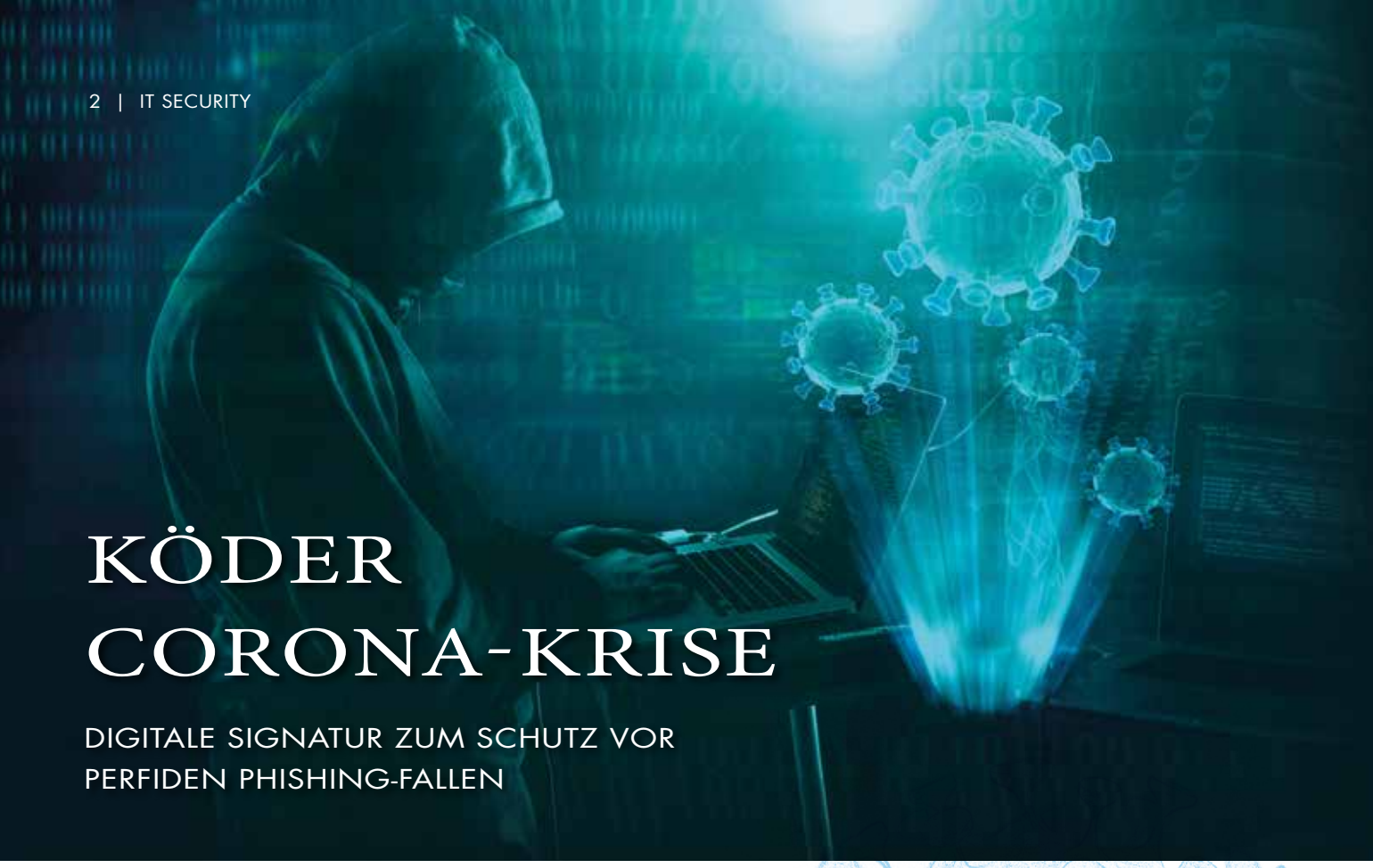

KÖDER CORONA-KRISE

DIGITALE SIGNATUR ZUM SCHUTZ VOR PERFIDEN PHISHING-FALLEN

Die Corona-Pandemie hat die Cybergefährdungslage nochmals verschärft. Sie kommt wie gerufen für Kriminelle, die Phishing-Mails mit Bezug zu COVID-19 versenden, um Lösegelder zu kassieren oder sensible Daten abzugreifen. Die Betrüger bringen E-Mails in Umlauf, in denen sie etwa Heilmittel versprechen oder Unterstützung bei der Beantragung von Finanzhilfen der Bundesregierung anbieten. In vielen Fällen sehen die Fake-Mails täuschend real aus und sind kaum von echten zu differenzieren. Nicht selten werden als Absender bekannte Dienstleister missbraucht, sodass die Wahrscheinlichkeit nochmals größer ist, der Falle im Posteingang auf den Leim zu gehen. Der Einsatz einer digitalen Signatur könnte dies verhindern.

Phishing ist eine äußerst heimtückische Methode, um Schutzbarrieren zu durchbrechen und sich so Zugriff auf Unternehmensnetzwerke zu verschaffen, Datendiebstahl zu betreiben oder Schadsoftware zu platzieren. Besonders kritisch wird es, wenn Betrüger aktuelle Themen wie das Coronavirus missbrauchen, die eine Vielzahl von Personen ansprechen. Stelle man sich einmal folgendes Beispiel vor: Die Mitarbeiter eines großen Energieversorgungskonzerns erhalten eine seriös aussehende E-Mail mit dem Hinweis, dass sie – als Teil eines KRITIS-Betriebes – früher als andere eine Corona-Impfung bekommen. Sie werden gebeten, für weitere Informationen auf einen Link oder Anhang zu klicken. Hoffnungsvoll öffnet ein Großteil der Mitarbeiter die Mail und interessiert sich für die angeblich weiterführenden Details. Und schon haben die Cyberkriminellen ihr Ziel erreicht.

