GlobalSign by GMO

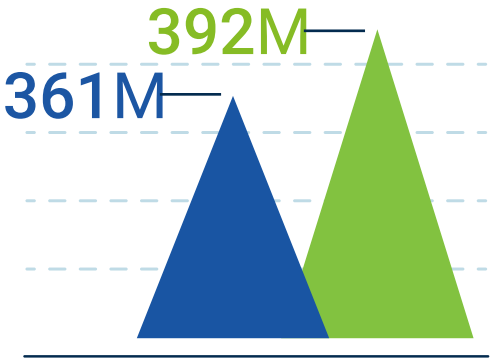
SICHERUNG DER KOMMUNIKATION

Von der Phishing-Abwehr bis zum automatisierten Schutz

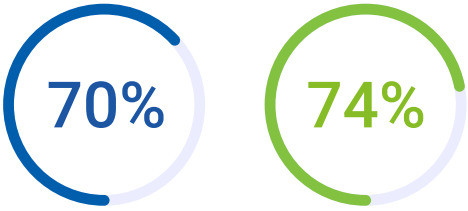
Inhalt

Einleitung

In der heutigen digitalen Landschaft ist E-Mail-Sicherheit extrem wichtig. Laut Statistica.com werden täglich weltweit etwa 361 Milliarden E-Mails verschickt und empfangen. Und diese Zahl wird bis 2026 voraussichtlich auf rund 392 Milliarden ansteigen. Da E-Mails in der geschäftlichen Kommunikation so extrem wichtig sind, stellen sie ein bevorzugtes Ziel für Cyberkriminelle dar. Im April 2024 berichtete gov.uk, dass 70% der mittelgroßen Unternehmen und 74% der großen Unternehmen in den letzten 12 Monaten einen Cybersicherheitsvorfall erlebt haben. Bei 84% dieser Vorfälle handelte es sich um Phishing-Angriffe. Dieses E-Book bietet einen Einblick in die sich stetig weiterentwickelnden Herausforderungen im Bereich der E-Mail-Sicherheit. Zudem zeigt es, wie Automatisierung die Schutzvorkehrungen verbessern kann, insbesondere in Anbetracht der alarmierenden Statistiken.



Täglich versendete E-Mails, deren Anzahl bis 2026 voraussichtlich weiter steigen wird.



Mittelständisches Unternehmen | Großes Unternehmen

erlebten in den letzten 12 Monaten eine Cybersicherheitsverletzung

Anhand eines näheren Blicks auf die Partnerschaft zwischen GlobalSign und NoSpamProxy erläutern wir, wie unsere kombinierten Lösungen einen robusten Verteidigungsrahmen gegen E-Mail-basierte Bedrohungen bieten. Digitale Zertifikate und Verschlüsselung gewährleisten die Authentizität, Integrität und Vertraulichkeit der E-Mail-Kommunikation und spielen daher bei dieser gemeinsamen Verteidigungsstrategie eine zentrale Rolle. Durch die Automatisierung werden die Sicherheitsmaßnahmen weiter gestärkt, da sie die Verwaltung digitaler Zertifikate vereinfacht. Weitere Elemente der Strategie sind die Implementierung von Sicherheitsprotokollen wie S/MIME und insgesamt die Verringerung des Risikos menschlicher Fehler. Dieses E-Book erläutert, wie die Automatisierung solche Prozesse rationalisiert und zu einer robusteren E-Mail-Abwehr beiträgt.

Digitale Zertifikate und Signaturen verstehen

Das Verständnis von digitalen Zertifikaten und Signaturen ist unverzichtbar, da sie die Grundlage für eine sichere E-Mail-Kommunikation in der immer stärker gefährdeten digitalen Landschaft bilden.

Digitale Zertifikate

Digitale Zertifikate sind elektronische Nachweise, die Identitäten verifizieren. Sie sind also unerlässlich, um Vertrauen in die digitale Kommunikation zu schaffen. Dieser Verifizierungsbedarf erstreckt sich allerdings auch auf KI-Anwendungen. Denn digitale Zertifikate bestätigen die Identität von vertrauenswürdigen Algorithmen und Nutzern und erhöhen dadurch die Integrität und Zuverlässigkeit automatisierter Entscheidungsprozesse.

