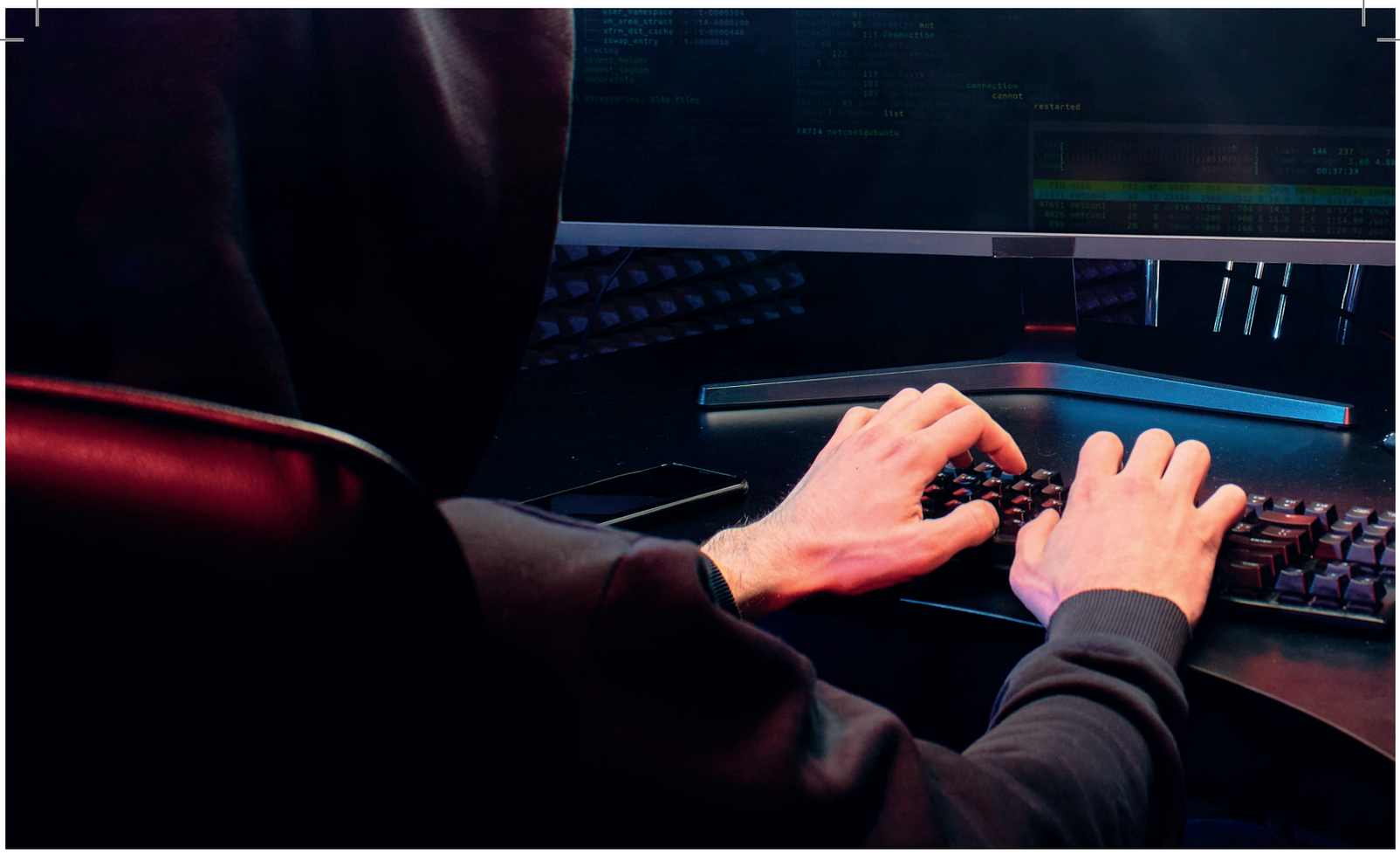


Social Engineering
Phishing als aktuelle und zunehmende Gefahr

Die Nachrichten über Phishing-Attacken sind zu einem ständigen Begleiter geworden. Beinahe jede Woche liest man neue Meldungen über E-Mail-Aufforderungen, seine Bank-, Paypal-, E-Mail- oder sonstige persönliche Angaben preiszugeben. Ein Klick auf den beiliegenden Link genügt und ein Formular ermöglicht die einfache Eingabe dieser Daten.

