FORTRA

LEITFADEN *(Cybersicherheit)*

Leitfaden Zur Verschlüsselung Und Zum Sicheren Datentransfer

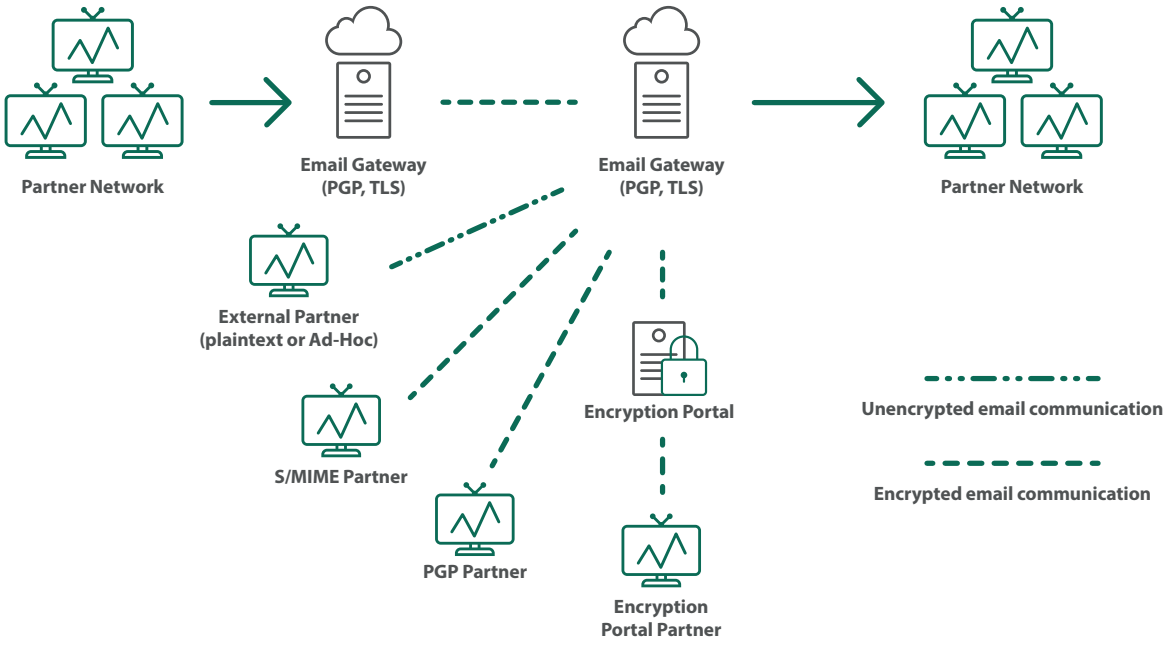
Einleitung

E-Mail-Verschlüsselung ist der Prozess, bei dem der Inhalt von E-Mail-Nachrichten verschlüsselt oder unkenntlich gemacht wird. So ist gewährleistet, dass sensible Informationen ausschließlich vom beabsichtigten Empfänger gelesen werden können.

Während es seit Jahren üblich ist, eingehende E-Mails auf Viren und Spam zu überprüfen, beschäftigen sich viele Firmen erst jetzt mit dem Schutz von ausgehenden E-Mails. Dafür gibt es zwei Gründe. 1. Das mangelnde Verständnis der Vorteile und Unterschiede zwischen den vielzähligen Optionen. 2. Kosten und Nutzerfreundlichkeit der Lösungen. In der Vergangenheit waren sowohl Verschlüsselungs- als auch DLP-Lösungen bekanntermaßen schwierig zu konfigurieren und warten, weshalb sie nur für große Unternehmen mit dem nötigen IT-Fachwissen in Frage kamen.

Die heutigen Lösungen zur Erhöhung des E-Mail-Schutzes werden zwar immer intelligenter, wirken jedoch weniger komplex und sind kostengünstiger zu warten, siehe Abbildung 1. Je nach Situation ist sind unterschiedliche Lösungen erforderlich, und zutreffendste Lösung kann von Fall zu Fall unterschiedlich sein. Daher muss diese automatisch erfolgen – anhand des Empfängers und der übertragenen Informationen.

