Keine Chance für Phishing und Malware

Digitale Signatur als zentraler Baustein des sicheren E-Mail-Verkehrs

E-Mails sind nach wie vor das wichtigste geschäftliche Kommunikationsmittel. Gleichzeitig gehören sie zu den besonders beliebten Einfallstoren bei Hackern. Ein Großteil der verübten Cyberangriffe erfolgt über Phishing-Mails mit manipulierten Anhängen oder Links. Die Kriminellen verschaffen sich so gezielt Zugriff auf Unternehmensnetzwerke, greifen Registrierungsdaten ab oder verbreiten Schadsoftware. Insgesamt werden die Phishing-Methoden immer professioneller, und die Fake-E-Mails sind kaum mehr von echten zu unterscheiden; es sei denn, eine digitale Signatur kommt zum Einsatz.

Von Günter Esch, SEPPmail – Deutschland GmbH

Immer wieder liest man davon, dass Cyberkriminelle gefälschte elektronische Nachrichten versenden, um etwa an Passwörter für Online-Dienste zu gelangen, Geldtransaktionen abzupassen oder Trojaner in Umlauf zu bringen. Die Hacker geben sich als seriöse Absender aus, zielen aber bloß darauf ab, sensible Unternehmensinformationen zu erlangen. Derartige Phishing-Mails sind in vielen Fällen nicht auf Anhieb als solche zu erkennen, denn die Angriffe entpuppen sich häufig als äußerst perfide. Gerade wenn E-Mails auf die Schnelle geöffnet werden, hat man ruckzuck einmal versehentlich auf einen Link geklickt. Aus diesem Grund ist die Einführung entsprechender E-Mail-Sicherheitsmaßnahmen unverzichtbar. Eine von ihnen: die digitale Signatur. Ein ungebrochenes Siegel signalisiert dem Empfänger, dass die eingegangene E-Mail tatsächlich vom angegebenen Absender stammt, auf dem Versandweg nicht verändert wurde und damit sicher ist.

RFC-konforme Signatur über Zertifikate

Die digitale Signatur dient dem Unterschreiben von elektronischen Dokumenten und hat zum Ziel, die Identität des Unterzeichners nachzuweisen. Sie sorgt für die gewünschte Authentizität und Integrität beim E-Mail-Verkehr und verhindert, Phishing-Nachrichten auf den Leim zu gehen. Um E-Mails mit einer Signatur zu versehen, ist ein Zertifikat vonnöten, das bei einer akkreditierten Zertifizierungsstelle beantragt werden muss. Diese sogenannten Certificate Authorithies (CAs), beispielsweise SwissSign, DigiCert, D-TRUST oder Sectigo, belegen schließlich, dass das Zertifikat, also der persönliche, öffentliche Schlüssel, zu einer bestimmten Person gehört. Bei modernen Lösungen lassen sich die benötigten Zertifikate über eine Managed-Public-Key-Infrastructure (MPKI) bei der ersten ausgehenden E-Mail des Nutzers automatisch durch die Appliance beziehen. Alternativ können sie manuell für den jeweiligen User importiert werden. Dafür müssen die erforderlichen Funktionalitäten wie die PKI, die Konnektoren zu offiziellen CAs sowie die Zuweisungsmöglichkeit der Zertifikate zu den Anwendern standardmäßig in der Lösung integriert sein. Zudem sollte das Verfahren von sämtlichen E-Mail-Clients unterstützt werden, ohne dass empfängerseits spezifische Softwarekomponenten oder Tools zur Signaturprüfung notwendig sind. Auf diese Weise trägt eine geeignete Lösung zur Minimierung des administrativen Aufwands bei der Erstellung digitaler Signaturen bei, und der gesamte PKI-Prozess geht deutlich schneller vonstatten.

