SOPHOS

Wer liest Ihre E-Mails mit?

Worauf Sie bei der Wahl eines sicheren E-Mail-Gateways achten sollten

Autor: **Chris McCormack**, Senior Product Marketing Manager

Seit bekannt wurde, dass die US-Regierung im großen Stil elektronische Daten abfängt, ist das Thema Online-Datenschutz einmal mehr in den Fokus der Öffentlichkeit gerückt. Dabei ist der Verlust sensibler Unternehmensdaten in den meisten Fällen nicht auf behördliche Überwachung oder Wirtschaftsspionage zurückzuführen. Vielmehr sind E-Mails das größte Risiko für die Offenlegung vertraulicher Daten. In diesem White Paper erhalten Sie daher wertvolle Tipps zum Thema E-Mail-Sicherheit. Sie lernen die besonderen Herausforderungen bei der Durchsetzung von Datenschutzrichtlinien kennen und erfahren von uns, warum Sie ein sicheres E-Mail-Gateway benötigen, das mehr bietet als eine bloße Verschlüsselung.

Sophos White Paper September 2013

Ihre E-Mails sind ein offenes Buch

Fast der gesamte E-Mail-Verkehr durchläuft das Internet unverschlüsselt und in Klartext, was in etwa mit dem Versenden einer Postkarte vergleichbar ist. Jeder, der mit bösen Absichten oder auch durch Zufall auf eine Ihrer E-Mails stößt, kann mitlesen, ohne dass Sie es bemerken.

Sie fragen sich vielleicht, wer sich für Ihre E-Mails interessieren sollte. Haben Sie schon einmal an Ihren Internet- oder Ihren E-Mail-Anbieter gedacht? Google hat auf jeden Fall Interesse. In aktuellen Gerichtsakten bekennt Google, dass Gmail-Nutzer keine „berechtigte Erwartung" hinsichtlich der Privatsphäre oder Vertraulichkeit ihrer Daten haben sollten.[1] In seinem Bestreben, im Mai 2013 eine Sammelklage abzuwehren, erklärte Google:

> „Alle E-Mail-Benutzer müssen zwangsläufig davon ausgehen, dass ihre E-Mails eine automatische Verarbeitung durchlaufen. Genau wie der Absender eines Briefs an einen Geschäftskollegen nicht erstaunt sein sollte, wenn dieser von der Sekretärin geöffnet wird, sollten auch Benutzer webbasierter E-Mail-Services damit rechnen, dass ihre E-Mails bei der Zustellung durch den [E-Mail-Anbieter] des Empfängers verarbeitet werden. Tatsächlich besteht kein rechtlicher Anspruch auf den Schutz von Daten, die freiwillig Dritten übergeben werden."[2]

Die US-Verbraucherschutzorganisation „Consumer Watchdog" hält dies für ein „schockierendes Geständnis" und rät Personen, die bei E-Mails Datenschutz-Bedenken haben, von der Nutzung von Gmail ab.[3] Leider ist damit das Problem nicht gelöst. Genauso gut könnte man gleich gänzlich vom E-Mail-Schreiben abraten. Denn auch wenn Sie selbst Gmail nicht nutzen, müssen Sie per E-Mail mit Kunden, Geschäftspartnern oder anderen Stakeholdern kommunizieren, die möglicherweise ein Konto bei Gmail haben.

Vielleicht haben Sie auch schon von PRISM gehört, einem geheimen Massen-Data-Mining-Programm zur elektronischen Überwachung unter der Leitung der US-amerikanischen National Security Agency (NSA), das bereits seit einigen Jahren existiert. Die NSA hat bislang unbekannte Mengen an E-Mail-Daten von Google, Internetanbietern und anderen Online-E-Mail-Diensten wie Hotmail und Yahoo gesammelt und gespeichert.

Die Risiken beim Versand von E-Mails beschränken sich jedoch nicht auf internationale Spionage von Google, NSA und Co. Haben Sie auch schon einmal versehentlich auf „Alle antworten" geklickt, obwohl die E-Mail eigentlich nur für einen Empfänger bestimmt war? Oder wegen der automatischen Ergänzungsfunktion Ihres E-Mail-Clients versehentlich eine E-Mail an die falsche Person geschickt? Solche Missgeschicke sind alles andere als die Ausnahme. Sensible Daten an den falschen Empfänger zu senden, kann schwerwiegende Folgen haben. Nicht nur ist es u. U. erforderlich, die Öffentlichkeit über die Datenpanne zu informieren – es drohen darüber hinaus u. a. empfindliche Geldstrafen, ein nachhaltiger Vertrauensverlust sowie ein dauerhaft beschädigtes Ansehen.

