbar, um die Entwicklung des E-Mail-Verkehrs und die Anzahl von Spam, Junk-Mails usw. analysieren zu können.

Diese Lösungen sind jedoch recht teuer und werden nach der Anzahl der Nutzer abgerechnet. Im Durchschnitt müssen Sie mit mehreren Dutzend Euro pro Monat und pro Benutzer rechnen. Rechnen Sie das anhand Ihrer Mitarbeiterzahl aus: Das ist ein erheblicher Betrag für Unternehmen, die es manchmal vorziehen, darauf zu verzichten. Auf diese Weise überlassen sie den Cyberkriminellen ein freies Feld.

Antispam: Welche Unterstützung bietet Ihr E-Mail-Anbieter?

Beliebte Anbieter von Business-E-Mail-Anbieter sind manchmal Opfer ihres eigenen Erfolgs. Die Kehrseite der Medaille: Ihr Support ist nur schwer erreichbar oder verfügbar. Im Falle eines Vorfalls ist es wichtig, Zugang zu einem effizienten und reaktionsschnellen Support zu haben. Darüber hinaus ist es oft notwendig, diese Lösungen mit Hilfe von Integratoren zu implementieren, was die direkte Beziehung zum Hersteller einschränkt.

Wenn Sie sich an einen überschaubaren Anbieter von Antispam-Lösungen wie Alinto wenden, haben Sie alle Chancen auf einen reaktiven, zugänglichen Partner, der sich Ihrer Probleme bewusst ist. Dies ist ein nicht zu unterschätzender Vorteil, wenn man bedenkt, welche Folgen eine Nichtverfügbarkeit von E-Mails oder eine Cyberattacke haben kann. Informieren Sie sich gut, bevor Sie Ihre Wahl treffen, denn nicht alle Anbieter bieten das gleiche Maß an Betreuung und Support.

Auch wenn die großen professionellen E-Mail-Anbieter standardmäßig einen Spam-Schutz anbieten, ist es unerlässlich, die Sicherheit der E-Mail-Postfächer Ihrer Mitarbeiter zu erhöhen. Es steht Ihnen eine breite Palette von ergänzenden Lösungen zur Verfügung. Um die richtige Wahl zu treffen, sollten Sie eine Liste von Kriterien aufstellen, die Sie für unverzichtbar halten: Support, Funktionalität, Ergonomie, Kundennähe, Preisgrundlagen usw. Vergessen Sie das nicht: Es ist die Software, die sich an Ihre Herausforderungen anpasst und nicht umgekehrt!

Fünf wichtige Funktionen für Ihre E-Mail-Sicherheitslösung

Sie sind davon überzeugt: Sie brauchen zusätzlichen Schutz für Ihre berufliche Mailbox. Es ist jedoch schwierig, sich unter den verfügbaren Lösungen zu entscheiden. Zwischen den direkt in den E-Mail-Dienst integrierten Anti-Spam-Lösungen und zusätzlicher Software sind Sie unschlüssig.

Unserer Ansicht nach sind fünf Funktionen unverzichtbar. Sie müssen von Ihrem zukünftigen Anbieter unbedingt angeboten werden. Hier sind sie.

Funktion Nr. 1
Filterung von eingehenden E-Mails

Natürlich muss Ihre künftige E-Mail-Sicherheitssoftware Ihnen eine leistungsfähige Filterung eingehender E-Mails bieten. Dies geschieht durch mehrere Methoden:

- Reputationsbasierte E-Mail-Filterung: Filterung bekannter Spammer, Abfrage von internationalen Reputationsdatenbanken ...
- Weiße Liste (oder Whitelist): Auswahl der Absender, deren E-Mails das Unternehmen akzeptiert.
- Schwarze Liste (oder Blacklist): Liste der Absender, deren E-Mails das Unternehmen ablehnt.
- Inhaltsanalyse: Blockierung einer Nachricht auf der Grundlage ihres Inhalts (Analyse von Wörtern, Links, Bildern, Anhängen usw.).

