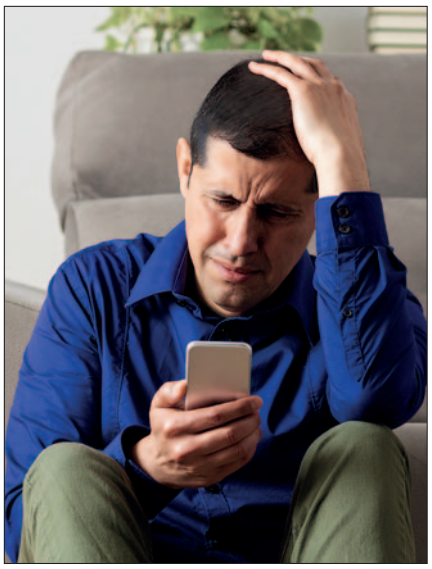
# Phishing: Falsches Vertrauen

**Durch Fälschen, Irreführen und Betrügen gelingt es Kriminellen, ihre Opfer beim Phishing zu unüberlegten Handlungen zu verleiten. Der Phishing-Activity-Trends-Report vom dritten Quartal 2022 belegt weltweit eine Zunahme der Zahl an Phishing-Attacken im Vergleich mit 2020.**

Montagmorgen: Max beginnt neben einem Kaffee in seinem Büro seine E-Mails zu bearbeiten, die über das Wochenende in seinem Posteingang gelandet sind. Es klingelt auch das Telefon unaufhörlich. Dadurch abgelenkt, öffnet er eine E-Mail, die auf den ersten flüchtigen Blick von der Wirtschaftskammer stammen dürfte. Darin wird er aufgefordert, die Daten seines Unternehmens zu aktualisieren, wenn er weiterhin in ihrer Datenbank gelistet werden möchte. Wenn er dies bis zu einem bestimmten Datum in nicht allzu ferner Zukunft versäume, würde seine Firma deaktiviert und als dauerhaft inaktiv markiert werden. In der Hektik des Montagmorgens klickt er auf den Link und gib die geforderten Daten ein. Erst nach dem Absenden und genauerer Betrachtung der E-Mail dämmerte ihm, dass sie nicht von der Wirtschaftskammer stammen kann. Max wurde durch Unachtsamkeit Opfer eines Phishing-Angriffs.

**Phishing** ist ein Beispiel für Social Engineering, bei dem Kriminelle durch das Vermitteln von Dringlichkeit die Nutzer verunsichern und zu unüberlegten Handlungen verleiten. Ganz gleich, ob sich eine Phishing-Kampagne gegen eine einzelne Person oder eine breite Masse richtet, zu Beginn steht immer



**Vorsicht vor angeblichen Links oder Anhängen der Hausbank oder Firmen**

eine betrügerische Nachricht. Täter geben sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner aus, um an die persönlichen Daten eines Internetnutzers zu gelangen, wie Kontodaten oder Kreditkartennummern. Oder sie verleiten ihn zur Ausführung eines Schadprogramms durch Anklicken eines fingierten Links. Kontoplünderungen, Identitätsdiebstahl oder das Installieren einer Schadsoftware können die Folge sein.

**Social Engineering.** Bereits lange bevor es E-Mails und Internet im Alltag der Menschen gab, versuchten Betrüger mit Hilfe von Social Engineering via Telefonanrufen das Vertrauen ihrer Opfer zu erschleichen und so an vertrauliche Informationen zu gelangen. Ab den 2000er-Jahren hatten es die Betrüger zunehmend auf Bankkontos abgesehen. Die Phishing-Mails enthielten einen Link, der zu einer gefälschten Bank-Webseite führte. Hierfür verwendeten die Betrüger eine ähnliche Variation der Original-Domain und täuschten dadurch ihre Opfer.

Neu an der Vorgehensweise ist, dass es immer öfter zu Betrugsversuchen mit Schadsoftware („Malware“) kommt. Das sind in der Regel Phishing-Mails mit einem Anhang, der, sofern man ihn öffnet, Schadsoftware auf dem PC, Smartphone oder Tablet installiert. Falls es sich dabei um „Ransomware“ handelt, sperrt diese Software den Zugang zu allen Daten im System und gibt ihn erst nach Zahlung eines Lösegelds frei (oder auch nicht).