1 http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

2 http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm

3 http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care

Spoofing, Spearphishing und Snowshoe-Spam

Eine weitere große Gefahr stellen Angriffe via E-Mail dar. Zu den bekanntesten Angriffsformen gehört das so genannte Phishing, bei dem versucht wird, über gefälschte, seriös anmutende E-Mails an Informationen wie Benutzernamen, Passwörter oder Kreditkartendaten zu gelangen.

Phishing ist oft erfolgreich, weil die Angreifer dabei ein Verfahren nutzen, das gemeinhin als Mail-Spoofing bekannt ist. Hierbei wird die E-Mail-Adresse des Senders gezielt so gestaltet, dass sie einem echten seriösen Account stark ähnelt. So wird vorgetäuscht, die E-Mail stamme aus einer vertrauenswürdigen Quelle (z. B. von einer Bank). In manchen Fällen wird sogar der Domainname eines Unternehmens verwendet, damit es so aussieht, als käme die E-Mail von einem internen Sender wie der IT-Abteilung.

Mittlerweile ist eine weitere, noch trickreichere Angriffsform auf dem Vormarsch, bei der versucht wird, gezielt Kontakt zu Einzelpersonen oder Gruppen innerhalb von Unternehmen oder Einrichtungen aufzunehmen. Diese als Spearphishing bezeichnete Taktik erfolgt oft im Rahmen sogenannter Advanced Persistent Threats. Ziel solcher Angriffe ist es, sich Zugang zu bestimmten Unternehmensnetzwerken zu verschaffen und dadurch an vertrauliche Daten zu gelangen.

Außerdem gibt es natürlich immer noch den altmodischen E-Mail-Spam. Dank Ihres Anti-Spamfilters landet der Großteil des Spams vermutlich gar nicht erst in Ihrem Posteingang, und die merkwürdigen E-Mails von nigerianischen Prinzen, die es durch den Filter schaffen, erkennen Sie leicht selbst als Spam.

Und doch fallen Internetnutzer immer wieder auf Spam-Mails herein und lassen sich dazu bringen, schädliche Anhänge zu öffnen. Forscher haben herausgefunden, dass Spam, der vorgibt, von sozialen Medien wie Facebook zu stammen, besonders effektiv ist.[4]

Spammer werden immer einfallsreicher, wenn es darum geht, Spam-Filter zu umgehen. Beim Snowshoe-Spamming z. B. wird für den Versand der Mails eine große Zahl unterschiedlicher IP-Adressen genutzt. Dadurch ist es für Spam-Filter sehr schwierig, all diese Mails als Spam zu identifizieren und die Chance steigt, dass es die eine oder andere Mail in den Posteingang der Nutzer schafft.

Einhaltung gesetzlicher Vorschriften

Sensible Daten von Kunden, Geschäftspartnern und Mitarbeitern zu schützen, ist nicht nur bewährte Praxis, sondern oft auch gesetzlich vorgeschrieben. Besonders im Gesundheitswesen, im Finanzsektor und in Behörden genießt die Einhaltung solcher Vorschriften höchste Priorität. Und selbst, wenn Sie nicht in einer dieser Branchen tätig sind, müssen Sie Datenschutzgesetze einhalten, die unter Umständen Ihre Kunden betreffen.

In fast allen Ländern gelten mittlerweile eine Reihe von Gesetzen und Vorschriften bezüglich der Compliance und Offenlegungsanforderungen im Fall einer Datenschutzverletzung. Alle haben gemein, dass sie bestimmte Anforderungen an die Verschlüsselung personenbezogener Daten stellen, die entweder elektronisch gespeichert oder übertragen werden (über E-Mail oder sonstige Verfahren). Diese Gesetze regeln meist die fälligen Bußgelder oder Geldstrafen im Falle von Datenschutzverstößen sowie die offenzulegenden Informationen im Falle einer Datenschutzverletzung oder eines Datenverlusts.

