5 GRÜNDE …

… für mehr **E-Mail**-Sicherheit

Laut The Radicati Group wird die Gesamtzahl der pro Tag gesendeten und empfangenen Geschäfts- und Verbraucher-E-Mails 2020 die 306 Milliarden-Grenze übersteigen und bis zum Jahresende 2024 auf über 361 Milliarden anwachsen. Das bedeutet: mehr als die Hälfte der Weltbevölkerung nutzt E-Mails | VON DEBBIE HAYES

Aber haben wir wirklich verstanden, wie wichtig E-Mail-Sicherheit ist? Wir liefern Ihnen für 5 Gründe, warum E-Mail-Sicherheit für Unternehmen Priorität haben sollte:

1. In unserer zunehmend digitalen Welt ist Vertrauen alles: Besonders jetzt, wo viele von uns Geschäfte und Kommunikation aus der Ferne abwickeln, sollte man sicher sein können, daß die E-Mails tatsächlich von der Person verschickt worden sind, die sie vorgibt zu sein. Sie wollen ebenso sicherstellen, daß die Empfänger ihrer E-Mails wissen, daß sie zweifelsfrei von Ihnen stammen. Sie sparen Zeit und Kosten, wenn Sie nicht doppelt prüfen und bestätigen müssen, ob jemand eine E-Mail gesendet hat. Das Signieren von E-Mails mit einem digitalen Zertifikat ist der beste Weg, um Empfängern – Kunden, Kollegen, Lieferanten – visuell anzuzeigen, daß eine E-Mail vertrauenswürdig ist. Digitale Zertifikate die von einer Public Key Infrastructure (PKI) unterstützt werden, sind die am häufigsten verwendete Technologie beim Sichern von E-Mails, und sie wird von praktisch allen Anwendungen erkannt. Das bedeutet, daß Sie die Schlüssel besitzen, die Ihre Signatur vertrauenswürdig und sicher machen. >>

2. E-Mail-Sicherheit hilft, geschäftliche Risiken zu vermeiden: Eine weitere wichtige Komponente der E-Mail-Sicherheit ist die Verschlüsselung. Wenn Sie E-Mails ohne Verschlüsselung senden, kann prinzipiell jeder auf die darin enthaltenen Informationen zugreifen. Mit anderen Worten, jemand kann die E-Mail abfangen, den Inhalt lesen oder sogar ändern und sie dann in Ihrem Namen an den Absender zustellen lassen. Wenn Hacker Zugriff auf persönliche Informationen erlangen, hat ein Unternehmen schnell seinen Vertrauensvorschuß verspielt.

3. E-Mail-Sicherheit senkt Compliance-Risiken und die Höhe der damit verbundenen Bußgelder: Die meisten Unternehmen unterliegen Regeln und Vorschriften, zum Schutz von personenbezogenen Verbraucherdaten. Die HIPAA-Datenschutzbestimmung wurde beispielsweise erlassen, um Gesundheits- und Patientendaten zu schützen. Die Datenschutz-Grundverordnung ist eine weitere wichtige Vorschrift, nach der Unternehmen personenbezogene Daten der Benutzer „in allen Formen" schützen müssen – dies schließt Daten ein, die per E-Mail erhoben und übermittelt werden. Weitere Informationen zu den Richtlinien der DSGVO für E-Mails finden Sie unter *GDPR.eu*. Die Nichteinhaltung der geforderten Vorschriften kann Bußgelder in nicht unerheblichen Höhen nach sich ziehen.

4. E-Mail-Verschlüsselung schützt vertrauliche Informationen: Die E-Mail-Verschlüsselung schützt vertrauliche Informationen wie Kreditkartendaten, Kontonummern und viele weitere mehr. Sie verhindert, daß Außenstehende sich zwischen Ihre E-Mails und den Mail-Server schalten und sensible Daten abfangen. Eine Methode an Daten zu gelangen, sind Phishing-Angriffe. Inzwischen versenden mehr Menschen als je zuvor E-Mails. Damit steigt die Zahl der Cyberkriminellen, die E-Mail für ihre Zwecke nutzen. Einem Bericht des PCMag zufolge haben Phishing-Angriffe seit Beginn des Social Distancing durch die COVID-19-Pandemie um 350% zugenommen. Wer böswillig agierenden Entitäten oder Hackern den Zugriff auf Daten ermöglicht, gefährdet potentiell das gesamte Unternehmen.

5. Das Signieren von E-Mails kann Identitätsdiebstahl verhindern: Wenn eine Person in den Besitz Ihrer persönlichen Daten wie Benutzername und Passwort gelangt, kann sie Ihre Identität dazu benutzen, gefälschte E-Mails in ihrem Namen zu versenden. Wenn allerdings jeder seine E-Mails digital mit seiner Identität signieren würde, gäbe es keine Phishing-E-Mails. Man wüßte zweifelsfrei, wer die Mail geschickt hat. Die Suche nach einer E-Mail-Verschlüsselungslösung, die den Bedürfnissen Ihres Unternehmens entspricht, ist nicht unbedingt leicht. Es stehen viele Optionen zur Verfügung, aber letztendlich brauchen Sie eine Lösung, die einfach zu bedienen, zuverläßig, sicher und kostengünstig ist.

S/MIME, das für Secure/Multipurpose Internet Mail Extensions steht, ist eine Technologie, mit der Sie E-Mails verschlüsseln können. Sie ermöglicht es Ihnen, zusätzlich E-Mails digital zu signieren, um sich als legitimen Absender der E-Mail auszuweisen. Auf diese Weise läßt sich feststellen, welche E-Mails authentisch sind und welche möglicherweise als Teil eines Phishing-Angriffs gesendet wurden. S/MIME basiert auf asymmetrischer Verschlüsselung, die ein Paar mathematisch verknüpfter Schlüssel verwendet – einen öffentlichen Schlüssel und einen privaten Schlüssel, die E-Mails vor unerwünschtem Zugriff schützen. Es ist nicht möglich, den privaten Schlüssel anhand des öffentlichen Schlüssels herauszufinden. E-Mails werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dem korrespondierenden privaten Schlüssel entschlüsselt werden. Angesichts dessen ist es nicht überraschend, daß S/MIME heute das am häufigsten verwendete E-Mail-Sicherheitsprotokoll ist – es ist extrem einfach zu benutzen und alle E-Mail-Clients und -Server sind dazu kompatibel.

Debbie Hayes, GlobalSign

Als Mitarbeiter von großen Unternehmen oder KMUs können Sie Ihre E-Mails mit S/MIME signieren, um die Identität als legitimes Unternehmen nachzuweisen. Jedes Mal, wenn Sie eine E-Mail erstellen und signieren, fügt Ihr privater Schlüssel Ihre einzigartige digitale Signatur in die Nachricht ein. Wenn der Empfänger Ihre E-Mail öffnet, wird Ihr öffentlicher Schlüssel zur Verifizierung der Signatur verwendet. Dadurch ist sichergestellt, daß der Empfänger weiß, daß die E-Mails tatsächlich von Ihnen stammen. Phishing-Angriffe sind inzwischen extrem raffiniert und haben nicht mehr viel mit der ursprünglichen Gattung gemein. Dadurch wird es immer schwieriger zu erkennen, ob eine E-Mail gefälscht ist oder nicht. Deshalb ist es so wichtig, E-Mails zu signieren und so die Identität zu authentifizieren.

Noch Fragen?
https://www.globalsign.com/de-de/sichere-email

Bild: GlobalSign