Cryptshare®
Making e-mail better

Our thanks to
Microsoft suse vmware IBM

Was wir an E-Mail lieben und hassen

- E-Mail-Verschlüsselung
- Anhänge jeder Größe
- IT-Compliance

Cryptshare®
Making e-mail better

Die Verschlüsselung von E-Mails sollte für alle CISOs im Jahr 2017 ganz oben auf der Liste für Budgetanforderungen stehen. Was lieben und hassen wir eigentlich an E-Mails und welche alten Systeme können wir loswerden?

Es gibt zahlreiche gute Gründe die dafürsprechen, dass uns E-Mail noch viele Jahre begleiten wird. Also sollten wir alles daransetzen, das Beste aus dieser Technik herauszuholen. In diesem Beitrag werden wir die häufigsten Bedrohungen für die E-Mail-Kommunikation identifizieren. Wir klären, warum uns diese heute mehr beschäftigen als noch vor einigen Jahren. Außerdem gehen wir auf einige einfache technische Maßnahmen ein, um Risiken zu minimieren und werden einige Begriffe der Verschlüsselungssprache entzaubern. Ferner werden wir Systeme ausfindig machen, die ausrangiert werden können. Zum Schluss schauen wir uns einige ganz konkrete Vorteile an: finanzielle Einsparungen und Risikominimierung. Sie werden uns zu einer ausgewogenen und rationalen Investitionsentscheidung bringen und unser Herz für E-Mail wieder höherschlagen lassen.

Managementübersicht

Früher haben wir E-Mail geliebt. Seit E-Mail als Kommunikationsmedium verfügbar ist, steigt ihr Einsatz immer mehr, der Gebrauch ist keinesfalls rückläufig und im Geschäftsleben ist E-Mail sowieso die erste Wahl, wenn wir intern oder extern kommunizieren. Was lieben wir also an E-Mail? Zunächst ist sie ein universeller Standard, jeder private oder geschäftliche Nutzer eines Computers oder Smartphones hat E-Mail und kann mit jedem anderen E-Mail-Nutzer kommunizieren, unabhängig welches Endgerät oder E-Mail-Programm er verwendet. Sie ist ein allseits akzeptierter Standard, eine universelle Sprache. Das ist sehr viel wert und deshalb liebenswert.

Aber es ist unmöglich (geworden), die Zeitung aufzuschlagen oder Radio zu hören, ohne über eine Geschichte zu stolpern in der es um Datenschutzverletzungen, Datenverlust oder Datenmissbrauch geht und bei der nicht E-Mail im Zentrum der Geschichte steht. Wird nur öfters darüber berichtet oder gibt es wirklich neue Bedrohungen? Wie beeinflussen diese Ihr Geschäft? Sind Ihre Systeme, einschließlich E-Mail, stark genug oder ist es möglich, dass Sie bereits kompromittiert wurden und nur noch nichts mitbekommen haben? Sind einige Ihrer Abwehrsysteme veraltet? Müssen sie ersetzt oder aktualisiert werden?

Cryptshare®
Making e-mail better

Neue Bedrohungen entstehen jeden Tag und jede neue Welle ist von größerer Raffinesse und Komplexität. Es ist nicht mehr zeitgemäß zu glauben, dass Ihre E-Mails nicht gescannt und auf Geheimnisse hin untersucht werden, besonders wenn sie den geschützten Bereich Ihres eigenen Unternehmensnetzwerks verlassen. Sie haben sicher bereits viel in den Datenschutz in Ihrem Unternehmen investiert, doch die Menschen mit denen Sie tagtäglich kommunizieren, haben nichts von diesen Investitionen: Kunden, Lieferanten und Geschäftspartner. Es ist an der Zeit zu handeln!

Externe Einflüsse erhöhen den Druck für mehr Sicherheit

Ein neues Datenschutzgesetz nimmt das Risiko stärker ins Blickfeld. Jeden Tag werden Ihnen sensible Informationen aller Art anvertraut: Informationen, die Ihr eigenes Unternehmen oder die ihrer Kunden und Lieferanten betreffen, personenbezogene Daten, Finanzdaten, vertrauliche Pläne u.v.m. Letztendlich verlässt sich jeder einzelne mit dem Sie kommunizieren darauf, dass diese Informationen geheim bleiben oder zumindest vertraulich behandelt werden. Natürlich sind die Anforderungen an die Datensicherheit je nach Branche unterschiedlich.