4 "Evolving spammers using bogus social media email to fool users," BizReport, August 28, 2013, http://www.bizreport.com/2013/08/evolving-spammers-using-bogus-social-media-email-to-fool-use.html

In drei einfachen Schritten zu Compliance

1. Erstellen Sie eine Richtlinie und klären Sie Ihre Benutzer auf

Stellen Sie Ihren Mitarbeitern und Stakeholdern eine Richtlinie zur Verfügung, in der die wichtigsten Elemente Ihrer Datenschutzstrategie erläutert werden. Konzentrieren Sie sich auf die Datentypen, die Sie schützen müssen, Ihre Gründe, diese zu schützen, die Konsequenzen, falls kein Schutz erfolgt, sowie die zu treffenden Maßnahmen zum Schutz der Daten.

2. Installieren Sie Datenschutztechnologie für E-Mails

Um einen verlässlichen Schutz zu ermöglichen, benötigen Sie für Ihre Benutzer nicht nur eine Richtlinie, sondern auch eine wirksame, transparente Sicherheitstechnologie. Diese muss nicht nur versehentliche Datenverluste verhindern, sondern auch Schutz für sensible Daten bieten, die das Unternehmen verlassen. Ein sicheres E-Mail-Gateway mit richtlinienbasierter Verschlüsselung ist die Basis zur Durchsetzung Ihrer Datenschutz-Compliance.

3. Beginnen Sie mit den wichtigsten Schutzfunktionen und erweitern Sie diese nach und nach

Datenschutz kann schnell eine kaum zu bewältigende Aufgabe werden. Deshalb sollten Sie Ihre erforderlichen Datenschutz-Maßnahmen unbedingt nach Prioritäten ordnen. Beginnen Sie dort, wo Datenverluste besonders wahrscheinlich sind – bei Ihren E-Mails. Vergewissern Sie sich, dass Sie über die notwendigen Richtlinien verfügen, um zunächst besonders sensible Daten von Kunden, Mitarbeitern oder Geschäftspartnern zu schützen – beispielsweise Kreditkartendaten. Sobald diese Richtlinien einwandfrei funktionieren, können Sie über weitere Maßnahmen nachdenken.

Herausforderungen

Gute Gründe für den Schutz von E-Mails gibt es genug. Welche Herausforderungen halten Sie noch davon ab, Ihre E-Mails mit einer Verschlüsselungslösung zu sichern?

Zu viel Aufwand: Die meisten Lösungen zur E-Mail-Verschlüsselung sind schwierig zu erwerben, zu installieren und zu bedienen. Viel Aufwand ist nötig, um eine Infrastruktur zu testen und bereitzustellen, die dann auch noch weitreichende Auswirkungen auf das gesamte Unternehmen hat. Wesentlicher einfacher wäre es, wenn Ihr derzeitiger IT-Security-Anbieter eine Lösung für Sie hätte, die Sie nur anschließen müssen und sofort nutzen können – ohne ein großflächiges Bereitstellungsprogramm und Experten, die das Ganze koordinieren.

Hohe Kosten: Die meisten Verschlüsselungslösungen sind teuer in der Anschaffung und verursachen auch langfristig laufende Kosten für Verwaltung und Wartung. Wäre es nicht ideal, wenn es eine Lösung für die E-Mail-Sicherheit gäbe, die Verschlüsselung und DLP im Rahmen Ihres bestehenden Anti-Spam-Budgets bieten könnte?

Benutzerfreundlichkeit: Die meisten Lösungen zur E-Mail-Verschlüsselung beeinträchtigen die Arbeitsabläufe der Endbenutzer. Denn um sensible Daten verschlüsseln zu können, müssen die Benutzer bei diesen Lösungen selbst aktiv werden. Fehler sind damit vorprogrammiert. Oder die Benutzer müssen verschlüsselte E-Mails außerhalb des normalen E-Mail-Workflows verarbeiten, was die Produktivität mindert und auf wenig Akzeptanz bei den Benutzern stößt. Bessere Lösungen werden transparent im Hintergrund ausgeführt, benötigen keine separate Clientsoftware und verschlüsseln E-Mails automatisch auf Grundlage von DLP-Richtlinien, ohne Benutzer bei der Arbeit zu behindern.

Die Herausforderungen meistern: Was sollte Ihnen eine gute Lösung bieten?

