Quishing – ein Phänomen gedeiht zwischen Impfselfies und Ausgangssperren

In der COVID-19-Pandemie fand ein totgeglaubter, schwarz-weiß karierter Kasten seinen Platz zwischen Impfselfies und Ausgangssperren: Der QR-Code. Einst kaum die routinierte Handbewegung zum Smartphone wert, etablierte er sich in den letzten Jahren zur Allzweckwaffe. Schnelltests, Warn-Apps, Impfzertifikate, Cocktailkarten, Bahntickets, kontaktlose Zahlungen oder um es auf dem Punkt zu bringen: die Eintrittskarte zur Normalität. Wo Licht ist, ist bekanntermaßen auch Schatten. Und so birgt die Anwendung ein angsteinflößendes Gefahrenpotenzial in sich.

Das verhängnisvolle QR-Comeback

QR-Code steht für „Quick Response Code“. Eine zweidimensionale Version des Barcodes, die scheinbar ganz selbstverständlich und organisch aus unserem Bedürfnis entstand, auf alles maximal schnell und einfach zugreifen zu wollen – alles nur einen Scan entfernt. Dabei können viele Informationen unmittel-

bar übertragen werden. Die einfache Handhabung und die Pandemie waren wie Brandbeschleuniger für neue Phishing-Kampagnen. Sogenanntes Quishing: eine Komposition aus „QR“ und „Phishing“.

Beim traditionellen Phishing fischen Cyberkriminelle mit zweifelhaften E-Mails, Instant-Messages oder Websites nach Passwörtern und anderen persönlichen Daten.

Beim Quishing machen sich Kriminelle die eingangs beschriebenen Eigenschaften des QR-Codes zunutze, um trügerische Informationen hinter dem Schachbrett ähnlichen Muster zu verstecken. Quishing E-Mails sind meist sorgfältig gestaltet, – ja fast schon mit Liebe zum Detail. Auf Authentizität getrimmt. Es ist in einschlägigen Kreisen scheinbar nicht mehr angesagt, potenzielle Opfer mit dem Erbe eines Vermögens von mehreren Millionen US-Dollar anzulocken. Auch wenn, besonders jetzt in der dunklen Jahreszeit, eine kurze Gedankenreise zur Traumsommerresidenz in Saint-Tropez so manche Empfänger:innen eine willkommene Abwechslung bereiten würde.

Moderne Cyberkriminelle gehen subtil vor. Sie greifen die Schwäche des menschlichen Geistes an. Die unerträgliche Selbstgeißelung, sich mit unliebsamen Dingen beschäftigen zu müssen. Sie drohen beispielsweise mit einer Kontosperrung ihrer Bank oder ihres Lieblingsonlineshops.

Kontaktlose Empfängnis mit Sündenfall

Handelsübliche Sicherheitsmechanismen durchleuchten nur gewöhnliche Anhänge und URLs. Doch diese Maßnahmen versagen meist bei QR-Codes. Besonders beliebt ist die Aufforderung, Änderungen in der Datenpolitik zuzustimmen oder neue Sicherheitsverfahren einzurichten. Alles bequem per QR-Code selbstverständlich. Auch wichtige Dokumente, welche sich mithilfe des QR-Codes einfach herunterladen lassen, befinden sich im kriminellen Werkzeugkasten.

Verständlicherweise möchten Empfänger:innen die unliebsame Melange aus vermeintlichem Handlungszwang und dem »ich möchte mich jetzt eigentlich viel lieber mit etwas anderem beschäftigen« -Gefühl, schleunigst beiseiteschaffen. Doch wer suhlt sich nicht gern in der scheinbaren Produktivität, wenn man noch schnell die lästig attribuierte »Banksache« erledigt. Rasch ist der Code gescannt – mit oftmals fatalen Folgen. Völlig anders als bei der heiligen Maria kann diese kontaktlose Empfängnis hier zur Sünde werden.