Einige Branchen, wie bspw. das Gesundheitswesen, Verwaltungen, Versicherungen, Banken und Betreiber kritischer Infrastrukturen stehen sogar unter strenger Beobachtung von Regulierungsbehörden. Wir müssen uns der traurigen Realität stellen und uns bewusstmachen, dass es leider Menschen gibt, die ein starkes Interesse am Diebstahl Ihrer Daten haben, aus rein finanziellen Gründen oder um Ihre Geschäftsabläufe zu stören. Es gibt zahlreiche Gründe, gezielt Daten abzugreifen und das geschieht auch zunehmend - E-Mail ist dabei ein bevorzugtes Angriffsziel.

Traditionelle E-Mail-Verschlüsselungsmethoden sind nicht mehr sinnvoll

Sie und Ihre Kommunikationspartner sind von öffentlichen Netzwerken, v.a. dem Internet abhängig. Und obwohl es effektive und etablierte Verschlüsselungsmethoden gibt, die für E-Mail verwendet werden können, erfüllen sie drei grundlegenden Anforderungen nicht. Erstens, die Lösungen setzen eine meist komplexere Beschaffung und Einrichtung von öffentlichen und privaten Schlüsseln voraus und können nicht ad-hoc zwischen zwei Kommunikationsteilnehmern eingesetzt werden, die vorher nicht die erforderliche Einrichtungsprozedur durchlaufen haben. Zweitens, die Anwendung ist für Unternehmen und ihre Kunden sehr umständlich. Drittens, sie sind in Anschaffung und Betriebsführung teuer.

Die Sprache der Verschlüsselung ist oft unklar. Ist asymmetrische Verschlüsselung von Haus aus besser als symmetrische? Sind längere Schlüssel automatisch besser? Funktioniert Public-Key-Infrastruktur noch? (PKI bezeichnet in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.) Dieses Whitepaper erklärt Fachausdrücke in einfachen Worten und entzaubert so die Sprache der Verschlüsselung, um Licht ins Dunkel zu bringen und Ihnen wichtige Entscheidungen, die Sie jetzt treffen müssen, zu erleichtern.

Cryptshare®
Making e-mail better

Holen Sie mehr raus und sparen Sie Geld

Es gibt preiswerte Lösungen, mit denen Sie einige veraltete Produkte wie FTP- und SFTP-Server, PGP- oder PKI-Verschlüsselungswerkzeuge und das ein oder andere Schatten IT-Werkzeug Ihrer Mitarbeiter loswerden können. Innehalten und Nichtstun ist keine Option für die Wahrung der Datensicherheit. Selbst wenn Sie bereits massiv in den Schutz Ihrer Daten investiert haben, gibt es noch viel zu tun, um ständig neu aufkommenden Bedrohungen, die sich immer weiter ausbreiten, zu trotzen.

Wir sind der Meinung, dass die effektivste Lösung, Ihre Daten zu schützen, sobald sie Ihre Verteidigungslinie, also Ihr eigenes Netzwerk, verlassen haben, so aussehen sollte: einfach bedienbar, ad-hoc einsetzbar, direkt integrierbar in die Anwendungen, mit denen Sie bereits heute arbeiten und vollständig nachvollziehbar. Zudem sollte sie erschwinglich sein und im Idealfall einige alte Systeme ersetzen.

Wir sollten der E-Mail wieder positiv entgegentreten, denn die guten Eigenschaften überwiegen. Wenn wir ihre Unzulänglichkeiten beseitigen, kann E-Mail auch für zukünftige Business-Anforderungen das ideale Kommunikationsmedium bleiben.