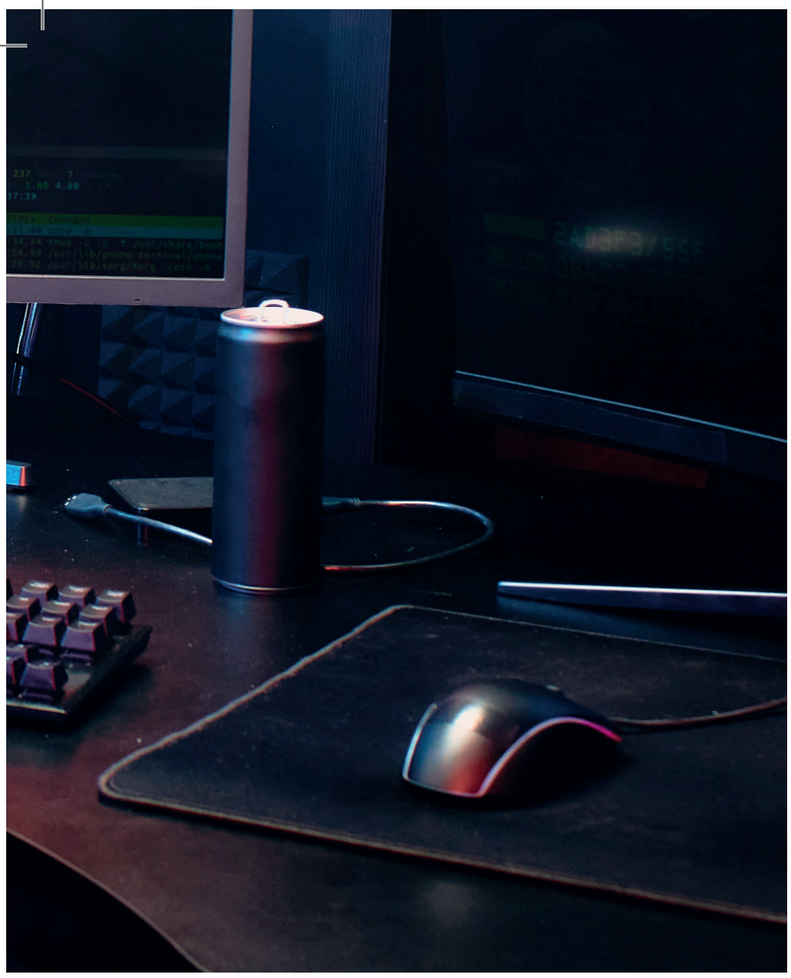
Im Juni 2005 wurde zum ersten Mal ein Schweizer Finanzinstitut Ziel einer Phishing-Attacke. Ein auf Englisch formuliertes E-Mail forderte PostFinance-Benutzer auf, die Login-Daten sowie die nächsten drei unbenutzten Streichlistennummern (TAN) zur Daten-Kontrolle einzugeben. Der in der E-Mail enthaltene Link führte zu einer perfekt nachgebildeten Internetseite in Russland.

Eigentlich sollten in einem solchen Fall die Alarmglocken läuten, doch trotzdem folgten rund ein Dutzend Kunden diesem Aufruf. Blitzschnell wurden die Konten leer geräumt. Zum guten Glück der Geprellten übernahm die PostFinance dazumal kulant den Schaden.

In der Zwischenzeit hat die Gefahr von Phishing-Attacken stark zugenommen und wird auch in Zukunft zu einem ständigen, ärgerlichen Begleiter. Jedoch sind es längst nicht mehr nur plumpe Versuche via E-Mail, sondern es werden ausgefeiltere Methoden verwendet. Zum Beispiel in Kombination mit trojanischen Pferden, oft irrtümlich als Trojaner bezeichnet, die jede Tastatureingabe aufzeichnen und augenblicklich weitermelden. Auch besteht die Gefahr, dass ein korrekter Aufruf einer Webseite unbemerkt auf einen anderen Server umgeleitetet wird. Diese Technik wird schon von einigen Viren ausgenutzt und verhindert gleichzeitig das Aufrufen bekannter Antivirenhersteller-Homepages.