Für noch mehr Flexibilität und Anpassungsfähigkeit sollten Sie sich für eine Lösung entscheiden, die es Ihnen ermöglicht, Filter einfach zu ändern, anzupassen, zu löschen oder hinzuzufügen, mit wenigen Klicks und entsprechend den Bedürfnissen Ihrer Endbenutzer.

Funktion #2
Antispam und Antivirus

In Bezug auf die erste Funktion ist es wichtig, eine Sicherheitslösung zu wählen, die mit einem leistungsfähigen Anti-Spam- und Anti-Virus-System ausgestattet ist. Denn während die erste Funktion die Legitimität des Absenders sicherstellt, kann dieser unwissentlich Spam oder einen Virus versenden. Die Nachricht muss daher eingehend analysiert werden. Viele unerwünschte E-Mails schaffen es, die in E-Mail-Lösungen integrierten Anti-Spam-Tools zu umgehen und in den Posteingängen Ihrer Benutzer zu landen.

Entscheiden Sie sich für eine Lösung, die auf leistungsstarken Technologien basiert, die international genutzte Datenbanken abfragt, aber auch ihre eigenen Spam-Datenbanken nutzt, die sich an die lokale Semantik anpasst und die E-Mails an verschiedene Antivirenprogramme weiterleitet, um Cyber-Bedrohungen besser zu filtern.

Damit die Software genau bestimmen kann, ob es sich bei der empfangenen E-Mail um Spam handelt, analysiert sie mehrere Elemente der E-Mail: Links, Betreff, Anhänge, Bilder usw. nach festgelegten Kriterien.

Funktion #3
Schutz Ihres Rufes

Es ist wichtig, dass Ihr Domänenname einen guten Ruf hat, damit die von Ihren Nutzern gesendeten E-Mails, insbesondere kommerzielle E-Mails, nicht als Spam eingestuft werden. Zu diesem Zweck wird ein Absender-Score erstellt. Dabei werden mehrere Elemente berücksichtigt, wie zB die harte oder weiche Bounce-Rate, Öffnungsraten, Spam-Beschwerden, die regelmäßige Bereinigung Ihrer Datenbanken, die Verwendung von Identifizierungsprotokollen und die Qualität Ihrer E-Mails (vermeiden Sie Anhänge, Bilder oder Betreffzeilen, die zu werblich sind).

Der Zweck der Absenderbewertung besteht darin, zu verhindern, dass Sie in Blacklist-Datenbanken landen, und die Zustellbarkeit der E-Mails Ihrer Mitarbeiter zu erhöhen.

Funktion #4
Der Geschäftskontinuitätsplan

Wenn ein Unternehmen nicht auf sein E-Mail-Postfach zugreifen kann, kann dies verheerende Folgen haben. Genau das kann jedoch bei einem Systemausfall oder der Nichtverfügbarkeit einer IT-Infrastruktur passieren.

Deshalb raten wir Ihnen, eine E-Mail-Lösung mit einem Business Continuity Plan (oder BCP) zu wählen. Auf diese Weise können Ihre Nutzer ihre Postfächer über ein Webmail-Backup-System in völliger Transparenz weiter nutzen und sind nicht vom Ausfall des Mailservers betroffen, selbst wenn dieser in der Cloud eines großen Anbieters steht. Keiner von ihnen garantiert oder kann eine tatsächliche 100%ige Verfügbarkeit anbieten.

Außerdem wird, sobald der Zugriff auf den Server wieder möglich ist, der während des Ausfalls erfolgte E-Mail-Austausch wieder mit der Mailbox synchronisiert, sodass keine Informationen verloren gehen. Ein echter Bonus.

Funktion #5
Integration in die bestehende Umgebung

Neben den Funktionen kann auch eine einfache Bereitstellung des Service den Unterschied ausmachen. Wählen Sie eine E-Mail-Sicherheitslösung, die sich an Ihre Arbeitsumgebung anpasst: E-Mail-Anbieter, Hosting, Bedarf an benutzerdefinierten Regeln, Autonomie bei der Nutzung der Lösung, Verfügbarkeit von APIs usw.