**Stress erzeugen.** Das Erzeugen von Stress und eines Gefühls der Dringlichkeit steht im Vordergrund. Der Betreff einer E-Mail entscheidet zunächst, ob sie geöffnet wird, oder nicht. Bereits in der Betreffzeile wollen die Kriminellen

## PRÄVENTIONSTIPPS

### Phishingversuche erkennen

- Der Text in der E-Mail gibt dringenden Handlungsbedarf vor, wie „Damit Sie auch weiterhin unsere Onlinedienste nutzen können, bitten wir Sie, Ihre Daten über den angeführten Link zu aktualisieren“.
- Konsequenzen werden angedroht: „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren.“
- Sie werden zur Eingabe von vertraulichen Daten aufgefordert, wie etwa den PIN für Ihren Online-Banking-Zugang oder eine Kreditkartennummer.
- Die E-Mail enthält Links oder Formulare, die Sie ausfüllen sollen.
- Die E-Mail scheint von einer bekannten Person oder Unternehmen zu stammen, jedoch kommt Ihnen das Anliegen des Absenders ungewöhnlich vor.
- Die Anrede in der E-Mail ist unpersönlich: „Sehr geehrter Kunde“, „Sehr geehrter Nutzer“.
- Kein seriöses Unternehmen oder Bankinstitut fordert per E-Mail zur Eingabe persönlicher Daten, wie Passwörter und dergleichen auf.
- Generell sollten Sie jeden Link in E-Mails oder sozialen Netzwerken vor dem Aufruf sorgsam prüfen. Wenn eine Internetadresse zwar den Namen der Institution trägt, aber ungewöhnliche Zahlen oder Zeichen enthält, ist Vorsicht geboten.
- Wenn Sie nach einer TAN gefragt werden, ohne jedoch eine Transaktion getätigt zu haben, handelt es sich um eine Phishing-Seite.
- Seien Sie misstrauisch, wenn Sie nach der Anmeldung etwa bei Ihrer Bank aufgefordert werden, bekannte Daten wie Name, Adresse oder IBAN neuerlich einzugeben. Es handelt sich wohl um eine gefälschte Seite.

Wichtigkeit vermitteln oder Besorgnis erregen. So geben die Täter häufig vor, dass der Account des Nutzers gesperrt werde, wenn er seine Daten nicht innerhalb kurzer Zeit aktualisiere. Aufgrund des dadurch erzeugten Stresses können Warnsignale übersehen und Vorwissen zum Thema Phishing vergessen werden. Da die E-Mails an viele Personen gleichzeitig versendet werden, ist die Anrede üblicherweise allgemein gehalten, wie etwa „Sehr geehrte Damen und Herren“ oder „Sehr geehrter Nutzer“. Damit die Täter an die gewünschten Informationen gelangen, können Phishing-Mails entweder schädliche Weblinks, schädliche Anhänge oder Dateneingabeformulare enthalten.

**Verschiedene Arten, aber ein Ziel.** Es gibt unterschiedliche Arten von Phishing-Angriffen, doch das Ziel, Daten oder Profit zu lukrieren, eint sie: E-Mail-Phishing, CEO-Betrug, Malware, Smishing, Pharming oder auch Angler-Phishing sind nur einige der gängigen Varianten. Es steht nicht immer nur das wahllose Versenden an die Masse im Vordergrund, sondern es kann auch zielgerichtet geschehen, wie etwa beim CEO-Betrug oder dem sogenannten Spear-Phishing. Hierbei gehen Nachrichten nur an bestimmte Personen innerhalb einer Organisation.

**Katalysator Homeoffice.** Die Covid-19-Pandemie hat besonders den Arbeitsalltag vieler verändert. Nachdem Homeoffice schnell flächendeckend zur Anwendung kam und sich die Arbeitsumgebung daher in die eigenen vier Wände verlegte, verschaffte das Angreifern einen Vorteil, da die Sicherheitsmaßnahmen zu Hause oft nicht mit denen im Büro vergleichbar waren. Da Mitarbeiter häufig nur ungenügend sensibilisiert waren und ihre private Geräte


**Smishing: In SMS-Textnachrichten wird man dazu verleitet, auf einen Link zu klicken oder Malware zu laden**

zu Arbeitszwecken nutzten, bot sich Kriminellen eine Angriffsfläche. Durch den Fernzugriff, den der Mitarbeiter auf die Unternehmensserver benötigt, kann der Täter jeden beliebigen Remote-Angestellten ins Visier nehmen, um sich Zugang zur internen Unternehmensstruktur zu verschaffen.