Lauernde Datenmuränen

Folgt man den trügerischen Aufforderungen, findet man sich auf gefälschten Websites wieder. Mühevoll dekoriert. Schließlich soll die Kopfzeile im gleichen Königsblau schimmern wie das kopierte Volksbank-Logo. Mit verschiedenen Techniken werden gefährliche Links verschleiert und Warnungen umgangen. Gängig sind Landingpages, auf denen Content-Management-Systeme wie WordPress samt Plugins missbraucht werden, um potenzielle Opfer in die Falle zu locken. Es wurde auch beobachtet, dass sich Cyberkriminelle an Googles Feed-Proxy-Dienst „FeedBurner“ für die Umleitung vergreifen. Ebenfalls gebräuchlich ist die eigene benutzerdefinierte Domain für die Umleitung als auch als endgültige Phishing-Seite. Das heißt: Gefahr besteht – auch wenn Abwehrsysteme keinen Alarm schlagen.

Einmal in der perfekten Illusion gelandet, geht es den Cyberkriminellen nur um eins: persönliche Daten. Wie eine Muräne in ihrer Höhle, darauf lauernd, Usernamen und Passwörter abzuschöpfen. Wenn dann noch der Feierabend oder der Sundowner auf der Terrasse wartet, werden viele Empfänger:innen leichtsinnig. Über das etwa zusätzliche L bei “vollksbank.de” wird hinweggesehen und prompt stehen die eigenen Daten in der täuschend echten Anmeldemaske. Phishing-URLs für Sparkassen beginnen häufig mit „spk-„, während ein „vr-„ das Volksbank-Imitat ziert.

Eine besondere Gefahr im beruflichen Umfeld besteht dann, wenn mit privaten Smartphones unternehmensinterne Sicherheitsstrukturen umgangen werden, wofür sich Quishing bestens eignet. Ist der gefährliche Code gescannt, finden schädliche Inhalte ihren heimlichen Weg auf mobile Endgeräte. Dort ist es nicht mehr weit zu E-Mail-Postfächern, Kontaktdaten oder Dokumenten, die über Cloud-Lösungen organisiert werden. Ein perfektes Einfallstor. Sind in so einem Fall kritische Daten betroffen, breitet sich das Feuer wahrscheinlich auch auf Firmenressourcen aus. Darunter ist zuletzt Ransomware durch das enorme Bedrohungspotenzial auffällig geworden. Ein unheilvoller Imperativ, der laut BSI noch um ein Vielfaches höher ausfällt, wenn Unternehmensnetzwerke betroffen sind.

Digitale Reginheris

Ransomware zielt auf die Verschlüsselung von Userdaten ab. Ist dieser Prozess erfolgreich abgeschlossen, folgt eine Lösegeldforderung. Die Fallhöhe von betroffenen Unternehmen ist enorm. IT- und Geschäftsprozesse kommen zum Erliegen. Oftmals folgen Drohungen, die verschlüsselten Daten zu veröffentlichen oder weiterzuverkaufen. Unternehmen aller Couleur sind im Visier. Laut dem von Hiscox veröffentlichten Cyber Readiness Report 2022 zahlen 48 % deutscher Unternehmen Lösegeld nach solch einer Attacke. Die Forderungen bewegen sich häufig im sechsstelligen Euro-Bereich, dem BSI sind aber auch achtstellige Lösegeldforderungen bekannt.

Zum Schreck vieler Opfer stellen Betrügende auch nach der Zahlung weitere Forderungen. Das wirkt beinahe so, als wären die Akteure aus einer einigermaßen spannenden Geschichtsdoku entsprungen. Wie im Jahr 845, als der Wikingeranführer Reginheri mit seinen Streitkräften Paris belagerte. Der westfränkische König Karl der Kahle hielt einen Kampf für aussichtslos und entrichtete 7000 Pfund Silber Lösegeld für den Abzug der dänischen Truppen. Ähnlich der Kollegschaft knapp 1200 Jahre später, konnten die Nordmänner und Schild-Maiden der Verlockung nicht widerstehen, nochmals Lösegeld zu erpressen. Also folgten weitere Überfälle.

