HZ208307 · ISSN 1868-5757 · www.datakontext.com Februar 1/2021

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

Künstliche Intelligenz: Fair oder gefährlich?

Warum Ethik in der KI zum zentralen Thema wird

Schwerpunkt Cybersecurity:
Trends, E-Mail, Ransomware, Banking

Datenschutz:
Folgenabschätzung risikobehafteter Tools am Beispiel von Microsoft 365

Cloud-Forensik:
Blick in die großen „Verstecke“ von Cyberkriminellen

DATAKONTEXT

So wird das Top-Angriffsziel E-Mail zum Hacker-Flop

VORSORGE IST BESSER

Jeder kennt sie, jeder nutzt sie: die gute alte E-Mail. Als praktisches, einfaches und schnelles Kommunikationsmittel hat sie sich nicht nur im privaten Bereich, sondern vor allem im Geschäftsalltag seit vielen Jahren etabliert. Dies belegt auch eine Statista-Umfrage zur Nutzung von E-Mails, Mobile Messenger/SMS und sozialen Netzwerken für die Kommunikation nach Gesprächspartnern im Jahr 2020: Im Rahmen der Umfrage gaben 63,2 Prozent an, mit Unternehmen via E-Mail zu kommunizieren.(1) Das wissen natürlich auch Cyberkriminelle, die E-Mails gern nutzen, um sich Zugang zu Unternehmensnetzwerken zu verschaffen, Datendiebstahl zu betreiben oder Schadsoftware zu installieren. Aus diesem Grund sollten Firmen entsprechende Vorkehrungen treffen und ein umfassendes E-Mail-Security-Konzept etablieren.

ALS NACHSORGE

Moment, ich schicke die Infos eben kurz per Mail!“ Nahezu jeder hat diesen Satz bereits einmal gehört. Gerade dann, wenn es schnell gehen muss, versendet man häufig „mal eben“ eine E-Mail, beispielsweise an die Kollegen, Kunden oder Partner. Dies liegt nicht zuletzt daran, dass sich E-Mails besonders einfach übermitteln und archivieren lassen.

Bei all den Vorteilen, die der Versand von elektronischen Nachrichten bietet, ist allerdings zu beachten, dass unverschlüsselte E-Mails einer Postkarte gleichen und ohne großen Aufwand von Dritten mitgelesen werden können. Allein schon aus datenschutzrechtlichen Gründen ist dies äußerst bedenklich. Gemäß der Datenschutz-Grundverordnung (DS-GVO) gilt es, jegliche personenbezogene Inhalte in E-Mails zu verschlüsseln. Verstöße gegen diese Richtlinie können mit hohen Bußgeldern geahndet werden. Davon abgesehen sollte es auch unabhängig von der Gesetzgebung im Sinne jeder Firma sein, alle unternehmenskritischen Daten zu schützen. Geraten sie in die falschen Hände, kann dies einen immensen wirtschaftlichen Schaden nach sich ziehen, der im Worst Case den Ruin eines Unternehmens bedeutet. Als einem der Hauptangriffsziele für Cyberattacken sollten E-Mails also unbedingt durch professionelle Maßnahmen abgesichert werden. Denn wie auch in jedem anderen Lebensbereich ist Vorsorge immer besser als Nachsorge.

DIGITALE SIGNATUR ALS ECHTHEITSBEWEIS

Eine Unterschrift schafft Verbindlichkeit und Authentizität. Folglich müssen wichtige Papierdokumente immer persönlich unterzeichnet werden. Was für Dienst- oder Kaufverträge gilt, sollte auch bei E-Mails Anwendung finden. Der erste Schritt in Richtung E-Mail-Sicherheit liegt daher in der Einbindung einer digitalen Signatur. Ein ungebrochenes Siegel zeigt dem Empfänger, dass die erhaltene elektronische Nachricht tatsächlich vom angegebenen Absender stammt und auf dem Versandweg nicht verändert wurde. Auf diese Weise ist es möglich, „falsche“ E-Mails von „echten“ zu differenzieren und so das Phishing von Daten zu verhindern.

Zur digitalen Signatur von E-Mails wird ein Zertifikat benötigt, das sich bei einer akkreditierten Zertifizierungsstelle beantragen lässt. Diese sogenannten Certificate Authorithies (CAs) belegen dann, dass das Zertifikat, also der persönliche, öffentliche Schlüssel, zu einer bestimmten E-Mail-Adresse und Organisation gehört.