- Definition und Zweck
  Mithilfe digitaler Zertifikate wird die Identität von Personen, Geräten oder Diensten verifiziert. Sie werden von Einrichtungen ausgestellt, die als Zertifizierungsstellen (CAs) bezeichnet werden.
- Public Key Infrastructure (PKI)
  PKI verwaltet digitale Schlüssel und Zertifikate, die das Rückgrat einer sicheren Kommunikation bilden. PKI erstellt, verteilt und verifiziert öffentliche und private Schlüssel und gewährleistet dadurch, dass die an der Kommunikation beteiligten Parteien authentisch und vertrauenswürdig sind.
- Arten von Zertifikaten
  Zu den verschiedenen Arten von Zertifikaten gehören Secure Sockets Layer (SSL) und Transport Layer Security (TLS) zur Sicherung von Websites, Client-Zertifikate zur Authentifizierung von Benutzern sowie Code Signing-Zertifikate zur Sicherung von Software/Anwendungen.

Digitale Zertifikate und Signaturen verstehen

Zertifizierungsstellen (CAs), wie zum Beispiel GlobalSign, sind vertrauenswürdige Einrichtungen, die solche Zertifikate ausstellen. Sie spielen eine entscheidende Rolle im Lebenszyklus der Zertifikate, da sie Lösungen für eine effektive Zertifikatsverwaltung bieten und sicherstellen, dass die von ihnen zertifizierten Unternehmen legitim sind.

Digitale Zertifikate sind also eine Schlüsselkomponente für die digitale Sicherheit. Deshalb ist es für Unternehmen entscheidend, sie angemessen zu verwalten. Diese Verwaltung umfasst das Ausstellen, Erneuern und Widerrufen von Zertifikaten. Als primärer Schutz vor alten und neuen Bedrohungen, einschließlich derer, die KI nutzen, ist ein effizientes Lebenszyklusmanagement von Zertifikaten zur Aufrechterhaltung einer sicheren Kommunikation unerlässlich.

Digitale Signaturen

Eine digitale Signatur ist eine elektronische Signatur, die unterstützt wird durch ein digitales Zertifikat, das für einen Identitätsnachweis sorgt. Auch wenn digitale Signaturen beim Signieren von Dokumenten weite Verbreitung finden, sind sie auch für die Sicherheit von E-Mails entscheidend, da sie deren Authentizität und Integrität gewährleisten. Wenn zur Verifizierung von Absendern Zertifikate genutzt werden, machen digitale Signaturen es für böswillige Akteure deutlich schwerer, echte Benutzer nachzuahmen oder E-Mail-Inhalte zu manipulieren. Unternehmen, die ihre Sicherheitsmaßnahmen verbessern wollen, sollten daher die Vorteile der Implementierung digitaler Signaturen kennen und verstehen.

Vorteile der Implementierung digitaler Signaturen:

Verbesserte Sicherheit

Digitale Signaturen überprüfen die Identität eines Absenders und stellen sicher, dass E-Mails während der Übertragung unverändert bleiben. Das hilft beim Schutz vor Manipulationen und gewährleistet die Integrität der Nachricht.

Erhöhtes Vertrauen

Sie bauen auch Vertrauen zwischen den kommunizierenden Parteien auf, da sie durch die Authentifizierung des Absenders das Risiko von Phishing-Angriffen oder anderen E-Mail-basierten Bedrohungen verringern.

Kosteneffizienz

Durch die Reduzierung des Risikos von Betrug und Datenschutzverstößen können digitale Signaturen auch die potenziellen Kosten senken, die sonst durch Sicherheitsvorfälle, Rechtsstreitigkeiten oder Compliance-Verstöße entstehen.

Bedrohungen für die E-Mail-Sicherheit

Um Ihre E-Mail-Kommunikation sichern zu können, müssen Sie zunächst die Arten von Bedrohungen kennen, denen Ihr Unternehmen ausgesetzt sein kann:

Die häufigsten Arten von E-Mail-Phishing-Angriffen:

- Email Bombing
  Posteingänge werden mit unzähligen E-Mails überschwemmt, die oft als Deckmantel für echte Angriffe dienen, zum Beispiel für nicht autorisierte Finanztransaktionen.
- Business Email Compromise (BEC)
  Hier werden Führungskräfte oder Finanzabteilungen ins Visier genommen, um an deren sensible Daten zu gelangen.
- Spear Phishing
  Die Angreifer geben sich als vertrauenswürdige Quellen aus und nutzen dies, um die Empfänger zur Weitergabe vertraulicher Daten zu überreden.
- Allgemeine Phishing-E-Mails
  Die Angreifer verleiten die Benutzer durch trügerische Mittel dazu, auf bösartige Links zu klicken oder schädliche Anhänge herunterzuladen.