All-in-One-Lösung für gesteigerte E-Mail-Sicherheit

Neben der Signatur spielt auch die Verschlüsselung eine tragende Rolle beim Schutz von

E-Mails. Denn unverschlüsselte Mails gleichen einer Postkarte und können von Dritten ohne Weiteres abgefangen und mitgelesen werden. Hinzu kommt, dass die Europäische Datenschutzgrundverordnung (EU-DSGVO) die Verschlüsselung elektronischer Nachrichten, die personenbezogene Informationen enthalten, eindeutig vorschreibt. Umso verwunderlicher ist es, dass längst nicht alle Unternehmen eine Verschlüsselungslösung nutzen. Oftmals wird davon ausgegangen, der Prozess sei mit zu viel Aufwand verbunden und würde den gewohnten Flow des Arbeitsalltages unterbrechen. Doch anders als von vielen erwartet, gibt es bereits zuverlässige Lösungen, die es erlauben, einfach und sicher mit jedermann via E-Mail zu kommunizieren. Um sowohl die Signatur als auch die Verschlüsselung abzudecken, bietet sich die Nutzung eines Secure-E-Mail-Gateway an, das beides beherrscht. Als i-Tüpfelchen lassen sich über ein solches Gateway auch übergroße Dateien geschützt übermitteln, damit nicht länger auf kostenfreie Filehosting-Dienste zurückgegriffen wird, die ein zusätzliches Risiko darstellen. Ein Central-Disclaimer-Management, das die E-Mails zentral mit Firmeninformationen ergänzt, rundet das Komplettpaket letztlich optimal ab.

Verschlüsselung – alles andere als kompliziert

Wird eine Appliance zur Verschlüsselung implementiert, ist das nicht zwangsläufig mit großem Mehraufwand verbunden. Auf der Suche nach einer passenden Lösung sollten lediglich ein paar wesentliche Punkte beachtet werden. So ist es unter anderem essenziell, dass die Secure-E-Mail-Lösung alle gängigen Verschlüsselungsverfahren wie S/MIME, OpenPGP, TLS und Domainverschlüsselung unterstützt. Beim Versand einer E-Mail gilt es daher zunächst zu prüfen, ob der Empfänger über eigenes Schlüsselmaterial verfügt. Schlägt keine der Standard-

techniken an, sollte das Verfahren der Spontanverschlüsselung Anwendung finden. Diesbezüglich ist es wichtig, dass die E-Mails komplett ausgeliefert und nicht auf der Appliance zum Download zurückgehalten werden. Außerdem sollten sich alle E-Mails ohne zusätzliche Softwareinstallation im gewohnten E-Mail-Programm empfangen und nach der kurzen Eingabe eines Passwortes entschlüsseln lassen. Hinsichtlich der verschiedenen vorstellbaren Anwendungsszenarien ist hier eine Auswahl diverser Passwort-Optionen sinnvoll. Beispielsweise kann eine entsprechende Appliance ein Initialpasswort für den Absender erstellen, das dieser dem Empfänger über einen zweiten Übertragungsweg, etwa via Telefon, mitteilt. Alternativ ist die Funktion eines Einmalpasswortes denkbar, für das nicht mehr als die E-Mail-Adresse und die Handynummer des Absenders benötigt werden. Mittels dieser beiden Informationen lässt sich mit einer professionellen Lösung jede beliebige E-Mail seitens des Absenders verschlüsseln, und der Empfänger bekommt per SMS ein einmalig gültiges Kennwort zur Entschlüsselung. Durch die Nutzung des SMS-Passwortes kann die E-Mail problemlos abgerufen werden. Sofern ein Adressat nur selten oder einmalig eine vertrauliche Nachricht erhält, eignet sich ein E-Mail-Passwort, das einer spezifischen E-Mail zugeordnet ist. Dazu bedarf es keiner vorherigen Registrierung.

Fazit

Cyberkriminelle schrecken vor nichts zurück. Sie finden immer wieder neue Maschen, um Unternehmen hinters Licht zu führen, Schadsoftware zu platzieren und Datenklau zu betreiben. Nahezu ständig gibt es Warnhinweise zu neuen Phishing-Versuchen. So machen in der letzten Zeit etwa immer wieder Phishing-Mails mit Bezug zu COVID-19 die Runde. Kürzlich wurden zum Beispiel E-Mails in Umlauf gebracht, die gefälschte Antragsformulare für Corona-Überbrückungshilfen beinhalten. Um derartigen Angriffen nicht zum Opfer zu fallen, ist eine gute Vorsorge die halbe Miete. Mit der Einbindung einer adäquaten E-Mail-Sicherheits-Komplettlösung, bestehend aus Signatur, Verschlüsselung, Large-File-Transfer und Central-Disclaimer-Management, sind Unternehmen auf der sicheren Seite, was den Schutz des digitalen Postfaches betrifft. ■