Dies ist unerlässlich, um den Schutz Ihrer E-Mails zu verstärken und eine unabhängige Verwaltung zu gewährleisten. Ob On-Premises oder in der Cloud, vor Ort oder ausgelagert, Ihre künftige Lösung soll sich an Ihre Anforderungen anpassen, nicht andersherum.

Natürlich ist diese Liste der «Muss»-Funktionen nicht vollständig. Unserer Meinung nach sind dies jedoch die wesentlichen Kriterien, die Sie bei der Auswahl einer Sicherheitslösung für Ihre geschäftlichen E-Mails berücksichtigen sollten. Wenn Sie mehr darüber wissen möchten, kontaktieren Sie uns doch.

Welche Unterstützung ist für die Einrichtung eines Anti-Spam-Systems erforderlich?

Wie wir bereits gesehen haben, sind die Funktionen Ihrer E-Mail-Sicherheitssoftware von entscheidender Bedeutung. Aber es gibt noch einen weiteren wichtigen Aspekt, den Sie berücksichtigen sollten: den Support. Ob während der Konzeption und des Scopings Ihres Projekts, während der Bereitstellung der Lösung oder bei neuen Fragen im Anschluss daran, Sie sollten einen lokalen Dienstleister wählen, der als echter Partner agiert.

Und das ist es, was wir bei Alinto bieten! Erfahren Sie, wie wir die Unterstützung unserer Kunden in den Mittelpunkt unserer Lösung stellen.

Antispam-Software : Fachwissen und Unterstützung steht an erster Stelle

Es ist nicht nötig, es zu wiederholen: Der Schutz Ihrer geschäftlichen E-Mails ist für Ihr Unternehmen von strategischer Bedeutung. Daher ist es wichtig, sich an einen Partner zu wenden, der dies in seiner DNA hat und der über ein echtes Wissen über E-Mail-Sicherheit verfügt. Und genau das ist die Stärke von Alinto.

Seit mehr als 20 Jahren begleiten die Experten von Alinto Unternehmen bei der Verwaltung ihrer geschäftlichen E-Mail-Systeme. Wir erfüllen ihre Erwartungen, verfolgen die Entwicklungen und Trends in Bezug auf Cyberangriffe und bieten immer fortschrittlichere Funktionalitäten an. Wir investieren 30 % unseres Umsatzes für Forschung und Entwicklung, um immer besser Lösungen anzubieten und die E-Mails unserer Kunden zu sichern. Durch mehrere Übernahmen von Unternehmen, die sich auf E-Mail-Sicherheit spezialisiert haben, verfügen wir über alle notwendigen Kompetenzen und Kenntnisse, um den Schutz Ihrer E-Mail-Postfächer und darüber hinaus Ihrer Informationssysteme zu gewährleisten.

Der Kundendienst und die Supportabteilung sind der Dreh- und Angelpunkt unseres Unternehmens. Dank eines Ticketingsystems werden unsere Experten in Echtzeit über die von ihren Kunden angetroffenen Situationen alarmiert. So können sie innerhalb eines risikogerechten Zeitrahmens eine Antwort geben oder die der Problematik angemessenen Entscheidungen treffen.

Einsatz von Anti-Spam-Lösungen: Reaktionsschnelligkeit ist das Schlüsselwort

In Verbindung mit dem Kundensupport stehen Ihnen die Beratungsteams von Alinto während aller Phasen Ihres Projekts zur Verfügung. Im Vorfeld, indem wir Ihnen helfen, Ihr Projekt zu planen. Während der Implementierung, indem wir Sie bei der Installation der Software und der Konfiguration der erforderlichen Funktionen begleiten. Und im Nachhinein, mit der Beantwortung Ihrer Fragen, der Wartung, dem Support ...