Bedrohungen für die E-Mail-Sicherheit

KI und Cybersicherheit

Da Cyberbedrohungen immer komplexer werden, nimmt die Rolle der KI für die Cybersicherheit stark zu und bietet einerseits neue Verteidigungsmöglichkeiten und andererseits auch neue Risiken. In diesem Abschnitt erörtern wir die wichtigsten Begriffe und untersuchen, wie KI die Landschaft der E-Mail-Sicherheit verändert. Das Verständnis dieser Konzepte ist entscheidend, um sich wirksam vor neuen Bedrohungen schützen zu können.

Grundlegende Terminologie:

KI (Künstliche Intelligenz):

- Bezieht sich auf Computersysteme, die Aufgaben ausführen können, für die normalerweise menschliche Intelligenz erforderlich ist.
- Dazu gehören das Lernen aus Daten, logisches Denken, Problemlösung, Wahrnehmung sowie Sprachverständnis.
- Es werden Algorithmen und Daten genutzt, um Entscheidungen und Vorhersagen zu treffen.

Deep Fake:

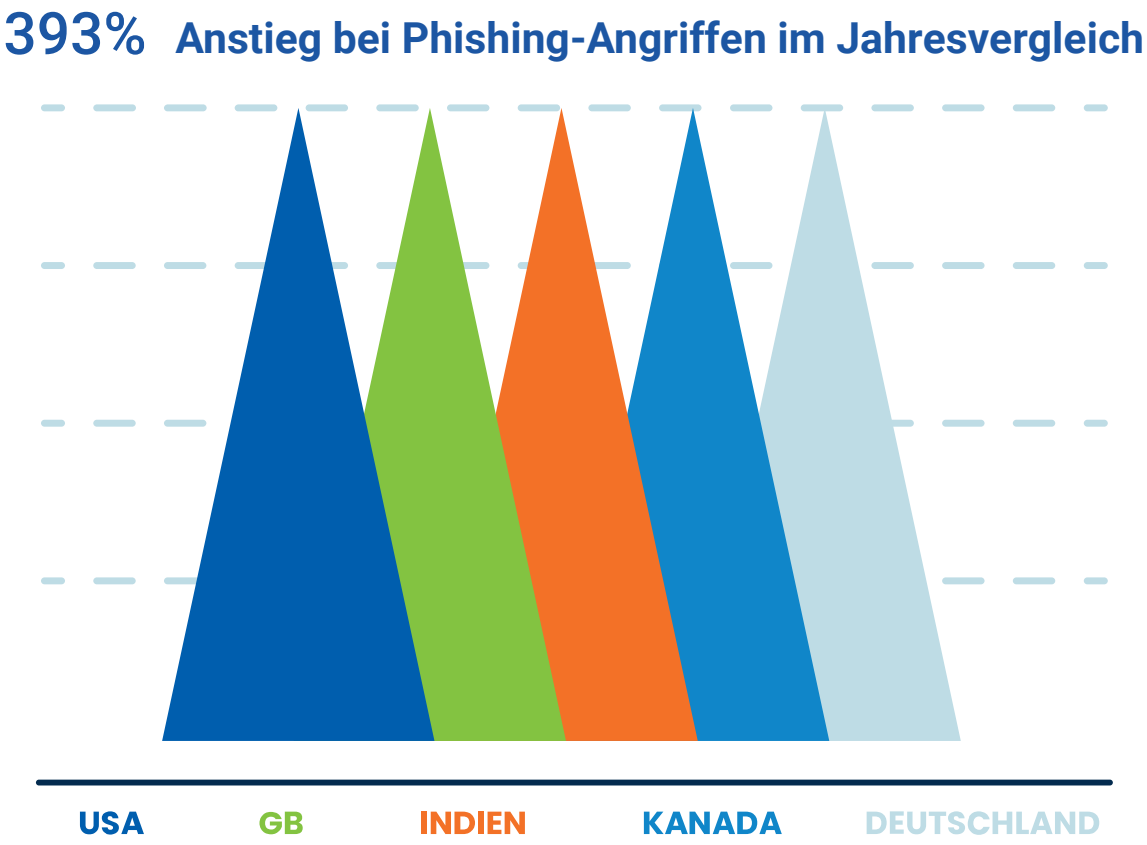
- Hier wird künstliche Intelligenz zur Erstellung oder Bearbeitung von Audio-, Video- oder Bildmaterial eingesetzt.
- Dadurch lassen sich sehr realistische gefälschte Inhalte erzeugen, die nur schwer von echten Medien zu unterscheiden sind.

