RATGEBER PHISHING

Phishing ist für Privatpersonen eine der schlimmsten Bedrohungen im Internet, weil es schnell kostspielige Folgen haben kann. Mit jeder Menge hinterlistigen Tricks versuchen die Angreifer, Druck aufzubauen und die Internet-User zu vorschnellem Handeln zu verleiten. Das Ziel: Sie klicken auf einen Link und geben im Internet persönliche oder Zahlungsdaten an, die die Kriminellen dann für eigene Zwecke missbrauchen. Phishing gibt es mittlerweile in vielen Formen – als E-Mails, Anrufe, SMS, WhatsApp-Nachrichten, Werbebanner oder in sozialen Medien. Ein gutes Schutzprogramm warnt Sie vor den meisten gefälschten Internetseiten, aber auch nicht vor allen. Nur wer die Tricks kennt, Ruhe bewahrt und genau nachdenkt, ist vor solchen Betrugsmaschen sicher.

Definition: Was ist Phishing?

Phishing kommt vom englischen "password harvesting" ("Passwörter ernten") und "fishing" ("angeln"). Es geht um Versuche, Menschen mit gefälschten Nachrichten, Mails oder SMS auf Betrugsseiten zu locken. Dort versuchen die Angreifer dann Zugangsdaten zu stehlen, etwa fürs Online-Banking, oder Schadsoftware auf die PCs der Opfer zu bringen. Phishing passiert unter Umständen auf gefälschten Internetseiten, die etwa die Amazon-Seite eins zu eins kopieren und nach Anmeldedaten fragen – und diese dann speichern. Die Betrüger versuchen auch, ihre Opfer mit falschen Rechnungen, Abmahnungen, angeblichen Kontolöschungen oder Ähnlichem auf die Seite zu locken.

Phishing-Trick: Persönliche Ansprache

Aus Hacks von Internetseiten gibt es im Internet mittlerweile Milliarden Datensätze zu Dumping-Preisen. Die darin enthaltenen Passwörter sind häufig schon geändert. Der Name und die E-Mail-Adresse bleiben aber in der Regel gleich. Das machen sich Cyberkriminelle zunutze und verschicken automatisch generierte Mails mit persönlicher Ansprache – oft mit vermeintlichen Rechnungen. Wer diesen Trick nicht kennt, möchte sich das Ganze vielleicht genauer anschauen und öffnet den Anhang. Tun Sie das nicht! Sind Sie Kunde beim vermeintlichen Absender? Dann öffnen Sie die zugehörige Internetseite direkt und schauen dort nach oder kontaktieren den Support. Sind Sie kein Kunde, ignorieren Sie die Mail einfach.

Phishing-Trick: Gefälschter Absender

Haben die Kriminellen ein E-Mail-Konto gekapert, verschicken sie auch gern mal an das komplette Adressbuch eine Mail, die so aussieht, als hätte der Kontakt eine Datei geteilt. Darin steckt aber ein Trojaner, der die Kontrolle über den PC übernimmt oder persönliche Dateien verschlüsselt und Lösegeld verlangt, sobald man ihn startet. Auch in diesem Fall gilt: Kommt es Ihnen komisch vor, dass Sie diese Datei erhalten? Dann fragen Sie beim Absender auf anderem Wege nach, etwa per Telefon. Öffnen Sie die Datei nicht, wenn Sie nicht sicher sind, dass sie harmlos ist!

Phishing-Trick: Verirrte Mail

Ebenso gern nutzen Betrüger (angeblich) verirrte Mails. Beispielsweise stammen solche Nachrichten scheinbar von der Personalabteilung, enthalten Gehaltsliste oder Budgets und sollten eigentlich an den Chef gehen, sind aber zufällig bei Ihnen gelandet. Hier ist der Trick, die Neugier des Empängers auszunutzen. Dem ist absolut klar, dass die Mail nicht für ihn gedacht ist, er kann daher auch nicht nachfragen. Aber natürlich interessiert ihn auch, was die anderen so verdienen oder wie hoch das Budget der Abteilung ist. Verzichten Sie darauf, reinzugucken! Es ist äußerst unwahrscheinlich, dass die Mail sich tatsächlich verirrt hat. Stattdessen dürfte sie Malware enthalten.

