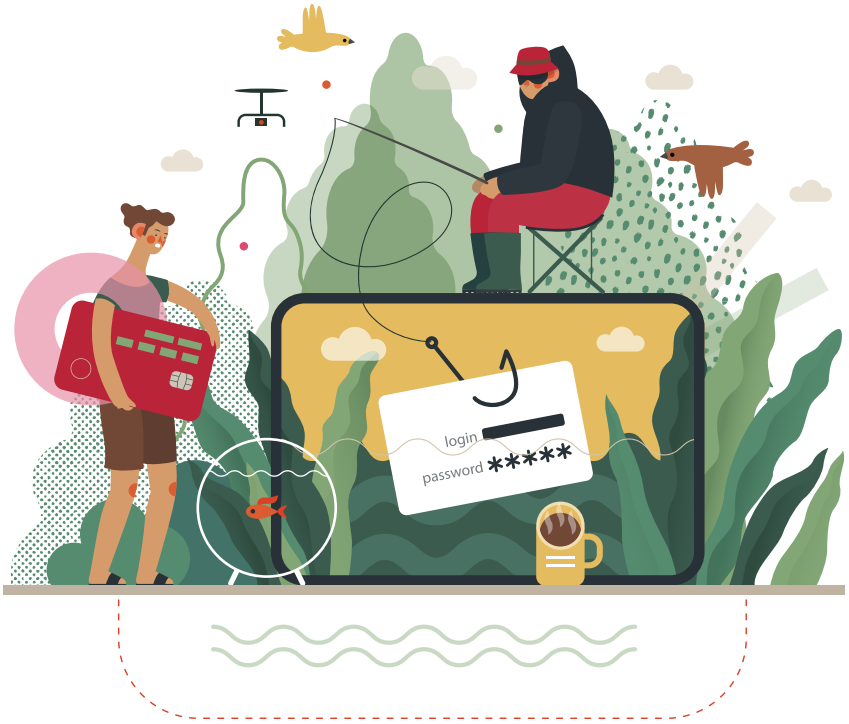

Phishing: Mit Phishing-Mails (von *fishing*, engl. für *„Angeln“*) versuchen Kriminelle immer wieder an die Passwörter der Empfänger zu gelangen.

Faktor Mensch in der IT-Sicherheit – Teil 1: Phishing, Malware & Co. – sicherer Umgang mit E-Mails

Sicherheitsbewusstsein als essentielle Ergänzung zu technischen Schutzmaßnahmen

Firewalls, Anti-Virus-Lösungen, Intrusion Detection- und Prevention Systeme sowie Backups und regelmäßiges Testing der Datenwiederherstellung sind technische Basis und unverzichtbar zum Schutz vor den tagtäglichen Bedrohungen aus dem Internet.

Der Faktor Mensch, also die Rolle der eigenen Mitarbeiter im Gefahrenszenario, darf jedoch nicht außer Acht gelassen werden. Eine aktuelle Studie* zur Lage der IT-Sicherheit zeigt: Irrtum und Nachlässigkeit eigener Mitarbeiter sind Hauptursache für Schäden in deutschen Unternehmen. Entsprechend sind die häufigsten Ursachen für Datenlecks sogenanntes Social-Engineering, Phishing und Unachtsamkeit. Unter den Infektionswegen für Schadsoftware (Malware) haben E-Mails den Spitzenplatz inne.

Eine Sensibilisierung der Mitarbeiter für die Gefahren aus dem Cyberspace, also die Schaffung sogenannter Security Awareness, ist somit unerlässlich. Privatanwender sind ebenso betroffen.

Unsere Artikel-Serie soll diesen Aspekt der IT-Sicherheit daher besonders beleuchten. In Teil 1 beschäftigen wir uns mit dem sicheren Umgang mit E-Mails:

Malware, gefährliche Anhänge, gefälschte Links – wie schütze ich mich?

E-Mails sind Einfallstor Nummer eins für Viren, Trojaner und andere Schadsoftware. Sie verstecken sich in Dateianhängen oder hinter einem Link und können massiven Schaden anrichten: Angefangen von der allmählichen oder schlagartigen Löschung von Daten über das meist unbemerkte Ausspähen und Versenden von Passwörtern bis zur vollständigen Verschlüsselung aller Daten, einschließlich Lösegeldforderung für deren Freigabe, durch sogenannte Ransomware (Erpressungstrojaner).

Antivirenprogramme vereiteln das Ausführen infizierter Dateien und mitunter untersuchen und blockieren sie entsprechende E-Mails schon beim Empfang, also noch bevor diese in Ihrem Postfach landen. Aber neue Varianten von Schadsoftware erscheinen quasi im Stundentakt. Es ist daher nur schwer möglich Antivirus-Programme immer topaktuell zu halten. Hier ist deshalb auch der gesunde Menschenverstand gefragt!

Der bloße Erhalt einer solchen E-Mail hat noch keine Folgen. Erst durch Öffnen des Anhangs bzw. Anklicken des betreffenden Links wird das Schadprogramm ausgeführt. Grundsatz Nummer 1 lautet daher, niemals Dateianhänge oder Links unbekannter Absender zu öffnen. Aber auch E-Mail-Anhängen bekannter Absender kann nicht bedenkenlos vertraut werden. Viren und Würmer durchsuchen einen befallenen PC nach E-Mail-Adressen und versenden sich selbst an diese weiter unter der Absenderadresse des eigentlichen Nutzers. So können auch E-Mails, die vermeintlich von Kollegen,

*<kes>/Microsoft-Sicherheitsstudie 2018, Ergebnisse zum Download unter: **www.infoserve.de/it-sicherheit-lagebericht-2018**

Seien Sie aufmerksam im Umgang mit E-Mails: Gefälschte Bestellbestätigungen namhafter Anbieter sind immer häufiger im Umlauf und verleiten dazu Kriminellen unwissentlich Tür und Tor zu Ihren persönlichen Daten zu öffnen.