Abbildung 1: Sichere E-Mail-Optionen



Verschlüsselung

Mit Hilfe der Verschlüsselung wird sichergestellt, dass der Inhalt einer E-Mail nicht abgefangen und gelesen werden kann, insbesondere wenn die E-Mail an einen Empfänger außerhalb des Unternehmens geschickt wird. Der ideale Ort für die Verschlüsselung ist daher der Punkt, an dem die E-Mail in das Unternehmen eindringt oder dieses verlässt. Mit modernen E-Mail-Gateways, die vor eingehenden Bedrohungen schützen, lassen sich auch ausgehende E-Mails automatisch verschlüsseln. Es gibt verschiedene Verschlüsselungsoptionen (siehe Tabelle 1). Nachfolgend werden die einzelnen Verschlüsselungstypen genauer erläutert.

Datenverlust kann verheerende Auswirkungen für den Ruf des Unternehmens haben, doch jetzt gibt es auch noch ein Gebot für eingehende Informationen. Der Erhalt unerwünschter Daten kann nämlich genau so viele Probleme bereiten, wie Daten, die das Unternehmen verlassen. In diesem Zusammenhang sind einige Szenarien zu berücksichtigen.

Transport Layer Security (TLS)

Für die Verschlüsselung von Mitteilungen zwischen einem Benutzer und anderen Unternehmen reicht TLS völlig aus. TLS-Verbindungen können „opportunistisch“ vorgehen und sicherstellen, dass verschlüsselte Nachrichten, die in diesem Modus verschickt werden, automatisch eine TLS-Verbindung wählen. Alternativ können Verbindungen zwischen Unternehmen vorgegeben werden und eine vordefinierte Verschlüsselungsstärke haben, um sicherzustellen, dass Nachrichten nur dann verschickt werden, wenn während des Handshakes ein angemessenes Sicherheitsniveau erreicht ist.

	Verschlüs-selung von Standort zu Standort	Verschlüsselung zwischen Standort und Empfänger	Verschlüsselung von Desktop zu Desktop	Standardbasiert	Verschlüs-selungsstärke	Austausch von Schlüssel oder Kennwort	Transparenz hinsichtlich der Empfänger
TLS	Ja	Nein	Nein	Ja	Mittel	Nein	Ja
S/MIME, PGP	Ja	Ja	Ja	Ja	Hoch	Ja	Standort zu Standort: Ja – Verschlüsselung zum Empfänger erfordert evtl. einen Schlüssel oder ein Plugin auf dem Client
Kennwort (Windows)	Nein	Ja	Nein	Ja	Mittel	Ja	Ja
Kennwort (AES)	Nein	Ja	Nein	Ja	Hoch	Ja	Erfordert ein AES256-kompatibles ZIP-Paket
Portal	Nein	Ja	Nein	Ja	Hoch	Nein	Erfordert möglicherweise ein Plugin zum Abrufen von Nachrichten

Nachrichtenverschlüsselung (S/MIME, PGP und kennwortgeschützte ZIP-Dateien)

Gute Verschlüsselungslösungen unterstützen internationale Standards für die Mitteilungsformate OpenPGP und S/MIME. Dies ermöglicht den Nachrichtenaustausch zwischen Empfängern, die gängige E-Mail-Clients wie Outlook, Outlook Express und Notes verwenden.

Intelligente E-Mail-Gateways können S/MIME und OpenPGP auch dazu nutzen, richtlinienbasierte sichere Verbindungen zwischen zwei Gateways oder zwischen einem Gateway und einem Empfänger herzustellen. Bei der integrierten Verschlüsselung kann der E-Mail-Gateway Mitteilungen entschlüsseln und anschließend weitere Tools wie Spamschutz, Virenschutz oder Inhaltsfilter-Engines nutzen, um sicherzustellen, dass die Nachrichten voll und ganz der E-Mail-Richtlinie des Unternehmens entsprechen.

Ad-hoc-Verschlüsselung

Bei Empfängern, die weder PGP noch S/MIME verwenden, können E-Mail-Gateways der neuen Generation trotzdem Nachrichten in einem sicheren Format verschicken, und zwar in Form von kennwortgeschützten ZIP-Archiven. Man spricht hierbei auch von Ad-hoc-Verschlüsselung. Selbst hier können Sie wählen, ob Windows-kompatible oder AES-verschlüsselte ZIP-Formate verwendet werden sollen.