Phishing-Trick: Makros

Mit Makros lassen sich einfache Funktionen in Office programmieren und so etwa Berechnungen für Tabellen erledigen. Kriminelle nutzen Makros aber auch dazu, Ihren PC anzugreifen. Sie sollten sie

daher nur dann aktivieren, wenn Sie genau wissen, was diese bewirken. Phishing-Versender nutzen regelmäßig Makros in angehängten Dokumenten und verweisen oft darauf, dass man diese mit mobilen Geräten erstellt hat und Sie sie daher aktivieren müssen, damit sie korrekt angezeigt werden. Das ist Quatsch! Wer so etwas behauptet, will Ihnen Schadsoftware unterjubeln.

Phishing-Trick: Schockmomente

Wenn wir geschockt sind, reagieren wir sehr schnell und denken oft nicht richtig nach. Genau das wollen die Internet-Betrüger. Deshalb schicken sie Horror-Botschaften über hohe Rechnungen oder eventuelle Gerichtsverfahren, behaupten, dass etwas mit wichtigen Benutzer-Accounts oder Bankkonten nicht stimmt und Ähnliches. Meist ist ein Link enthalten, der zu einer gefälschten Webseite führt. Dort wollen die Angreifer dann Ihre Anmeldeinformationen abgreifen und setzen darauf, dass Sie in der Eile nicht so genau hinsehen. Deshalb: Egal welche Horror-Botschaften per Mail kommen, bleiben Sie ruhig und denken Sie nach. Ist es wirklich üblich, solche Nachrichten per E-Mail zu erhalten? Und ist das wirklich die korrekte Internetseite?

Phishing-Trick: Corona

Corona ist nach wie vor allgegenwärtig – und viele interessieren sich für aktuelle Zahlen, neue Regeln, Masken und mehr. Auch das nutzen die Kriminellen aus und locken etwa mit Super-Sonderangeboten, exklusiven Infos oder Ähnlichem. Die Ware kommt natürlich nie an, und die Informationen gibt es auch so im Netz. Dafür hagelt es saftige Rechnungen, gefälschte Anwaltsschreiben oder Schadsoftware. Seien Sie daher auch bei E-Mails mit Corona-Bezug sehr vorsichtig.

Phishing-Trick: Cloudspeicher

Viele Schutzprogramme untersuchen E-Mail-Anhänge und melden, wenn dort etwas Verdächtiges enthalten ist. Einige Angreifer sind daher dazu übergegangen, Mail-Anhänge aus der Cloud einzubinden. Die Dateien sind dann nicht wirklich angehängt, sondern nur als Link in der Mail und liegen in Wirklichkeit auf Online-Speichern wie OneDrive oder Dropbox. Sofern es sich nicht um sehr große Dateien oder die vertrauenswürdige Firmen-Cloud handelt, sind solche Links zu Cloudspeichern verdächtig. Seien Sie daher in diesen Fällen besonders skeptisch.

Phishing-Trick: SMS aufs Handy

Auch Smartphone-Besitzer sind vor Phishing-Versuchen nicht sicher: Immer häufiger verschicken Kriminelle SMS-Nachrichten, die auf angeblich wartende Pakete oder Sprachnachrichten hinweisen. Die Empfänger sollen einen Link für weitere Infos öffnen und landen auf altbewährten Betrugsseiten. Da die Absender ständig wechselnde Nummern verwenden, lassen sich diese nicht zuverlässig blockieren. Am besten ignorieren Sie solche Nachrichten.