Geschäftspartnern oder Freunden stammen, Schadsoftware enthalten. Sollten Sie keinen Dateianhang angefordert haben, vergewissern Sie sich also beim Absender, dass die Nachricht tatsächlich von ihm stammt.

Der Medienbruch nimmt zwar der E-Mail einen Teil ihrer Effizienz und Direktheit; ein kurzer Anruf ist aber immer noch besser, als aufwendig den PC entwanzen zu müssen.

Unternehmen können sich, um den internen E-Mail-Verkehr diesbezüglich abzusichern, sogenannter Authentifizierungstools bedienen. Diese verhindern, dass sich externe Mail-Absender als interne tarnen können.

Phishing – Angeln nach Passwörtern.

Nicht nur Malware stellt eine Bedrohung per E-Mail dar. Mit Phishing-Mails (von fishing, engl. für „Angeln") versuchen Kriminelle immer wieder an die Passwörter der Empfänger zu gelangen. Dabei handelt es sich inzwischen längst nicht mehr um leicht erkennbare, da dilettantische Nachrichten mit zahlreichen Rechtschreibfehlern, in denen man beispielsweise aufgefordert wird zum Datenabgleich sein Online-Banking-Passwort mitzuteilen. Phishing-Mails werden immer professioneller und sind auf den ersten Blick meist nicht als solche zu erkennen.

Dazu werden oftmals Bestellbestätigungen oder Rechnungen namhafter Online-Versandhäuser oder Telekommunikationsanbieter bis ins Detail gefälscht; inklusive der Absender-Adresse. Der Empfänger glaubt tatsächlich eine Nachricht von beispielsweise amazon, ebay oder Vodafone erhalten zu haben. Über Links zum vermeintlichen Rechnungsdownload oder zu Bestelldetails wird er auf ebenfalls gefälschte, aber täuschend echt aussehende, Anmelde-Seiten weitergeleitet, wo dann die Login-Daten des Users abgegriffen werden.

Hier wird sich einmal der Name eines seriösen Anbieters zunutze gemacht, um Vertrauen zu generieren und gleichzeitig wird die menschliche Neugier geweckt und der Nutzer damit zu Unvorsichtigkeit verleitet. Denn wenn man eine Bestell- oder Versandbestätigung erhält, ohne etwas bestellt zu haben, wird man zwar zunächst einmal stutzig; aber der (gefälscht) seriöse Absender und die echt aussehende Mail lassen einen unter Umständen doch an sich selbst zweifeln und der Link zu den angeblichen Bestelldetails wird angeklickt.

Um dieser Falle zu entgehen, sollten Sie zunächst die Links in der E-Mail auf ihre Validität prüfen, indem Sie den Mauszeiger darüber bewegen und sich so die tatsächliche Ziel-URL anzeigen lassen. Hat diese nichts mit dem vorgeblichen Absender der Mail zu tun, handelt es sich ziemlich sicher um einen Phishing-Versuch.

Links in der E-Mail auf ihre Validität prüfen: Indem Sie den Mauszeiger darüber bewegen, lassen Sie die tatsächliche Ziel-URL anzeigen.

Bleibt dennoch eine gewisse Unsicherheit zurück, folgen Sie nicht den Links in der Mail, um die angebliche Bestellung zu überprüfen, sondern geben Sie die Web-Adresse des Anbieters direkt in den Browser ein, um sich in Ihren Account einzuloggen. Sollten Sie doch eine vergessene Bestellung getätigt haben oder eine Rechnung zum Download vorliegen, wird Ihnen dies dort angezeigt.

Diese Regeln zum Erkennen von und dem Umgang mit Phishing-Mails bzw. Mails mit Schadsoftware sind nicht abschließend. Prinzipiell gilt: Vorsicht ist die Mutter der Porzellankiste! Machen Sie sich die Gefahren im E-Mail-Verkehr bewusst und sensibilisieren Sie Ihre Freunde, Kollegen und Mitarbeiter.

Eine kleine Anregung für Geschäftsführer oder Abteilungsleiter zur Stärkung des Sicherheitsbewusstseins der Mitarbeiter: Küren Sie doch jeden Monat die dreisteste Phishing Mail, die ein Mitarbeiter erhalten und entlarvt hat und verleihen Sie kleine Preise dafür. So sorgen Sie dafür, dass Ihre Mitarbeiter immer aufmerksam bleiben gegenüber den Bedrohungen, und sich das Thema IT-Sicherheit bei ihnen verankert.

Sie möchten noch mehr für die IT-Sicherheit in Ihrem Unternehmen tun? INFOSERVE berät Sie zu technischen und organisatorischen Maßnahmen. Wir stellen Ihr Unternehmen mit einem umfassenden IT-Sicherheitskonzept von der Analyse der Ist-Situation über die Bereitstellung der entsprechenden Sicherheitsinfrastruktur bis zur Awareness-Schulung Ihrer Mitarbeiter auf sichere Füße. ■