Schadsoftware verändert sich schnell und macht es uns immer schwieriger, Bedrohungen frühzeitig zu erkennen - E-Mail-Verschlüsselung ist ein Must-Have geworden

In der Vergangenheit kündigte sich Schadsoftware in der Form eines vermeintlichen Lohnzettels per Mailanhang im Postfach an, der sich oft noch als relativ harmlos entpuppte, manchmal als zerstörerisch, oft jedoch als kostspielig, um die negativen Effekte der Malware wieder zu beseitigen. Das Motiv der Urheber war damals, in ihrer Szene berühmt zu werden. Heute ist das anders. Die Motive sind oft finanzieller Natur. Malware wird mit List eingeschmuggelt, ist oft hoch kompliziert und daher viel schwerer zu erkennen, bis es zu spät ist. Es ist sicherer anzunehmen, das alle Daten im Transfer grundsätzlich gefährdet sind und in die falschen Hände geraten können. Also müssen sie verschlüsselt werden.

Versteh die Motive, derer die deine Daten klauen wollen – es hilft Dir, Dich besser zu schützen

Früher wurde Malware oft von ausgegrenzten Jugendlichen geschrieben und über die Malware-Industrie wurde gesagt: „es sind nur Teenager, die noch keine Freundinnen haben“. Heute versucht eine neue Generation von Bösewichten Ihre Informationen zu stehlen, zu ihnen zählen gut organisierte kriminelle Vereinigungen, Regierungsorganisationen mehr oder weniger friedvoll gesinnter Länder und Einzeltäter, deren Motiv meist finanzieller Art ist. Im Falle von regierungsgesponserten Hacks können die Motive auch sehr viel düsterer sein. E-Mail ist eine der besten und einfachsten Angriffspunkte, auf die sich Hacker konzentrieren.

Wir sind mit Anwendungen wie MS Office und E-Mail vertraut. Sie sind leistungsstark und unterstützen uns mehr als alle anderen Werkzeuge am Arbeitsplatz. Doch Arbeitnehmern stellen sich heute immer neue und komplexere Anforderungen, die sich meist in Form von Dateien manifestieren, die viel zu groß für den Versand per E-Mail sind

Sicher werden wir diese nützlichen Tools nicht einfach so aufgeben. Unsere modernen Arbeitsmethoden sind so gestaltet, dass wir in unseren Jobs mit allseits bekannten Anwendungen immer mehr Nutzen schaffen. Wir verwenden diese beiden Anwendungen im Büro und wenn wir unterwegs sind und zunehmend auf mobilen Endgeräten. Dieses Whitepaper richtet sich an ausgewählte Gruppen, z.B. Kunden oder Lieferanten, die dieselben Tools verwenden. Allerdings besitzen diese Anwendungen eine begrenzte oder keine Verschlüsselungsfähigkeit und können mit großen Dateien oder Datenbündeln nicht gut umgehen.

Große digitale Datenmengen, die nicht per E-Mail versendet werden können, verleiten Ihre Mitarbeiter dazu andere Hilfsmittel für den Datenaustausch zu verwenden, wie z.B. USB-Sticks, File-Sharing-Lösungen für Endkunden wie Dropbox oder sie speichern alles auf CD und versenden es per Post. Dieses Ausweichen auf alternative Tools wird als ‚Schatten IT' bezeichnet. Doch es gibt einen besseren Weg!

E-Mail und das Internet haben sich als die Medien für den Austausch von Geschäftsinformationen etabliert

Transportmedien wie Fax, Kuriere oder Post sind seit langem als Übermittlungsmethoden in den Hintergrund getreten. Die Daten, die wir kommunizieren, sind zunehmend digitaler und nicht mehr gedruckter Natur. Dabei versenden wir Informationen per E-Mail über öffentliche Netze, in der Regel über das Internet. Der Grund dafür liegt darin, dass das Internet Daten schnell, zuverlässig und preisgünstig weltweit von A nach B übertragen kann.

Die E-Mail als Transportweg bietet dabei zusätzlich den Vorteil, dass heutzutage praktisch jeder mindestens über eine private und eine geschäftliche E-Mail Adresse verfügt, über die er erreicht werden kann. E-Mail ist leicht zu verwenden und eignet sich dabei außerdem für Nachrichten und Dateien jeglichen Datentyps gleichermaßen. Standards machen unsere Arbeit leichter, aber leider auch die der Hacker. Klartext wird durch Verschlüsselung zu Schlüsseltext umgewandelt und kann ohne den passenden Schlüssel zur Entschlüsselung nicht lesbar gemacht werden. Das zwingt kriminelle Banden in die Knie, doch bringt die Verwaltung von Schlüsseln immer einen administrativen Mehraufwand mit sich.