Der Teufel liegt im Detail

Wenn eine E-Mail vom Chef kommt, dann muss schnell reagiert werden. Oft so schnell, wie wenn der Chef neben einem stehen würde. Genau dies macht sich ein Angreifer zunutze. Die Autorität des Vorgesetzten, kombiniert mit einem E-Mail, aus welchem Zeitdruck hervorgeht, ist eine perfekte Falle. Vermutlich ist dies jedem schon mal passiert, dass er in diesem Fall zu schnell gedrückt hat. Durch eine saubere Vorbereitung weiss der Hacker zudem genau, wie die Hierarchie in der Firma aussieht. Das Organigramm auf der Firmen-Homepage oder die Einträge auf Xing/Linkedin helfen dabei weiter.



Nehmen wir an, Sie erhalten eine Nachricht Ihres Chefs. In unserem Beispiel wäre das Herr Max Mustermann von der Firma Login-Check. Die offizielle Webseite ist unter https://www.login-check.com erreichbar.

Mittwoch, 11. August 2021, 08:34 Uhr
max.mustermann@login-check.com
Überweisung

Mittwoch, 11. August 2021, 08:34 Uhr
max.mustermann@login-check.net
Überweisung

Erkennen Sie den Unterschied? Nur schon ein Buchstabe ausgewechselt, bei unserem Beispiel sind es drei, und schon ist der Absender ein vollkommen Anderer. Deshalb ist genaues Hinschauen so wichtig. Auf Smartphones ist es noch schwieriger den Unterschied zu erkennen. Dort wird auf den ersten Blick nur angezeigt, was der Angreifer Sie sehen lassen will: Name und Betreff. Erst ein Klick auf «View Details» zeigt, um welche Adresse es sich wirklich handelt.

Inhalt

Der Inhalt bietet ebenfalls ein wichtiges Indiz. Wenn der interne Ablauf für eine Zahlung klar geregelt ist und plötzlich Ihr Chef via E-Mail verlangt, eine grosse Summe zu übeweisen, ist das verdächtig. Mit Details sind Formulierungen, Schreibstiel und Grussworte gemeint. Wenn zum Beispiel der Lieferant immer mit «Gruss Max» das E-Mail beendet und nun steht «Freundliche Grüße Max». Das sind Details, welche von jemanden, der noch nie E-Mails von dieser Person erhalten hat, nicht erkennen kann. Aber wenn Sie die andere Person kennen, bekommen Sie ein seltsames Gefühl, da stimmt doch etwas nicht. Und auf dieses Gefühl sollte gehört werden. Es bewahrt möglicherweise vor grossem Schaden.

Formatierung

Vielleicht haben Sie eine besondere Schriftart, die Sie mögen (oder von Ihrem Unternehmen vorgegeben wird) und für Ihre E-Mails verwenden. Auch dies ist wiederum ein Detail, die eine Person oder ein Unternehmen ausmachen. Es gibt wenig Gründe weshalb die Schriftart sich plötzlich verändert. Sieht das E-Mail anders aus, ist wiederum Vorsicht angezeigt.

Technisch

Aber was, wenn man sich wirklich nicht sicher sein kann. Was, wenn alle oben erwähnten Tests positiv, im Sinne der Gültigkeit, ausfallen und im empfangenen E-Mail ein Link oder eine Datei vorhanden ist? Dazu gibt es einige Tricks, welche Sie anwenden können. Anhänge sind immer ein heikles Thema. Am sichersten wäre es, wenn gar keine Dateien, welche Sie über ein E-Mail erhalten haben, geöffnet werden. Denn mittlerweile wurde schon in vielen Arten von Dateien Viren entdeckt. Aber das ist im Geschäftlichen wie im Privaten keine akzeptable Lösung. Die Einschränkung ist zu gross. Somit muss von Dateityp zu Dateityp unterschieden werden. Dabei gilt, lieber ein PDF als ein Word-Dokument. Aber auch hier gilt: der PDF-Reader muss aktuell sein. Oder besser noch, ein «dummes» PDF-Programm, das PDFs anzeigt, aber keinen Code ausführt.