GPT (Generative Pre-trained Transformer):

- Große Sprachmodelle, entwickelt von OpenAI.
- Mithilfe von Deep Learning werden auf der Grundlage von Eingaben menschenähnliche Texte generiert.
- Das Training erfolgt mit großen Datensätzen, damit zusammenhängende Texte verstanden und erzeugt werden können.

Bedrohungen für die E-Mail-Sicherheit

Aufgrund der zunehmenden Beliebtheit von künstlicher Intelligenz und Deep-Fake-Technologien werden Cyberangriffe immer raffinierter und dadurch schwieriger zu erkennen. Angreifer nutzen KI auch, um ihre Social-Engineering-Taktiken zu verbessern. Das hat zu einem signifikanten Anstieg von 60% bei KI-gesteuerten Phishing-Angriffen geführt, wie Zscaler Research zeigt. Die USA, Großbritannien, Indien, Kanada und Deutschland führten die Liste der Länder an, die Ziel von Phishing-Betrügereien waren. Besonders betroffen war der Finanz- und Versicherungssektor, in dem die Zahl der Angriffe im Vergleich zum Vorjahr um 393% anstieg.



KI verbessert zwar den Schutz, indem betrügerische E-Mails erkannt, Phishing-Versuche analysiert und die Erkennung von Bedrohungen verbessert wird, sie birgt jedoch auch neue Risiken. Angreifer nutzen KI, um ihre Angriffe zu automatisieren und zu optimieren. Sie erstellen mit ihr sehr überzeugende Phishing-E-Mails und manipulieren digitale Inhalte mit einem noch nie dagewesenen Realismus. Laut dem Bericht „IBM X-Force Threat Intelligence Index 2024“ wurden KI und GPT im Jahr 2023 in über 800.000 Beiträgen auf illegalen Märkten und in Dark-Web-Foren erwähnt. Das zeigt deutlich das wachsende Interesse der Cyberkriminellen an diesen Technologien. Anhand der zwei Gesichter der KI lässt sich der dringende Bedarf an robusten Cybersicherheitsmaßnahmen erkennen, die sich an neue Bedrohungen anpassen können. Ein wirksamer Ansatz zur Abschwächung dieser Risiken und damit zur Sicherung der E-Mail-Kommunikation ist die Implementierung von S/MIME (Secure/Multipurpose Internet Mail Extensions).

Einführung in S/MIME

Sicherung von E-Mails

S/MIME, kurz für Secure/Multipurpose Internet Mail Extensions, sind Erweiterungen, die für den Versand digital signierter und verschlüsselter Nachrichten entscheidend sind. Sie erhöhen die E-Mail-Sicherheit, indem sie die Authentizität, Integrität und Vertraulichkeit der E-Mail-Kommunikation gewährleisten.

- Digitale Signaturen
  S/MIME nutzt digitale Signaturen, um Absender zu verifizieren und sicherzustellen, dass Nachrichten nicht verändert wurden. So kann der Empfänger sicher sein, dass die E-Mail wirklich von dem angegebenen Absender stammt.

- Verschlüsselung
  Informationen werden in Code für öffentliche und private Schlüssel umgewandelt, um mit deren Hilfe unbefugten Zugriff zu verhindern. Das stellt sicher, dass nur die vorgesehenen Empfänger die Informationen lesen können. S/MIME verschlüsselt auch den E-Mail-Inhalt selbst und schützt ihn so vor unbefugtem Zugriff. Nur der vorgesehene Empfänger kann die E-Mails wieder entschlüsseln und lesen.the email.