Natürlich gibt es Checklisten, die dabei helfen sollen, nicht auf Phishing-Mails hereinzufallen. Doch gerade wenn E-Mails auf die Schnelle geöffnet werden oder Köder wie die Corona-Krise genutzt werden, hat man fix einen Link angeklickt, ohne sich Gedanken über die zu beachtenden Punkte zu machen. Um diese Gefahr zu umgehen beziehungsweise von Anfang an ausreichend vorzusorgen, gilt es entsprechende Sicherheitsmaßnahmen zu ergreifen. Dazu gehört vor allem die Einbindung einer digitalen Signatur. Denn ein ungebrochenes Siegel signalisiert dem Empfänger, dass die eingegangene E-Mail wirklich vom angegebenen Absender stammt und auf dem Versandweg nicht verändert wurde.

Digitales Unterzeichnen elektronischer Dokumente

Eine digitale Signatur zielt darauf ab, die Identität des Unterzeichners nachzuweisen und die Authentizität und Integrität der elektronischen Nachricht sicherzustellen. Damit E-Mails mit einer Signatur versehen werden können, bedarf es eines qualifizierten Zertifikats, das sich bei einer akkreditierten Zertifizierungsstelle beantragen lässt. Diese sogenannten Certificate Authorithies (CAs), darunter zum Beispiel SwissSign, DigiCert, D-TRUST oder Sectigo, belegen schließlich, dass das Zertifikat, also der persönliche, öffentliche Schlüssel, zu einer bestimmten Person gehört. Eine moderne Lösung erlaubt es, die benötigten Zertifikate über eine Managed Public Key Infrastructure (MPKI) bei der ersten ausgehenden E-Mail des Nutzers automatisch

durch die Appliance zu beziehen. Alternativ sollten sie sich manuell für den jeweiligen User importieren lassen. Für diesen Prozess müssen sämtliche erforderlichen Funktionalitäten wie die PKI, die Konnektoren zu den offiziellen CAs sowie die Zuweisungsmöglichkeiten der Zertifikate zu den Anwendern standardmäßig in der Lösung integriert sein. Alle gängigen E-Mail-Clients unterstützen die Signaturprüfung, sodass der Empfänger keine spezifischen Tools braucht. Insgesamt minimiert eine geeignete Lösung somit den administrativen Aufwand bei der Erstellung digitaler Signaturen und sorgt dafür, den gesamten PKI-Prozess zu beschleunigen. Zudem wird mit der Signatur der öffentliche Schlüssel des Absenders verbreitet, durch den jeder Empfänger potenziell in der Lage ist, eine verschlüsselte Rückantwort zu senden.

DURCH DIE VERMEHRTE IMPLEMENTIERUNG DIGITALER SIGNATUREN WÜRDEN VIEL WENIGER PHISHING-ATTACKEN ERFOLGREICH ABLAUFEN.

Günter Esch, Geschäftsführer, SEPPmail – Deutschland GmbH, www.seppmail.de

Lückenlose E-Mail-Sicherheit

Um auf Nummer sicher zu gehen und nicht nur Phishing, sondern die gesamte Palette an Angriffsmethoden via E-Mail zu verhindern, eignet sich eine professionelle All-in-One-Lösung. Diese sollte auch die E-Mail-Verschlüsselung beinhalten, da unverschlüsselte elektronische Nachrichten problemlos von Dritten abgefangen und mitgelesen werden können. Anders als von vielen erwartet, ist die Verschlüsselung von E-Mails nicht zwangsläufig mit großem Aufwand verbunden. Es gibt bereits Lösungen, die sich durch einen hohen Benutzerkomfort auszeichnen, den gewohnten Arbeitsprozess nicht unterbrechen und eine sichere Kommunikation mit jedermann ermöglichen. Zur Abdeckung der Signatur und der Verschlüsselung eignet sich die Nutzung eines Secure E-Mail Gateway, das beides beherrscht. Das Gateway sollte zusätzlich die Möglichkeit bieten, auch übergroße Dateien geschützt zu übermitteln, damit auf keine unsicheren, kostenfreien Filehosting-Dienste zurückgegriffen werden muss. Zu guter Letzt ist außerdem ein Central Disclaimer Management ratsam, das die E-Mails zentral mit Firmeninformationen ergänzt und das Komplettpaket so optimal abrundet.

Fazit

Zahlreiche Hacker nutzen die Ängste und Hoffnungen der Menschen hinsichtlich des Coronavirus schamlos aus. Sie locken Firmen mit Phishing-Mails und platzieren auf diese Weise Schadsoftware oder machen sich unternehmensrelevante Informationen zu eigen. Durch die vermehrte Implementierung digitaler Signaturen hingegen würden viel weniger Phishing-Attacken erfolgreich ablaufen. Versehen Unternehmen E-Mails mit einer Signatur, trägt dies sowohl zu einer gesteigerten Sicherheit als auch zu einem verbesserten Image bei. Zur Gewährleistung eines durchgängigen E-Mail-Security-Konzepts sollte auf eine Komplettlösung zurückgegriffen werden, die neben der Signatur auch die E-Mail-Verschlüsselung, den Large File Transfer und das Central Disclaimer Management unterstützt. Mit einer derartigen All-in-One-Lösung ist es nicht länger notwendig, die Mails vor dem Öffnen detailliert zu prüfen, denn man kann sich sicher sein: Sie sind in jeder Hinsicht vertrauenswürdig.

Günter Esch