Außerdem sind die relativen Kosten dieses Übertragungswegs zumindest auf den ersten Blick weit geringer. Für viele Unternehmen ist Geschwindigkeit ein wertvoller Vorteil oder macht sogar ihren Erfolg aus. Aber mit den Vorteilen kommen auch die allseits bekannten Sicherheitsrisiken, wenn Daten per E-Mail übertragen werden. Die Risiken werden von den meisten bewusst, von einigen unbewusst akzeptiert. Dabei können sie ihre Privatsphäre auf einfache Weise schützen.

Viele nehmen das hohe Risiko in Kauf, weil sie meinen, dass robuste Sicherheitsmaßnahmen während der Datenübertragung zu schaffen sehr komplex und teuer ist. Wahrscheinlich noch entscheidender als Kosten und Komplexität ist im Alltag die Akzeptanz durch die Mitarbeiter. Denn selbst die besten Sicherheitsvorkehrungen scheitern, wenn die Nutzer sie nicht akzeptieren. Kostspielige Verschlüsselungsmethoden verlieren dann ihren Wert.

Die Dateiübertragung über das Internet kann auf verschiedene Weise erfolgen. Jede dieser Methoden hat Vor- und Nachteile.

Datenverkehr - Die gängigsten Übertragungsmodi sind:

- per E-Mail als Anhang
- durch Verwendung eines FTP- oder SFTP-Servers
- durch Verwendung einer Anwendung mit eigenem Web-Portal
- über ein öffentliches File-Sharing-Portal im Internet

Dateien, die während des Transfers mit Methoden wie FTP oder unverschlüsselt per E-Mail übertragen werden, sind einfach angreifbare Ziele. Mit allgemein zugänglichen Netzwerkanalyse-Tools, die auch von Netzwerktechnikern zur Suche und Behebung von Fehlern eingesetzt werden, können Datenpakete gescannt und gelesen werden, wenn sie im Klartext übertragen werden. Verschlüsselung macht diese Angriffe zunichte. Aber SFTP-Installationen, die verschlüsseln, verursachen jede Menge Arbeit für Admins und sind nur für einige sehr spezifische und begrenzte Anwendungsfälle geeignet.

Es ist Zeit, alte S/MIME und PGP sowie FTP und S-FTP basierte Lösungen zu ersetzen

S/MIME und PGP

Einige dieser Systeme stellen ein besonderes Risiko dar.

Im Fall von S/MIME beispielsweise ist der Nachrichteninhalt zwar verschlüsselt. Dennoch ist es möglich, die Nachricht zwischen Sender und Empfänger auf jedem Server entlang des Weges unbemerkt zu kopieren und einer Brute-Force-Attacke auszusetzen. Ist eine solche Attacke auf verschlüsselte Inhalte, bei denen ein asymmetrischer Schlüssel verwendet wird, erfolgreich, so kann der ermittelte Schlüssel immer und immer wieder verwendet werden, um verschlüsselt versendete Inhalte lesbar zu machen, ohne dass der Angriff vom Besitzer des Schlüssels je bemerkt wird. Dies wird vor allem dadurch möglich, dass bei jeder Kommunikation der selbe Schlüssel verwendet wird.

Eine weitere Lücke beim S/MIME und PGP besteht darin, dass die Betreffzeile nicht verschlüsselt werden kann, da diese eine technisch notwendige Meta-Information darstellt. Ein Angreifer, der den E-Mail Verkehr überwachen kann, kann so ableiten, wer mit wem über welches Thema spricht. Diese Information kann schon ausreichen, um eine Social Engineering Attacke zu starten und mit dem gewonnenen Wissen weitere Informationen

einem der beiden Kommunikationsteilnehmer weitere Informationen zu entlocken. Es ist schwer, Anwendern zu vermitteln, dass ihre E-Mail Texte zwar vertraulich sind, sie jedoch nur belanglose Betreffzeilen verwenden dürfen. Dies widerspricht außerdem den Grundsätzen für effektive Gestaltung von E-Mail Nachrichten.