Einführung in S/MIME fortgesetzt

Die Einrichtung von S/MIME umfasst mehrere Schritte:

Erstellung von Schlüsseln
Der erste Schritt ist hierbei die Erstellung eines Paares aus öffentlichem und privatem Schlüssel. Der öffentliche Schlüssel wird mit anderen geteilt, während der private Schlüssel sicher aufbewahrt wird

Anfordern eines digitalen Zertifikats
Ein öffentlich vertrauenswürdiges S/MIME-Zertifikat erhalten Sie von einer Zertifizierungsstelle (CA). Dieses Zertifikat verbindet den öffentlichen Schlüssel mit der Identität des Zertifikatsinhabers.

Konfigurieren von E-Mail-Clients
E-Mail-Clients müssen für die Verwendung von S/MIME konfiguriert werden. Dazu gehört in der Regel die Installation des S/MIME-Zertifikats und die Einrichtung des Clients, damit er das Zertifikat zum Signieren und Verschlüsseln von E-Mails einsetzen kann.

Vorteile der Implementierung von S/MIME:

Authentizität
Die Identität des Absenders wird überprüft und es wird sichergestellt, dass die E-Mail von einer legitimen Quelle stammt.

Vertraulichkeit
Sensible Informationen werden geschützt, da sie nur für den vorgesehenen Empfänger zugänglich sind.

Integrität
Es wird sichergestellt, dass der Inhalt der E-Mail während der Übertragung nicht verändert wurde.

Verwaltung
Die Sicherheits- und Verwaltungsprozesse werden optimiert, ohne dass umfangreiche Benutzerschulungen oder IT-Ressourcen erforderlich sind.

Sichere Kommunikation automatisieren

Dies ist der Schlüssel zur effizienten Verwaltung von Zertifikaten, insbesondere in großen Unternehmen. Der manuelle Aufwand wird reduziert, die Sicherheit verbessert sich und Vorschriften werden eingehalten. Im Zusammenhang mit sicheren E-Mails ist die Automatisierung bei der Implementierung von S/MIME-Zertifikaten unerlässlich. Durch die Automatisierung der Bereitstellung und Erneuerung von S/MIME-Zertifikaten können Unternehmen sicherstellen, dass ihre gesamte E-Mail-Kommunikation verschlüsselt und authentifiziert bleibt. Und das ohne das Risiko von abgelaufenen oder falsch konfigurierten Zertifikaten.Trotz der zunehmenden Bedeutung der Automatisierung halten sich einige Unternehmen aufgrund der damit verbundenen potenziellen Herausforderungen weiterhin zurück.

Herausforderungen bei der Automatisierung überwinden: Warum wir automatisierte Lösungen anbieten

Automatisierte Lösungen, die von vertrauenswürdigen Unternehmen wie GlobalSign und NoSpamProxy angeboten werden, sind darauf ausgelegt, potenzielle Herausforderungen in Chancen zu verwandeln.

Bedenken bezüglich der Verwaltung

Herausforderung: Häufige Aktualisierungen von Stammzertifikaten können lästig sein.

Lösung: Mit unseren automatisierten Workflows lassen sich Aktualisierungen mühelos verwalten. Dadurch verringert sich der Verwaltungsaufwand und es werden rechtzeitige Aktualisierungen sichergestellt.

Kosten und Gemeinkosten

Herausforderung: Automatisierung kann kostspielig sein, insbesondere für kleinere Unternehmen.

Lösung: Unsere Lösungen senken die Betriebskosten, indem sie den manuellen Aufwand minimieren und die Automatisierung für Unternehmen jeder Größe erschwinglich und effizient machen.

Technische Beschränkungen und Kompatibilitätsprobleme

Herausforderung: Technische Beschränkungen und Kompatibilitätsprobleme können entmutigend wirken.

Lösung: Die Automatisierung verbessert die Systemintegration, strafft die Prozesse und verringert technische Barrieren, um reibungslose Kompatibilität zu gewährleisten.

Fehlende Kenntnisse

Herausforderung: Die Umsetzung der Automatisierung kann ohne das richtige Fachwissen sehr komplex sein.