Phishing-Trick: Spenden

Die meisten Menschen haben einen instinktiven Impuls, anderen in Not zu helfen. Das nutzen Kriminelle aus. Mit Videos zu kranken Kindern, deren Eltern sich die Arztrechnung nicht leisten können, Kriegsopfern und Ähnlichem bitten sie um Spenden. Die landen aber natürlich nicht bei den im Video gezeigten Personen. Wenn Sie spenden möchten, tun Sie das besser direkt bei Hilfsorganisationen. Davon gibt es viele für unterschiedlichste Zwecke. Spenden Sie auf keinen Fall mit Kryptowährung. Dahinter steckt so gut wie immer Betrug.

Phishing-Trick: Sugardaddy

Andere Kriminelle schreiben junge Frauen auf Instagram an, dass sie deren Sugardaddy sein wollen. Die Frau sei gestorben und sie bräuchten einfach jemanden zum Reden und sind bereit, dafür viel Geld zu bezahlen. Bei der Bezahlung schicken sie dann einen Screenshot, der zeigen soll, dass etwas nicht geklappt hat. Um das zu korrigieren, sollen die Frauen einen kleinen Betrag schicken, der

dann mit dem Sugardaddy verschwindet. Nutzen Sie niemals die PayPal-Funktion "Geld an Freunde senden", wenn es keine Freunde sind.

Phishing-Trick: Neue Nummer

Neuerdings sehr beliebt ist auch die Masche, sich per SMS oder WhatsApp mit einer unbekannten Nummer zu melden und als Sohn oder Tochter auszugeben. Angeblich sei dies die neue Nummer, man solle sie speichern und doch gleich eine Nachricht schicken. Wer das macht, bekommt eine traurige Geschichte über ein kaputtes Auto oder Ähnliches erzählt. Darauf folgt die Bitte, ob man nicht die Rechnung übernehmen könne, weil gerade das Online-Banking oder die Kreditkarte streikt. Die Beträge liegen im hohen Hunderter- oder niedrigen Tausender-Bereich, sodass Eltern das durchaus einmal vorstrecken würden. Ein Anruf bei der alten Nummer oder über das Festnetz lässt den Schwindel schnell auffliegen.

So schützen Sie sich vor Phishing

Es gibt eine Menge Hinweise darauf, ob hinter einer Mail ein Phishing-Versuch steckt oder nicht. Viele sind jedoch nicht auf den ersten Blick zu erkennen:

1. Kontrollieren Sie den Absender der Nachricht. Als Name kann jeder eintragen, was er will. Die Absender-Adresse ist aber schwerer zu fälschen. Daher zeigen viele Phishing-Mails beispielsweise "Amazon" als Absender an, die dazugehörige Mail-Adresse lautet dann aber "skdjfp@sdoifhao.to" oder ähnlich. Achten Sie vor allem auf den Teil hinter dem @-Zeichen: Eine Mail von der Adresse amazon@xyz.com kommt sicher nicht vom Versandhändler, eine von xyz@amazon.de hingegen schon.
2. Achten Sie auf Bilder. Offizielle E-Mails haben normalerweise eine Signatur mit Firmenlogo und speziellen Formatierungen. Hacker versuchen, das nachzustellen, indem sie Fotos von diesen Signaturen in die Mails einbauen. Das lässt sich besonders gut erkennen, wenn Sie den Dark Mode bei Ihrem E-Mail-Programm oder im Postfach aktiviert haben, dann sind die gefälschten Signaturen nämlich weiß umrandet.
3. Kontrollieren Sie Links. Wenn Sie den Mauszeiger über einen solchen bewegen, ihn aber nicht klicken, sehen Sie links unten oder in einem Pop-up die vollständige Verknüpfung, die dahinter liegt. Steht im Text beispielsweise, dass Sie Ihr Amazon-Konto aufrufen sollen, und als Link dann eine Adresse, die nicht zu Amazon gehört oder eine Kurz-URL wie etwa bit.ly, ist das eine Fälschung!
4. Öffnen Sie keine Anhänge. E-Mail-Anhänge sollten Sie grundsätzlich nur dann anklicken, wenn Sie diese auch erwartet haben. Fast alle ungefragt geschickten digitalen Anlagen enthalten Schadcode!
5. Googeln Sie den Betreff oder den Absender. Phishing-Mails gehen meist an Millionen von Empfängern. Häufig finden Sie bei einer Google-Suche eine Warnung vor derartigen Mails.
6. Kontrollieren Sie URLs. Sollten Sie aus einer E-Mail heraus bei einem Login-Fenster landen, kontrollieren Sie die URL in der Adresszeile des Browsers selbst dann, wenn alles korrekt wirkt. Wichtig dabei ist, was vor dem ersten "/" steht. Eine Internetadresse besteht aus einem frei wählbaren Wort für die Seite, einem Punkt und einer Länder-Endung, etwa "computerbild" + "." + "de". Hinter der Landesendung folgen ein "/" und verschiedene Parameter sowie Unterseiten. Vor dem Wort für die Seite lassen sich aber auch noch beliebig Unterseiten vorschalten, die mit Punkten abgetrennt sind, zum Beispiel "amazon.de.computerbild.de". Die letzten beiden Wörter vor dem ersten "/" geben aber immer die Hauptseite an. Passen diese nicht zu der Seite, auf der Sie sich anmelden wollen, schließen Sie den Browser. Achten Sie auch auf "Tippfehler", etwa "arnazon.de".
7. Ein gutes Schutzprogramm filtert Spam-Nachrichten heraus und warnt Sie, wenn Sie sich auf gefälschten Internetseiten befinden.
8. Beachten Sie die Tipps gegen Phishing in Messengern.

Was tun, wenn man auf Phishing reingefallen ist?

Bei allen Vorsichtsmaßnahmen kann es passieren, dass man doch mal auf eine gut gemachte Masche hereinfällt. Dann ist schnelles Handeln gefragt. Hier die wichtigsten Tipps, was Sie in so einem Fall tun sollten:

- Scannen Sie den Computer mit einem Antivirus-Programm, um zu verhindern, dass die Betrüger noch mehr Daten abgreifen.
- Ändern Sie alle Kennwörter, die Sie angegeben haben – auch auf anderen Seiten, wenn Sie dort dieselben Zugangsdaten nutzen.
- Haben Sie Zahlungsdaten eingegeben, kontaktieren Sie den Anbieter oder die Bank. Kreditkarten lassen sich sperren und ersetzen, um Schaden zu vermeiden. Bei anderen Anbietern ändern Sie das Passwort. Kontrollieren Sie auch, ob schon ungewollte Zahlungen geflossen sind.
- Ist ein finanzieller Schaden entstanden, stellen Sie Anzeige bei der Polizei.
- Informieren Sie Freunde und Bekannte über die Masche, damit diese nicht drauf hereinfallen.

Phishing-Mails melden

Phishing-Mails lassen sich als Spam bei der Bundesnetzagentur melden. Da hinter den Nachrichten aber keine eingetragenen Firmen, sondern Internet-Kriminelle stecken, führt eine Beschwerde in den meisten Fällen zu nichts. Eine weitere Möglichkeit: Bei vielen E-Mail-Anbietern lässt sich Spam melden, damit solche Nachrichten automatisch aus dem Posteingang aller Nutzer verschwinden. Wie genau das geht, ist von Anbieter zu Anbieter unterschiedlich. Bei Gmail zum Beispiel antworten Sie auf die E-Mail, klicken auf die drei Punkte und auf *Phishing melden*. Sollten Sie tatsächlich Schaden durch Phishing genommen haben, melden Sie den Vorfall der Polizei und Ihrer Bank oder dem Anbieter, bei dem der Schaden entstanden ist. Unter Umständen bekommen Sie dadurch im Schadensfall wenigstens Ihr Geld zurück.