Zu guter Letzt lösen S/MIME und PGP nur die Frage, wie Texte sicher ausgtauscht werden können. Aufgrund von Größenbeschränkungen im E-Mail Verkehr bieten Sie jedoch keine Sicherheit beim Austausch von großen Dateien. Hierfür setzen viele Unternehmen daher zusätzlich eine FTP oder S-FTP Lösung ein.

FTP und S-FTP

Die Steuerung des Zugriffs bei FTP erfolgt in der Regel über Benutzerkonten. Hierbei bestehen folgende Herausforderungen und Risiken:

- Benutzerkonten stellen generell ein Risiko dar. Als Benutzername wird häufig die E-Mail-Adresse verwendet, die einfach zu erraten ist und somit keine Sicherheitshürde darstellt. Bei den Passwörtern neigen Anwender dazu, triviale Passwörter zu verwenden, die einfach durch Brute-Force-Angriffe oder durch Kenntnis einiger privater Informationen des Anwenders zu erraten sind (bspw. Geburtsdatum, Lieblingsorte, Namen der Kinder oder Haustiere, die leicht über Soziale Medien zu recherchieren sind).
- Es besteht das Risiko, dass Benutzer das gleiche Login für viele verschiedene IT-Systeme verwenden. Wird eins dieser Systeme gehackt, hat ein Angreifer Zugriff auch auf alle anderen Systeme.
- Administratoren haben i.d.R. immer Zugriff auf alle Daten. Dies gilt auch bei S-FTP Servern, wo Anwender über Zertifikate authentifiziert werden und die Datenübertragung verschlüsselt erfolgt. Die Speicherung der Daten wird durch S-FTP nicht verschlüsselt.
- Die stetige Anlage und Verwaltung von Benutzerkonten und der damit verbundenen Rechte auf den Datenbestand ist ein erheblicher administrativer Aufwand. Schnell ist ein Fehler gemacht und unbefugte Anwender erhalten plötzlich Zugriff auf zahlreiche Daten. Der Versuchung, ein neu auftauchendes Verzeichnis zu öffnen und den Inhalt zu erkunden, widersteht kaum ein Benutzer.
- Häufig bleiben Konten ausgeschiedener interner oder externer Mitarbeiter noch aktiv, weil die IT keine Kenntnis erhalten hat, dass das Konto nicht mehr benötigt wird. Hierdurch entstehen diverse Sicherheitsrisiken – nicht mehr benötigte Daten werden nicht gelöscht, neue Sicherheitsrichtlinien werden auf inaktiven Konten nicht mehr angewendet oder ausgeschiedene Mitarbeiter haben noch geraume Zeit Zugriff auf Daten. Auch sind inaktive Konten ein beliebtes Ziel für Hacker, da ihre Aktivitäten hier weniger schnell auffallen.
- Beim Zurücksetzen vergessener Benutzerpasswörter bestehen Risiken. Hier bieten sich diverse Angriffspunkte für Social Engineering Attacken, die bei Erfolg ebenfalls häufig Zugriff auf einen großen Pool von Daten ermöglichen. Ein Großteil der IT-Support-Aufwände in Unternehmen entfällt auf das Zurücksetzen vergessener Passwörter. In vielen Unternehmen wird der Prozess daher entsprechend lax gehandhabt und die Identität des Anforderers nicht hinreichend geprüft oder einfache, automatisierte Prozesse zum Zurücksetzen des Kennwortes angeboten.

Unabhängig von den technischen Eigenschaften einer Lösung ist außerdem zu bedenken, dass einfache Handhabung und Benutzerfreundlichkeit ein Schlüssel zum Erfolg sind. Denn wenn eine Lösung zwar ein hohes Maß an Sicherheit bietet, von den Anwendern jedoch aufgrund ihrer Komplexität in der Einrichtung oder Handhabung nicht akzeptiert und daher umgangen wird, ist das Ziel nicht erreicht.

Das Senden unverschlüsselter Dateien über das Internet birgt besondere Risiken

Die Risiken das Internet als Datei- und Datentransfermedium zu nutzen, hängen auch sehr stark von der Art der Dateien, der Firmen oder Einzelpersonen, die sie versenden und erhalten, ab. Es gibt zwei mögliche Auswirkungen, wenn Daten in die falschen Hände geraten.