Lösung: Wir bieten die Unterstützung und das Wissen von Experten und automatisieren Prozesse. Dadurch können Unternehmen automatisierte Systeme nahtlos implementieren und pflegen, ohne dass sie zusätzliche Ressourcen benötigen

Sicherheitsbedenken

Herausforderung: Bei automatisierten Systemen kann die Gewährleistung von Governance und Kontrolle eine Herausforderung sein.

Lösung: Unsere automatisierten Systeme erhöhen die Sicherheit, indem sie menschliche Fehler minimieren und robuste Überwachungs- und Alarmierungsmechanismen bereitstellen, die ein ordnungsgemäßes Zertifikatsmanagement gewährleisten.

Sichere Kommunikation automatisieren

Vorteile von automatisierten Lösungen:

Darüber hinaus können Unternehmen durch den Einsatz automatisierter Zertifizierungsabläufe weitere Vorteile haben:

Erhöhte Effizienz

Durch die Reduzierung des manuellen Aufwands ermöglichen automatisierte Systeme schnellere und genauere Prozesse für die Bereitstellung, Erneuerung und den Widerruf von Zertifikaten. Diese Effizienz führt zu einer erheblichen Zeitersparnis und mehr betrieblicher Agilität.

Verbesserte Sicherheit

Automatisierte Systeme minimieren das mit der Zertifikatsverwaltung verbundene Risiko menschlicher Fehler. Sie gewährleisten die rechtzeitige Ausstellung, Erneuerung und den Widerruf der Zertifikate. Unterstützt werden sie durch robuste Überwachungs- und Alarmierungsmechanismen, die Schwachstellen proaktiv aufdecken und entschärfen.

Skalierbarkeit und Konsistenz

Unternehmen können mit automatisierten Lösungen mühelos umfangreiche PKI-Implementierungen verwalten. Das gewährleistet die Konsistenz der Zertifikatskonfigurationen und beseitigt Unstimmigkeiten, die sonst die Sicherheit beeinträchtigen könnten.

Einhaltung gesetzlicher Vorschriften

Automatisierte Systeme rationalisieren die Einhaltung von Branchenvorschriften und -standards. Sie erleichtern die konsequente Überwachung, Prüfung und Verwaltung von Zertifikaten und verringern damit die Wahrscheinlichkeit von Strafen bei Nichteinhaltung.