WAS EINE SECURE-E-MAIL-LÖSUNG MITBRINGEN SOLLTE:

- *sichere und DS-GVO-konforme Kommunikation*
- *hohe Benutzerfreundlichkeit und Transparenz*
- *einfache Administration*
- *automatisierter Betrieb im Hintergrund*
- *Konfiguration in wenigen Schritten*
- *kurze Einführungszeit*
- *keine Störung des laufenden Prozesses bei Implementierung*
- *kompatibel mit anderen Technologien und Anbietern*
- *im Standard-E-Mail-Client nutzbar und intuitiv bedienbar*
- *flexibel skalierbar im Hinblick auf Gesetzesänderungen*

Über eine Managed Public Key Infrastructure (MPKI) beziehen moderne Lösungen automatisch die erforderlichen Zertifikate, sobald der Nutzer die erste E-Mail versendet. Auf diese Weise werden der administrative Aufwand bei der Zertifikatsgenerierung überflüssig, und der gesamte PKI-Prozess deutlich beschleunigt. Da sämtliche gängigen E-Mail-Clients die Signaturprüfung unterstützen, braucht der Empfänger keine zusätzlichen Softwarekomponenten oder Tools und kann seine E-Mails wie gewohnt abrufen.

UNBEFUGTEN ZUGRIFF VERMEIDEN

Neben der Signatur spielt auch die Verschlüsselung eine zentrale Rolle in puncto lückenloser E-Mail-Security und Datenschutz. Damit Betrüger zu keinem Zeitpunkt dazu in der Lage sind, E-Mails mit sensiblen Inhalten abfangen und mitlesen zu können, sollten Unternehmen eine Verschlüsselungslösung etablieren. Entgegen der Auffassung von vielen Verantwortlichen ist dies nicht zwangsläufig mit großem Aufwand verbunden. Inzwischen gibt es benutzerfreundliche Gateways, die sich einfach implementieren und nahezu unbemerkt in den Arbeitsalltag integrieren lassen.

Wichtig im Hinblick auf eine geeignete Secure-E-Mail-Lösung ist, dass sie alle gängigen Verschlüsselungsverfahren, wie S/MIME, OpenPGP, TLS und Domainverschlüsselung, unterstützt. Darüber hinaus muss es auch dann möglich sein, E-Mails DS-GVO-konform zu übermitteln, wenn der Adressat selbst kein eigenes Schlüsselmaterial besitzt. Empfängerseits sollten dafür lediglich ein beliebiger E-Mail-Client, ein Internetzugang sowie ein Webbrowser zur kurzen Passworteingabe notwendig sein.

GANZHEITLICHER E-MAIL-SCHUTZ DURCH ALL-IN-ONE-LÖSUNG

Aufgrund ihrer Einfachheit und Nachvollziehbarkeit sind E-Mails aus dem geschäftlichen Umfeld nicht mehr wegzudenken. Unternehmen nutzen sie sowohl für die interne Zusammenarbeit im Team als auch für den externen Austausch mit Kunden oder Partnern. Gleichzeitig zählen sie jedoch als Hauptangriffsvektor schlechthin. Damit sich Hacker keinen Zugriff auf E-Mails verschaffen können und Phishing-Attacken ins Leere laufen, ist die Integration einer ganzheitlichen Gateway-Lösung sinnvoll. Wie bereits thematisiert, sollte diese die digitale Signatur und die Verschlüsselung elektronischer Nachrichten gestatten. Das i-Tüpfelchen für einen vollumfassenden E-Mail-Schutz ist außerdem die Möglichkeit, auch übergroße Dateien verschlüsselt versenden und empfangen zu können. So lässt sich verhindern, dass die Mitarbeiter auf unsichere, kostenfreie Filesharing-Plattformen zurückgreifen, die wiederum die Datensicherheit gefährden. Mit den entsprechenden Vorkehrungen haben Hacker also keine Chance, und das beliebte Kommunikationsmittel E-Mail kann bedenkenlos verwendet werden, um der täglichen Arbeit nachzugehen. ■

Quellen:

[1] *https://de.statista.com/statistik/daten/studie/783875/umfrage/nutzung-von-email-und-sozialen-netzwerken-zur-kommunikation-nach-gespraechspartner/*

GÜNTER ESCH,
Geschäftsführer der SEPPmail – Deutschland GmbH