Was viele nicht wissen, auch in einfachen Bildern ist es möglich Viren zu verstecken. Hier gilt wiederum: Bild anzeigen Ja, Code ausführen Nein. Ganz klare Tabus sind Office-Dateien mit Makros, welche mit den Endungen .xlsm,. xltm, .docm usw. erkannt werden können.

Bei Interviews während eines Audits zeigt sich oft die Tendenz, dass Links in E-Mails kritisch betrachtet werden. In vielen Fällen werden solche E-Mails sofort gelöscht. Es gibt einen einfachen Weg, den Zielort des Links zu überprüfen. Die Funktion heisst «Mouse-Over». Einfach mit der Maus über den Link fahren und wenige Augenblicke später erscheint ein kleines Fenster, in welchem die wirkliche Ziel-Adresse angezeigt wird. Falls das E-Mail-Programm dies nicht kann, gibt es immer noch die Möglichkeit, einen Rechtsklick auf den Link auszuführen und dann die Link-Adresse zu kopieren.

Auch hier ist uns die dunkle Seite des Netzes aber wieder einen Schritt voraus. In seltenen Fällen verwenden Hacker andere Alphabete mit denselben Buchstaben (zum Beispiel das russische Alphabet). Somit sieht der Link im Vorschau-Fenster richtig aus, jedoch werden andere Server im Internet aufgerufen. Deshalb ist es am sichersten, wenn der Link manuell in der Browser-Adresszeile eingegeben wird.

Fragen

Eine persönliche Rückfrage ist immer noch die beste Methode, um die Echtheit einer E-Mail zu prüfen. Aber auch hier gibt es «do's and dont's». Niemals darf für die Überprüfung auf die E-Mail geantwortet werden. Denn wenn der Angreifer alles richtig gemacht hat, bekommt er diese Antwort und teilt Ihnen mit, dass alles in Ordnung ist. Am besten wird zum Telefon gegriffen. Falls es doch ein E-Mail sein muss, sollte ein neues erstellt werden und die E-Mail-Adresse des Empfängers manuell eingetragen werden. Nutzen Sie dazu auch nicht die Auto-Vervollständigung des E-Mail-Programms. Evtl. wird hier schon die manipulierte Adresse angezeigt.

Gesunder Menschenverstand und aktuelle Systeme bewahren Sie auch in Zukunft zuverlässig vor Missbrauch und Manipulation.

Merkpunkte:

- **Lieber einmal zu viel nachfragen. Wer schon einmal eine Verschlüsslungs-Malware (Ransomware) auf dem Computer hatte, weiss wie zeitintensiv es ist, diese wieder zu entfernen.**
- **E-Mail-Adresse oder Links von Hand eingeben. Denn beim Kopieren werden alle Teile mitgenommen, welche eventuell nicht gewünscht sind.**
- **Es kommt auf die Details an. Schauen Sie immer die komplette E-Mail-Adresse genau an.**
- **Auf das Bauchgefühl hören. Wenn Sie den Eindruck haben, dass etwas nicht stimmt, lassen Sie es.**
- **System aktuell halten. Halten Sie unbedingt Ihren Rechner immer auf einem aktuellen Stand. Dazu gehören der Virenscanner, das Betriebssystem, die genutzten Programme, wie auch die (Desktop-) Firewall.**

Autor

* Andreas Wisler ist Senior IT-Security Auditor und Inhaber der goSecurity AG (https://goSecurity.ch). Er berät unter anderem Unternehmen bei der erfolgreichen Einführung eines ISMS nach ISO 27001, ISO 27701 und ISO 22301. Zudem unterrichtet er an der Fachhochschule Nordwestschweiz verschiedene IT-Security-Themen. Unter https://27001.blog kann sein Blog verfolgt werden.