Windows-kompatible ZIP-Formate lassen sich ohne zusätzliche Software öffnen. Unternehmen, die stärkere Verschlüsselungsalgorithmen wie AES256 erfordern, verlangen jedoch, dass der Empfänger einen der zahlreichen ZIP-Clients hat, mit dem dieses Format verarbeitet werden kann.

Dies lässt sich auch durch geschützte PDF-Dateien erreichen, mit denen sensible Nachrichten oder Anhänge verschickt werden. Dieses Format ist beliebt, wenn es um die sichere Übermittlung von Abrechnungen und Dokumenten geht.

Kennwörter, die während der Ad-hoc-Verschlüsselung erstellt werden, lassen sich dynamisch erzeugen, und zwar entweder für einzelne Benutzer oder für die jeweilige Mitteilung. In vielen Fällen ist es dann am Absender, dem Empfänger das Kennwort mitzuteilen. Manche Systeme erstellen allerdings auch automatische E-Mails, die verzögert an den Empfänger verschickt werden.

Verschlüsselung Über Webportale

Oft bestimmt auch das technische Wissen des Empfängers, welche Verschlüsselungsmethode verwendet werden muss. Portalbasierte Verschlüsselung ist eine einfache Methode, die kein spezielles Wissen erfordert. Verschlüsselte E-Mail-Nachrichten werden über ein Verschlüsselungsportal verschickt und können dann jeder Art von Gerät in einem Browser geöffnet werden, auf PCs und Telefonen bis hin zu Tablets. Bei dieser Methode wird der Empfänger per E-Mail informiert, wenn beim Portal eine verschlüsselte Nachricht für ihn eingegangen ist.

Data Loss Prevention (DLP)

Bei bestimmten Informationen reicht jedoch auch E-Mail-Verschlüsselung nicht aus. Solche Informationen müssen stets im Unternehmen bleiben. Hier sind Data Loss Prevention (DLP)-Technologien nötig, die darauf achten, ob beschränkte Informationen einen Austrittspunkt durchlaufen, und diese dann blockieren. Mit einer DLP-Lösung kann der Inhalt von E-Mails und Anhängen untersucht und auf bestimmte Informationen überprüft werden. Enthält die E-Mail den gesuchten Inhalt, kommt die entsprechende Maßnahme zum Einsatz.

Hier ein einfaches Beispiel: Eine Richtlinie verhindert, dass E-Mails mit vulgären Inhalten das Unternehmen verlassen, während andere, komplexere Richtlinien auf Kreditkarten- oder Bankdaten achten und verhindern, dass diese aus dem Unternehmen fließen. Wie bereits bei den Lösungen zur E-Mail-Verschlüsselung ist der einfachste Ort für den Einsatz von DLP der Austrittspunkt am E-Mail-Gateway. Weil die Lösung nicht auf den einzelnen Computern, sondern am Gateway ausgeführt wird, sind alle mit dem Firmennetzwerk verbundenen Geräte geschützt.

Webbasierte E-Mails

Wenn es um Informationssicherheit geht, müssen jetzt oft nicht nur über das Firmennetzwerk verschickte, sondern auch webbasierte E-Mails berücksichtigt werden. Viele Unternehmen verlangen mittlerweile, dass für geschäftliche E-Mails stets und ausschließlich die berufliche E-Mail-Adresse verwendet wird. Das hat zur Folge, dass Mitarbeiter für soziale und persönliche Zwecke häufig eine private E-Mail-Adresse unterhalten. Die steigende Zahl persönlicher E-Mails beschert den Unternehmen jedoch auch ein erhöhtes Informationsrisiko, da sich Mitarbeiter kritische Informationen oft an ihre private E-Mail-Adresse schicken (meist, um zu Hause weiter an dem Dokument zu arbeiten). Im Hinblick auf den Schutz von Firmendaten muss dieser Kommunikationskanal unbedingt bedacht werden.

Eine Gateway-Lösung, die den gesamten webbasierten Datenverkehr (sowie herkömmliche Firmen-E-Mails) abfängt, bietet eine hervorragende Methode, um sicherzustellen, dass betriebliche Informationen im Unternehmen bleiben. Dieselben DLP-Richtlinien, die für Firmen-E-Mails gelten, können auch für webbasierte E-Mails (und für andere webbasierte Aktivitäten wie soziale Netzwerke) genutzt werden. Sind einheitliche Richtlinien zur Informationssicherheit sowie entsprechende Technologien für deren Durchsetzung vorhanden, fällt es der IT-Abteilung bzw. dem CIO oder CISO (die letztendlich für Unternehmensdaten verantwortlich sind) leichter, allgemeine Richtlinien zu erstellen und Verstöße aufzurufen.