Wie GlobalSign und NoSpamProxy helfen können

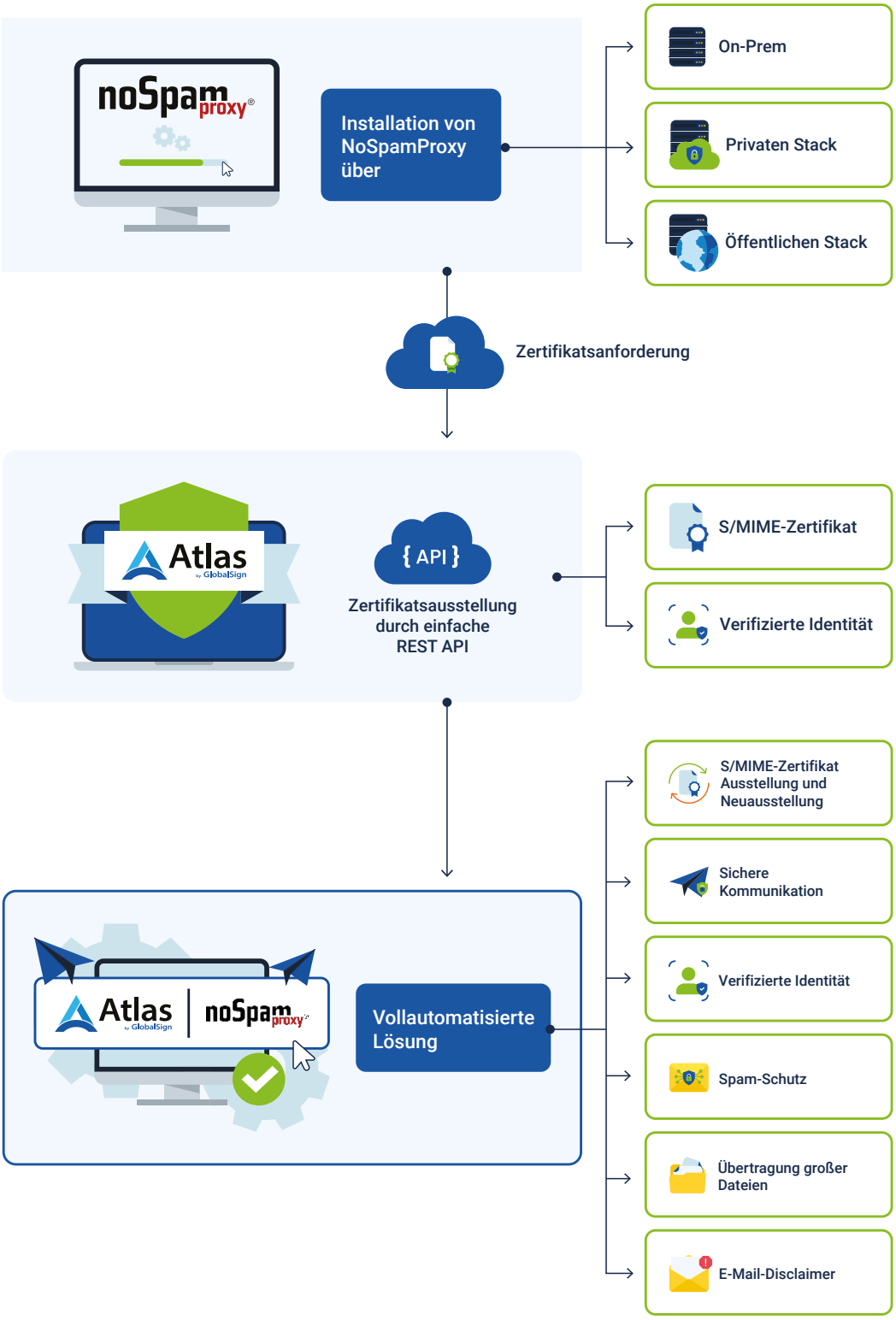
Für Unternehmen kann es schwierig sein, den Überblick über die sich ständig ändernden Gültigkeitszeiträume und die Lebenszyklen von Zertifikaten zu behalten. Diese Aufgaben sind sowohl zeitaufwändig als auch kostspielig. Durch die Partnerschaft mit GlobalSign und NoSpamProxy können Unternehmen eine sichere, automatisierte und skalierbare E-Mail-Sicherheitslösung implementieren, die ihre Kommunikation vor Cyberbedrohungen schützt und gleichzeitig Zeit und Ressourcen spart.

GlobalSign und NoSpamProxy bieten umfassende und nahtlos integrierbare Lösungen, die E-Mail-Sicherheit vom Sender bis zum Empfänger bieten. Unser kombinierter Ansatz gewährleistet zuverlässigen Schutz vor Phishing, Spam und anderen E-Mail-basierten Bedrohungen. Gleichzeitig automatisiert er die Zertifikatsverwaltung, um Effizienz und die Einhaltung von Vorschriften zu verbessern. Darüber hinaus bietet unsere jahrzehntelange Partnerschaft eine zusätzliche Ebene des Vertrauens und der Stabilität.

- NoSpamProxy
  Spezialisiert auf E-Mail-Sicherheit und mit einem umfassenden Schutz vor Spam, Phishing und anderen E-Mail-Bedrohungen. Durch fortschrittliche Algorithmen und maschinelles Lernen stellt NoSpamProxy sicher, dass nur legitime E-Mails Ihren Posteingang erreichen. Dadurch lässt sich das Risiko von Cyberangriffen, die von der E-Mail-Kommunikation ausgehen, erheblich reduzieren.

- GlobalSign
  Als führender Anbieter von digitalen Zertifikaten und Identitätsdiensten bieten wir Lösungen, die durch Verschlüsselung und digitale Signaturen eine sichere E-Mail-Kommunikation ermöglichen. Dadurch bleibt die Integrität und Vertraulichkeit Ihrer Nachrichten gewahrt und sensible Informationen werden vor unbefugtem Zugriff geschützt.