Direkter wirtschaftlicher Schaden

Wenn vertrauliche Informationen versehentlich oder absichtlich in die falschen Hände gelangt, entsteht ein wirtschaftlicher Schaden. Es kann sich hierbei um einen Konkurrenten handeln, einen Betrüger, einen zufälligen „Finder“, einen falschen Adressaten oder um Profis, die den Internet-Verkehr nach Daten absuchen, die sie dazu verwenden, um sich zu bereichern, d.h. Daten an die meistbietende Person zu verkaufen oder gar im Auftrag handeln („Crime as a Service“).

Die Art der Daten, die übermittelt werden, ist je nach Unternehmen unterschiedlich. Die Art und Weise, in der wir heute arbeiten, bedeutet unweigerlich, dass wir die umfassendsten und oft auch vertraulichsten Arbeiten in Anwendungen erstellen, die dafür ausgelegt sind, Daten in Dateien abzulegen – also in Anwendungen wie Microsoft Office, Adobe Acrobat und so weiter. Sollten diese Dateien in die falschen Hände geraten, können die Konsequenzen trivial oder schwerwiegend sein. Im schlimmsten Fall gehen Unternehmen pleite, weil sie ihren Wettbewerbsvorteil verloren haben, weil sie nach Veröffentlichung sensibler Informationen in Rechtsstreitigkeiten verwickelt sind und weil Sicherheitsdaten abhandengekommen sind, die das weitere Ausspionieren des Unternehmens ermöglicht haben.

Diese Art von Verlust ist nicht zwangsläufig eine kriminelle Handlung. Es gibt viele Hacker, die versuchen in vertrauliche Unternehmensbereiche nur so zum Spaß einzubrechen. Für sie ist es ein Spiel, das Wiederherstellen der Daten so schwierig wie möglich zu machen und so viel Schaden wie möglich anzurichten – das ist oft das wahre Ziel von Hackern.

Reputationsschäden, finanzielle Verluste oder Geldbußen

Wenn eine Datei in die falschen Hände gerät, sollte der potenzielle Reputationsschaden nicht unterschätzt werden. Weltweit gibt es eine Reihe von Vorfällen, bei denen der Verlust vertraulicher Daten bekannt wurde. Die Berichterstattung darüber hat den betroffenen Unternehmen und Agenturen natürlich geschadet. Zudem verpflichtet die EU-DSGVO zur Selbstanzeige bei Datenschutzverletzungen.

Zum Beispiel die unbeabsichtigte Veröffentlichung von persönlichen Kundeninformationen durch eine Bank, die Offenlegung von Forschungsinformationen eines Pharmaunternehmens oder der Verlust von CAD-Dateien, die eine zum Patent anzumeldende Produktinnovation darstellen, durch ein spezialisiertes Ingenieurbüro. Allesamt extreme Vorfälle, aber sie sind in der Praxis schon vorgekommen. Also wissen wir, dass es ein Risiko gibt. Aber wie entscheiden wir, welche Lösungen uns helfen uns zu schützen?

EDV-Recht und europäische Datenschutz Gesetzgebungen bringen für alle strengere Anforderungen bei der Datenübertragung - spezialisierte Regelwerke wie das amerikanische Gesetz, das den Datenschutz im Gesundheitswesen regelt, HIPAA, hängen die Latte für wichtige Dienstleistungen höher.

Größere Unternehmen investieren gleich nach Regierungen am intensivsten in Sicherheitslösungen. Dennoch - das Problem Daten ad-hoc zu übertragen und E-Mails zu verschlüsseln gibt es weiterhin, es spiegelt sich in Policy-Verletzungen und verlorenen oder gestohlenen Daten wieder. Die Regulierungsbehörden sind sich dessen bewusst und gehen Verletzungen, wann immer sie aufgedeckt werden, nach.

Zusätzlich lastet viel Druck auf Firmen-E-Mail-Systemen durch den Umfang und die Anzahl von E-Mail-Anhängen. Sie überschreiten nicht selten handhabbare Größen und verursachen dadurch übermäßig Kosten. Eine Umfrage unter europäischen Unternehmen zeigt, dass über 70% aller externen E-Mails mit Dateianhängen versehen ist.