**Die Zahl an Phishing-E-Mails nimmt weltweit zu.** Da auch die Gestaltung der gefälschten E-Mails und Webseiten zunehmend professioneller wird und offensichtliche Merkmale, wie etwa Tippfehler oder schlechtes Deutsch, wegfallen, sind viele auf den ersten Blick nicht mehr als Fälschung erkennbar.

Laut dem *Phishing-Activity-Trends-Report, 3rd Quarter 2022* der internationalen *Anti-Phishing-Working-Group (APWG)* erreichte die Anzahl der Phishing-E-Mails im dritten Quartal 2022 einen neuen Höhepunkt: Waren es im ersten Quartal noch 1,025.968 Phishing-Attacken, registrierte die Organisation im zweiten Quartal 1.097.811 und im dritten Quartal 1.270.883. Im August 2022 wurden 430.141 Attacken registriert, was den höchsten Monatswert seit Beginn der Aufzeichnungen darstellt. So hat sich die Zahl der gemeldeten Phishing-Angriffe, die der *APWG* gemeldet wurden, seit dem ersten Quartal 2020 mehr als verfünffacht.

**Schutz vor Phishing.** Um Phishing einzudämmen, braucht es eine Weiterbildung und Sensibilisierung der Nutzer, um Warnsignale erkennen zu können sowie robuste Cybersicherheitssysteme. E-Mail-Filter können ein hilfreiches Tool sein, aber die Schulung der Mitarbeiter ist essenziell, da es immer wieder zu falsch-negativ Einordnungen der Filter kommt. Anti-Phishing-Sicherheitslösungen, die mit Hilfe künstlicher Intelligenz eingehende E-Mails scannen, verdächtige Nachrichten erkennen und automatisch in Quarantäne verschieben, können eine weitere gute Sicherheitsmaßnahme darstellen. Regelmäßige Änderungen der Passwörter und Updates der Soft- und Firmware sowie Firewalls erhöhen die Sicherheit zusätzlich.

**Phishing-Simulationen.** *Watchlist Internet (www.watchlist-internet.at),* eine Informationsplattform zum Thema Internetbetrug, erklärt, wie man Phishing-Simulationen als effektives Schulungstool einsetzt. Bei Phishing-Simulationen lernen die Mitarbeiter, wie sie Phishing-Angriffe, Malware, Ransomware, Spyware und andere potenzielle Bedrohungen für die Sicherheit von Unternehmensdaten erkennen, vermeiden und melden.

Phishing-Simulationen zählen zum Standardprodukt, wenn es darum geht, Cyber-Sicherheit in einem Unternehmen umzusetzen. Doch oft werden solche Simulationen als Kontrollwerkzeug und weniger als Schulungsmaßnahme wahrgenommen. *Romana Tofan*

## PHISHING

### Was tun bei einem Schaden?

- Wenn Sie Opfer von Cyber-Kriminalität geworden sind, zeigen Sie das bei der Polizei an.
- Dokumentieren Sie Zahlungs- und Kontoinformationen der Anbieter.
- Beobachten Sie die Bewegungen auf Ihrem Konto und informieren Sie Ihre Bank über allfällige unautorisierte Abbuchungen.
- Ändern Sie Zugangsdaten und Passwörter, wenn Sie sie bekannt gegeben haben.
- Bei Betrugsverdacht können Sie die Meldestelle für Cybercrime des Bundeskriminalamtes unter *against-cybercrime@bmi.gv.at* kontaktieren.
- Wenn Ihr Unternehmen von einer Cyber-Attacke, Ransomware oder Verschlüsselungstrojanern betroffen ist, können Sie sich an die Cyber-Security-Hotline der Wirtschaftskammer Österreich unter 0800 888 133 wenden.
- Weitere Informationen und Hinweise finden Sie auf der Plattform *JuraForum.de* unter *www.juraforum.de/lexikon/phishing*. Hier erfahren Sie unter anderem wie Sie sich vor Phishing-Angriffen schützten, wie Sie solche E-Mails erkennen, was zu tun ist, wenn Sie einer Attacke zum Opfer gefallen sind und wer für den Schaden haftet.

FOTO: SIEGBERT LATTACHER