Geschützter Dateitransfer

Bei sehr großen Dateien (normalerweise über 1 GB) bietet E-Mail keine Option für die effektive Übertragung Während Datengrößen für Unternehmen früher überwiegend unbedenklich waren, können Videos und Rich Media heutzutage Problem darstellen. Für den Versand großer Dateien gibt es diverse Mechanismen, am gängigsten ist jedoch FTP (File Transfer Protocol), weil es besonders benutzerfreundlich ist. Bei FTP wird die Datei von der Quelle ans Ziel übermittelt, allerdings ohne Sicherheitsüberprüfung. Während per E-Mail verschickte Informationen bei eingehenden Nachrichten auf Viren und sonstige Malware überprüft und bei ausgehenden Nachrichten durch Datenschutzrichtlinien verwaltet werden können, ist dies bei herkömmlichem FTP nicht der Fall. Hier kommen sichere Datei-Gateways ins Spiel, die einen geschützten Dateitransfer ermöglichen. Einfach gesagt werden Richtlinien und Technologien zum Schutz von E-Mails dadurch auch für Dateiübertragungsmechanismen wie FTP übernommen. Die Verarbeitung kann dann komplett transparent erfolgen. Sie wird durch den Datei-Gateway automatisiert, ohne dass der Benutzer merkt, dass der überprüft wird.

Im Verteidigungssektor, wo Informationen von Netzwerken mit bestimmter Sicherheitsstufe in Netzwerke mit anderer Sicherheitsstufe übertragen werden müssen, werden sichere

Datei-Gateways schon seit Jahren eingesetzt. Mittlerweile halten sie jedoch auch zunehmend Einzug in den kommerziellen Sektor, wo sie die sichere Übertragung von Dateien zwischen Partnern ermöglichen, sowie in Unternehmen, in denen Daten intern getrennt werden müssen. So lässt sich garantieren, dass nur Informationen, die der Richtlinie entsprechen, an andere Parteien im Unternehmen weitergegeben werden können. Guaranteeing that only information which complies with policy is shared with other parts of the organization.

Zusammenfassung

E-Mails sind weiterhin ein wichtiges Werkzeug für Unternehmen aller Größen. Fast alles geistige Eigentum sowie vertrauliche Informationen von Unternehmen werden per E-Mail verschickt. Das wachsende Bedürfnis für Zusammenarbeit, neue Gesetze und Cyberangriffe auf betriebliche Informationen bedeuten, dass Unternehmen ihre Richtlinien zum Schutz von E-Mails erneut prüfen müssen, um kritische Informationen zu schützen. Aufgrund der zunehmenden Bedeutung von Information Governance, Kenntnissen über und den Schutz von Informationen – besonders deren Fluss in das Unternehmen und aus diesem heraus, beginnen selbst kleinste Unternehmen, sich mit neuen Technologien zum Schutz ihrer E-Mails zu befassen.

Früher waren spezielle Kenntnisse erforderlich, um Technologien zum Schutz von E-Mails einzusetzen, doch heute können selbst kleinste Unternehmen ihre E-Mails im Handumdrehen verschlüsseln und DLP-Richtlinien einführen, ohne ihre Verwaltungskosten in die Höhe zu treiben. Dieselben Sicherheitsrichtlinien, die für betriebliche E-Mails gelten, können mit Hilfe kombinierter Web- und E-Mail-Gateways auch auf webbasierte E-Mails angewendet werden. Dadurch haben Unternehmen die nötige Gewissheit, dass ihre Informationen geschützt sind, egal, über welchen Kommunikationskanal sie fließen.

Darüber hinaus bedeutet das Aufkommen webbasierter Kollaborationstools und extrem großer Dateien, dass sich Unternehmen mit Technologien zur sicheren Dateiübertragung befassen müssen, um dieselben Richtlinien, die für E-Mails gelten, auch auf Dateien anzuwenden, die mit anderen Unternehmen oder auch nur zwischen verschiedenen Abteilungen ausgetauscht werden.

FORTRA

Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.