Eine weitere Herausforderung für Unternehmen ist, Computer-Systeme, insbesondere E-Mail-Verkehr, vor Kriminellen zu schützen, die Informationen mit erheblichem kommerziellen Wert stehlen wollen. Es gilt spontan stattfindende Kommunikation mit jeglichen Arten von Inhalten zu sichern. Starke Verschlüsselung ist schwierig zum Einsatz zu bringen, wenn sich der Empfänger außerhalb der Richtlinien und Systeme des Senders befindet.

Typische Transaktionen könnten auch Verträge enthalten. Meist sind dies große und vertrauliche Unterlagen wie zum Beispiel Krankenakten für Kliniken oder Krankenhäuser, Aktenstapel für Gerichte einschließlich PowerPoint- oder Adobe-Dateien mit Grafiken, Tabellenkalkulationen und Text. Ein weiteres Beispiel ist ein Mitarbeiter, der Informationen mit externen Lieferanten austauscht und Daten für neue Produktprozesse sammelt. Die Dokumente enthalten typischerweise Videos, .pdf-Dateien, Tabellenblätter, Kundendaten und vieles mehr.

Was sind die gemeinsamen Attribute?

Die folgenden Formen des Austauschs haben einige gemeinsame Eigenschaften und sind in allen Branchen verbreitet. Einfache Verbesserungsmaßnahmen können zu beeindruckenden Einsparungen führen – die Entscheidung sollte je nach Anwendungsfall getroffen werden.

- Die Dateien sind relativ groß und können entweder vom Sender oder Empfänger nicht per E-Mail versendet bzw. empfangen werden (weshalb sie auf andere Weise übertragen werden müssen).
- Der Inhalt ist vertraulich, oft streng geheim, und somit ist Verschlüsselung erforderlich, außerdem ist ein zusätzlicher, getrennter Kanal für den Austausch des Passwortes wünschenswert.
- Der Absender ist verpflichtet, gesetzliche Bestimmungen zu Sicherheit und Vertraulichkeit zu erfüllen.
- Mindestens einer der Kommunikationspartner kann sich außerhalb des Unternehmens-netzwerks und damit außerhalb der durch das Unternehmen kontrollierten technischen Umgebung und Infrastruktur befinden.
- Der Absender muss nachweisen können, was versendet und empfangen wurde.
- Manche Informationen sind vertraulich und müssen auf sicherem Weg zu mehreren Empfängern versendet werden, d.h. Massenzustellung muss automatisiert konfigurierbar sein.

Eine gute Anforderungsliste sieht so aus

Befragt nach den Schwierigkeiten beim Implementieren von Software-Produkten, die den Unternehmen beim Lösen ihrer Probleme helfen sollen, wurden häufig folgende Anforderungen genannt.

Geordnet nach der Wichtigkeit basierend auf der Anzahl der Kunden, die diese Probleme geäußert haben:

- Usability: Jede Lösung sollte einfach zu bedienen und leicht zugänglich sein.
- Nachvollziehbarkeit: die Lösung muss das Aufzeichnen von Transaktionen ermöglichen.
- Policy Management: Die Lösung sollte es gestatten, dass Nutzungsrichtlinien verwaltet und technisch durchgesetzt werden können und eine Schnittstelle zu Lösungen wie Antivirenscanner und Archivierungswerkzeuge zulassen.
- Große Dateien: Die Lösung sollte mit großen Dateien umgehen, auf jeden Fall größer als 5GB, in einigen Fällen größer als 100GB
- Flexible Bereitstellungsoptionen: Die Lösung sollte verschiedene Bereitstellungsmethoden anbieten.
- Integration: Die Lösung sollte sich möglichst einfach in die vorhandene IT- und Sicherheits-Infrastruktur integrieren.
- Anpassung: Die Benutzeroberfläche der Lösung sollte an das Corporate Design angepasst werden können.
- Eine neue Lösung in diesem Bereich sollte mindestens zwei alte Lösungen ersetzen.