Dank der menschlichen Größe und der Stabilität unserer Teams kennen wir unsere Kunden und ihre Herausforderungen sehr gut. So reagieren wir schnell auf unterschiedliche Bedürfnisse, kommunizieren effizient zwischen unseren verschiedenen Abteilungen, um eine passende und schnelle Lösung zu bieten. Unsere Software und damit Ihr Schutz profitieren von dieser Agilität. Wir wissen, wie problematisch die Unterbrechung Ihres E-Mail-Dienstes sein kann. Daher ist Proaktivität das Schlüsselwort für unsere Dienstleistungen.

Mehr als nur Anti-Spam : Optimierung der Verwaltung des E-Mail-Systems

Um Ihre geschäftlichen E-Mails zu schützen, reicht es nicht aus, eine Anti-Spam-Software zu installieren, auch wenn dies unerlässlich ist. Es ist wichtig, darüber hinauszuschauen, um die Verwaltung und den Schutz Ihrer E-Mails zu optimieren. Wählen Sie daher eine Software, die zusätzliche Funktionen bietet.

Bei Alinto bieten wir zusätzlich zum Anti-Spam- und Anti-Virus-Schutz :

- Eine Lösung für die E-Mail-Archivierung, die für die Einhaltung der gesetzlichen Vorschriften nützlich ist. Sie wählen aus, was Sie aufbewahren möchten und was nicht, Sie können die Regeln und die Häufigkeit ändern ... und werden benachrichtigt, bevor die E-Mails gelöscht werden.

- Ein SMTP-Mail-Relay, um sicherzustellen, dass Sie «saubere» E-Mails versenden und den Ruf Ihrer E-Mail-Domäne nicht gefährden.

- E-Mail-Verschlüsselung, die ausgehende E-Mails mit einem Verschlüsselungssystem sichert, wird in einer Reihe von Branchen für den Datenaustausch benötigt. Nur Administratoren sind von der Verschlüsselung betroffen, die für die Nutzer völlig transparent bleibt.

- Fax- und SMS-Cloud-Services, um eine einzige Lösung für alle Ihre Kommunikationskanäle zu bieten. Dank der APIs oder direkt per E-Mail erhalten Sie das gesamte Know-how von Alinto, um Ihre Faxe und SMS zu entmaterialisieren.

Alinto bietet auch andere Dienstleistungen rund um die E-Mail an. Mit einem gemeinsamen Merkmal: Kundennähe! Sie haben ein Projekt oder Fragen? Zögern Sie nicht, uns zu kontaktieren!

Schlussfolgerung

Angesichts der Bedrohung durch immer hinterhältigere Cyberangriffe ist der Schutz von Geschäfts-E-Mails für Unternehmen keine Option mehr! Und es reicht nicht mehr aus, sich mit Standardversionen von Antispam-Software zu begnügen.

Aus diesem Grund ist die Entscheidung für eine E-Mail-Schutzsoftware für Unternehmen die beste Option, um alle, Chancen auf Ihrer Seite zu haben. Außerdem ist es wichtig, die Mitarbeiter zu sensibilisieren, über Best-Practices im Alltag zu informieren und Trends im Bereich Cybersicherheit zu beobachten und zu antizipieren.

Über uns

Alinto wurde im Jahr 2000 gegründet und ist ein Unternehmen, das sich auf E-Mail-Lösungen spezialisiert hat: E-Mail-Service im SaaS-Modus, Anti-Spam, E-Mail-Server... mit verschiedenen Produkten:

- **Alinto Protect / Cleanmail:** das sichere E-Mail-Relay, das gegen Internet-Risiken immunisiert, und permanenten Zugriff auf E-Mails gewährleistet.

- **Alinto Gateway / Serenamail:** Das SMTP-Mail-Relay ermöglicht es Servern oder Anwendungen, E-Mails zu senden und einen «sauberen» Datenverkehr zu gewährleisten.

Alinto ist in Frankreich, der Schweiz und Spanien vertreten, beschäftigt mehr als 30 Mitarbeiter und bietet mehr als drei Millionen Nutzern einen hochwertigen Service. Dank seiner E-Mail-Dienste werden täglich mehr als (15) 20 Millionen E-Mails verschickt.

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

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