Selbst wenn moderne Kriminelle keine geflochtenen Bärte oder geschulterte Äxte tragen, bleibt die Lage auch nach der Forderungserfüllung ernst. Egal ob man sich auf Erpressungen einlässt oder nicht, die Folgen für Privatpersonen, Unternehmen oder öffentliche Einrichtungen sind in den meisten Fällen gravierend. Quishing kann somit zu massiven Folgeschäden führen, wie Daten- und Reputationsverlust, DS-GVO-Verstöße oder finanzielle Schäden.

Wie schütze ich mich vor Quishing?

Weniger cineastisch aufgeladen als Wikingerüberfälle, aber mindestens genauso spannend ist die Frage: Wie schützt man sich vor Quishing?

„Scannen Sie im Zweifel keine QR-Codes“ – eine offensichtliche, aber gültige Aussage. Das Problem entsteht jedoch oft, weil erst gar kein Verdacht geschöpft wird. Cyberkriminelle nutzen tief sitzende menschliche Dispositionen und Bedürfnisse aus, um Personen geschickt zu manipulieren – sogenanntes Social Engineering. Hinzu kommt Unwissenheit. Schon ist er fertig, der katastrophale Cocktail. Das macht es schwer, sich zuverlässig dagegen zu schützen. Dennoch gibt es ein paar einfache Regeln, das Risiko zu minimieren:

- **Behandeln Sie QR-Codes wie Links.** QR-Codes auf Guerilla-Plakatkampagnen, Dokumenten oder in E-Mails sind nichts anderes als Links und bergen die gleiche Gefahr.
- **Geben Sie keine sensiblen Daten ein.** Seriöse Dienstleistende fordern Sie niemals per E-Mail auf, vertrauliche Zugangsdaten preiszugeben.
- Werfen Sie immer einen kritischen Blick auf die **E-Mail-Adresse** oder die **Adressleiste** im Browser, wenn Sie sich bereits auf einer fragwürdigen Seite befinden.
- Auch **E-Mail- und Website-Inhalte** sollten unter die Lupe genommen werden. Zum Schmunzeln bringende Tippfehler sind bei Cyberkriminellen aus der Zeit gefallen. Die meisten Texte sind gut formuliert. Dazu liefert das BSI einige Merkmale, bei denen Sie misstrauisch werden sollten, wenn mindestens eines zutrifft:

1. Dringender Handlungsbedarf
2. Drohungen von Konsequenzen bei Handlungsversäumnis
3. Forderung zur Eingabe von sensiblen Daten wie die PIN oder eine Kreditkartennummer
4. Die E-Mail enthält Links bzw. QR-Codes oder Formulare
5. Ungewöhnliches Anliegen einer bekannten Person oder Organisation

- Im Zweifel über einen offiziellen Kanal des genannten Angebots **nachfragen**.
- **Downloaden oder öffnen Sie niemals Dateien** in E-Mail-Anhängen oder Websites, dessen Echtheit nicht hundert Prozent klar ist.

Nutzen Sie **Zwei- oder Mehr-Faktor-Authentisierung**. Denn selbst wenn es Kriminellen gelingt, Daten in Erfahrung zu bringen, fehlt ihnen ein weiterer Faktor zum Einloggen.

Wie Teerlungen auf Zigarettenpackungen wirken Furchtappelle und vereinfachte Verhaltensregeln meist nur mäßig – oft nur ein paar Tage. Informationssicherheit muss Teil der Unternehmensphilosophie werden. Der wichtigste Tipp ist daher, die permanente Weiterbildung und das Awareness-Niveau in Ihrem Unternehmen zu fördern. Hierfür bieten wir Ihnen unseren Informationssicherheitskurs an, in dem Sie und Ihre Mitarbeiter:innen umfangreich über die verschiedenen Risiken von kriminellen Online-Angriffen informiert werden. Am Ende bleibt es dabei: Unwissenheit bei Ihren Angestellten ist immer noch die größte Angriffsfläche für diverse Cyberattacken.

Autor: Tom Carvalho