Cryptshare®
Making e-mail better

Schlussfolgerung

Nicht zu handeln ist keine Option. Jüngste Bedrohungen, neue Gesetze und einfachere Technologien sind mehr als ein guter Grund genau jetzt tätig zu werden. Finanzielle Einsparungen durch Ersetzen veralteter Technologien machen den Deal perfekt. Rufen Sie uns jetzt an und besprechen Sie Ihre Anforderungen mit uns!

Fragen Sie sich, ob Cryptshare Ihre Geschäftskommunikation per E-Mail sicherer machen kann?

Kontaktieren Sie mich für weitere Informationen!

Dominik Lehr
E: dominik.lehr@cryptshare.com
T: +49 761 389 130

Über Cryptshare:

Cryptshare ist die Softwarelösung um E-Mails und große Dateien jederzeit sicher austauschen zu können und die Sie dabei unterstützt, Richtlinien und Compliance-Vorgaben einzuhalten. Cryptshare ist preiswert und leistungsstark. Cryptshare – making e-mail better.
Weitere Informationen finden Sie unter www.cryptshare.com oder wiki.cryptshare.com.

Wie alles begann

Das Unternehmen Befine wurde 2000 gegründet. Es entwickelte zunächst kundenindividuelle Softwarelösungen im Auftrag von Blue Chip Unternehmen. Im Laufe der Jahre wurden diverse Lösungen für unterschiedliche Kunden entwickelt. Mit kleinen Änderungen oder einfachen Anpassungen wurden diese auch für einen größeren Kundenkreis anwendbar. Das Team erfüllte die Anforderungen vieler Kunden, indem es wiederverwendbare, stabile, skalierbare und effektive Lösungen für komplexe Probleme entwarf. Wir glauben, dass wir Probleme lösen, die andere nicht lösen können. Das ist unser Business, tagtäglich.

Die Entwicklung von Cryptshare

2007 kauften die ersten Kunden Cryptshare. Umgehend trafen Anfragen von anderen Unternehmen ein, eine Cryptshare-Lizenz kaufen zu wollen. Fehlende Möglichkeiten zum ad-hoc-Austausch von großen Dateien und die mangelnde Sicherheit von E-Mails wurden schnell als allgemeines Problem in großen und kleinen Unternehmen über alle Branchen hinweg identifiziert. Mit Hilfe der Rückmeldungen vom Markt und unserem starken Glauben an unsere Lösung haben wir eine Produkt-Roadmap definiert, in der die zusätzlichen Funktionen festgelegt wurden, die unsere schnell wachsende Kundengruppe benötigte. Einfache Bedienung, starke Verschlüsselung, regelmäßige Updates, anspruchsvolle Management-, Konfigurations- und Steuerungsfunktionen und die Möglichkeit, mit anderen Applikationen über einfache APIs zu kommunizieren zeichnen die Lösung aus. Viele weitere Funktionen wurden hinzugefügt, wobei Patentgenehmigungen für die wichtigsten Innovationen noch ausstehen.

Cryptshare heute

Dank der Reseller in vielen Ländern ist die Anzahl unserer Kunden seit 2010 rasch gewachsen, so dass auch der Umsatz in die Höhe schnellte. Der kontinuierliche Ausbau unseres Teams hat uns ermöglicht, die Roadmap noch spezifischer weiterzuentwickeln, mehr technischen Support zu leisten, ein noch spezielleres Produktmanagement aufzustellen sowie mit weiteren Vertriebs- und Marketingaktivitäten Kunden in 30 Ländern mit mehr als 3 Millionen lizenzierte Nutzern zu gewinnen.

Jetzt mehr erfahren.
Cryptshare - making e-mail better.

www.cryptshare.com

Cryptshare jetzt testen.

Cryptshare®
Making e-mail better

Befine Solutions AG

Schwarzwaldstraße 151
79102 Freiburg
Germany

Telefon: +49 761 / 38913-0
Fax: +49 761 / 38913-115
E-Mail: info@befine-solutions.com
Web: www.befine-solutions.com

Registergericht Freiburg, HRB 6144

Vertretungsberechtigter Vorstand: Mark Forrest, Dominik Lehr
Vorsitzender des Aufsichtsrates: Thilo Braun

UST-Ident: DE812922179

Stand: Juni 2017

E-Mail-Verschlüsselung
Anhänge jeder Größe
IT-Compliance