Im Folgenden finden Sie eine Checkliste mit Funktionen, die Ihnen eine gute Lösung für ein sicheres E-Mail-Gateway bieten sollte.

Einfache Bedienung und Verwaltung

- Die Lösung sollte im Idealfall die Funktionen Anti-Spam, DLP sowie eine einfache, richtlinienbasierte E-Mail-Verschlüsselung als Kombipaket in einem einzigen Produkt von einem einzigen Anbieter enthalten. Außerdem sollte sie sich einfach über eine zentrale Konsole verwalten lassen.
- Die Lösung sollte über vorkonfigurierte Typen sensibler Daten verfügen, damit Sie DLP-Richtlinien direkt ohne großen Aufwand einrichten können.
- Die Richtlinien zur E-Mail-Verschlüsselung sollten so einfach gestaltet sein, dass jeder Mitarbeiter neue Richtlinien einrichten oder bereits vorhandene Richtlinien abändern kann, ohne dafür eine Schulung besuchen oder Handbücher lesen zu müssen.
- Die Lösung sollte ohne langwierige und komplexe Schlüsselverwaltung auskommen.

Erschwinglicher Preis

- Im Idealfall sollte die Lösung DLP und E-Mail-Verschlüsselung zu einem Preis bieten, der im Rahmen Ihres aktuellen Anti-Spam-Budgets liegt.
- Die Lösung sollte sich einfach testen und implementieren lassen – ohne, dass zusätzlich zu Ihrer bestehenden Anti-Spam-Lösung noch spezielle Hardware, Software oder eine Schulung benötigt wird.

Hohe Benutzerfreundlichkeit

- Eine gute Lösung zur E-Mail-Verschlüsselung sollte E-Mails und Anhänge automatisch auf sensible Datentypen scannen und sie verschlüsseln, bevor sie das Unternehmen verlassen – automatisch und transparent, ohne dass Benutzer E-Mails speziell zur Verschlüsselung markieren müssen (kann schnell vergessen werden).
- Die Lösung sollte die Arbeitsabläufe der Sender und Empfänger nicht beeinträchtigen. Die Benutzer sollten in der Lage sein, E-Mails wie gewohnt zu senden – und zwar mit dem E-Mail-Client ihrer Wahl auf ihrem Desktop, Laptop, mobilen Gerät oder online.
- Es sollte keine Spezialsoftware oder das Aufrufen eines Webportals notwendig sein, damit Empfänger die verschlüsselten E-Mails einsehen können.

Die Lösung von Sophos: SPX Encryption und Data Loss Prevention

Sophos bietet Ihnen eine Lösung, mit der Sie all diese Herausforderungen meistern und Ihre Daten zuverlässig schützen können: Unsere innovative, zum Patent angemeldete SPX Encryption mit integrierter DLP-Richtlinie und vorkonfigurierten Typen sensibler Daten.

Die Lösung ist einfach bereitzustellen und beinhaltet ein Kombipaket aus Anti-Spam, E-Mail-Verschlüsselung und Data Loss Prevention in einer einzigen Appliance. Es muss keine spezielle Client-Software installiert werden.

Alle Elemente lassen sich über eine zentrale, intuitive Konsole ganz ohne Schlüssel- oder Zertifikatsverwaltung steuern, während ein eleganter DLP-Assistent dafür sorgt, dass Ihr Datenschutz innerhalb weniger Minuten einsatzbereit ist.

Unsere DLP-Engine wird mit Hunderten bereits vorkonfigurierten Typen sensibler Daten ausgeliefert, so dass Sie direkt wirksame DLP-Richtlinien erstellen können. Natürlich können Sie zusätzlich auch benutzerdefinierte Datentypen anlegen.

Die gesamte Lösung ist dabei transparent für die Benutzer und kann mit deren bevorzugtem E-Mail-Client genutzt werden (auch auf mobilen Geräten). Gleichzeitig ist die Lösung erschwinglich, denn mit unserer Sophos Email Appliance erhalten Sie eine Fülle von Funktionen – und das zu einem Preis, den Sie momentan wahrscheinlich nur für reinen Spamschutz zahlen (verfügbar in unserer UTM Email Protection, Version 9.2, Veröffentlichung Frühjahr 2014).

Kostenlose Testversion auf sophos.de

Sophos Email Appliance testen

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858-0 | +49 721 255 16-0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA

09.13.wpna.simple

SOPHOS