Integration der kombinierten Lösung von NoSpamProxy und GlobalSign



Bewährte Praktiken zur Sicherung der Kommunikation

Für weitere Verbesserungen der Kommunikationssicherheit in Ihrem Unternehmen sollten Sie folgende bewährte Verfahren berücksichtigen:

- Schulen Sie Ihre Mitarbeiter
  Führen Sie regelmäßige Schulungen über die Bedeutung sicherer Kommunikationspraktiken, das Erkennen von Phishing-Versuchen und den verantwortungsvollen Umgang mit sensiblen Informationen durch.
- Erneuern Sie Zertifikate regelmäßig
  Sorgen Sie dafür, dass Zertifikate, beispielsweise S/MIME-Zertifikate, regelmäßig erneuert werden, um ihre Gültigkeit zu behalten und die Kommunikation effizient sichern können.
- Aktualisieren Sie Software und Tools
  Führen Sie zum Schutz vor Sicherheitslücken regelmäßige Aktualisierungen von Software und Tools durch.
- Implementieren Sie Verschlüsselung
  Verwenden Sie für die gesamte sensible Kommunikationen eine Verschlüsselung, um Daten während der Übertragung zu schützen, unbefugten Zugriff zu verhindern und die Vertraulichkeit zu wahren.
- Automatisieren Sie Überwachungs- und Alarmierungssysteme
  Führen Sie automatisierte Systeme ein, um Kommunikationskanäle kontinuierlich zu überwachen. Solche Systeme können potenzielle Schwachstellen, unbefugte Zugriffsversuche oder Anomalien in Echtzeit erkennen. Automatische Warnmeldungen gewährleisten außerdem eine schnelle Reaktion und die Einhaltung der Sicherheitsrichtlinien.

Mithilfe solcher bewährten Verfahren kann Ihr Unternehmen seinen Schutz vor Cyberbedrohungen erheblich verbessern und die sichere Übertragung sensibler Daten gewährleisten.

Fazit

Zusammenfassend lässt sich sagen, dass die Bedeutung einer sicheren Kommunikation angesichts der fortschreitenden Entwicklung der digitalen Landschaft, die durch maschinelles Lernen noch verstärkt wird, keinesfalls unterschätzt werden darf. Die verschiedenen Arten und die Häufigkeit von Phishing-Angriffen zeigen, wie wichtig robuste Abwehrmechanismen sind. Durch ein grundlegendes Verständnis der bewährten Verfahren, die Implementierung von S/MIME-Zertifikaten und eine hochgradige Automatisierung lassen sich diese Probleme lösen und die Authentizität, Integrität und Vertraulichkeit der E-Mail-Kommunikation gewährleisten.

Ergreifen Sie am besten noch heute proaktive Maßnahmen, um die Kommunikation Ihres Unternehmens vor Cyberbedrohungen zu schützen. Durch die Zusammenarbeit mit GlobalSign und NoSpamProxy können Sie automatisierte Lösungen für mehr E-Mail-Sicherheit einsetzen, die Ihr Unternehmen schützen, die betriebliche Effizienz verbessern und die Einhaltung gesetzlicher Vorschriften gewährleisten.

Setzen Sie sich noch heute mit uns in Verbindung, um über Ihre E-Mail-Sicherheitsbedürfnisse zu sprechen – besuchen Sie www.globalsign.com/de-de/lp/nospamproxy

Über GMO GlobalSign

Als eine der weltweit etabliertesten Zertifizierungsstellen ist GlobalSign der führende Anbieter von vertrauenswürdigen Identitäts- und Sicherheitslösungen. Das Unternehmen ermöglicht es Organisationen, großen Unternehmen, Cloud-Dienstleistern und IoT-Innovatoren weltweit, sichere Online-Kommunikation durchzuführen, Millionen von verifizierten digitalen Identitäten zu verwalten und Authentifizierung sowie Verschlüsselung zu automatisieren. Die hochskalierbaren PKI- und Identitätslösungen unterstützen die Milliarden von Diensten, Geräten, Personen und Dingen, die das IoT ausmachen. GMO GlobalSign ist eine Tochtergesellschaft der in Japan ansässigen GMO Cloud KK und der GMO Internet Group und verfügt über Büros in Amerika, Europa und Asien. Weitere Informationen finden Sie unter https://www.globalsign.com.