INFOPAPER:
PHISHING ERKENNEN UND RICHTIG HANDELN

Inhalt

WAS IST PHISHING?

Phishing ist eine Form des Betrugs, bei dem das Opfer eine gefälschte E-Mail zugesendet bekommt, die im ersten Moment oft nicht als solche erkannt wird. Mit Phishing möchte der Angreifer den Empfänger dazu bringen, **sensible Daten preiszugeben.** Gemeint sind hier beispielsweise personenbezogene Daten und Passwörter.

Die volkswirtschaftlichen Schäden von Cyberangriffen, die mit gezielten Phishing-Attacken beginnen, werden laut dem Bundesamt für Sicherheit in der Informationstechnik jährlich auf einen zweistelligen Millionenbetrag geschätzt. **Für Nutzer ergeben sich diverse Risiken, die je nach Motiv des Angreifers variieren können.** Die gestohlenen Daten werden beispielsweise für Kontoplünderungen oder **weitere Hackerangriffe auf Unternehmen verwendet.**

Die am häufigsten verwendete Methode beim Phishing ist der massenhafte Versand von E-Mails mit gefälschtem Inhalt. Aber auch gezielte Angriffe werden immer beliebter: Beim Spear-Phishing recherchieren Angreifer im Voraus über ihre Opfer. Sie geben vor ihr Opfer persönlich zu kennen, versuchen so ihr Vertrauen zu gewinnen und auf diesem Weg an wertvolle Daten zu gelangen.

Wie erkenne ich eine Phishing-E-Mail?

Eine professionell gestaltete Phishing-E-Mail zu erkennen, ist für Laien oft nicht einfach – aber auch nicht unmöglich. Die nachfolgenden Punkte wurden gemeinsam mit den Experten vom Hornetsecurity Security Lab zusammengetragen und helfen bei der Identifikation von Phishing-E-Mails anhand unterschiedlicher Merkmale.

Der Absender

Häufig schreiben Cyberkriminelle im Namen von Onlineshops, wie Amazon und eBay, oder von Online-Banking-Plattformen, wie PayPal. Die **Detailansicht der E-Mail-Adresse** kann Aufschluss über die wahre Herkunft der Nachricht geben. Ist diese nicht plausibel oder beinhaltet Buchstabendreher oder kryptische Zahlen, ist das ein Warnzeichen.

Ein Beispiel: noreply@amzon.com anstelle von noreply @amazon.com. Mittlerweile lassen sich Absender-Adressen allerdings komplett fälschen, weshalb die E-Mail auf weitere Phishing-Merkmale geprüft werden sollte. Das Security Lab empfiehlt außerdem die Überprüfung des E-Mail-Headers, um detaillierte Informationen über die Nachricht zu erhalten.

Hinweise zu der Herkunft der E-Mail sind in den Received-Zeilen zu finden. Diese dokumentieren alle von der E-Mail durchlaufenen Server und Hosts. In der Regel kann man sich die detaillierte Ansicht des Headers im E-Mail-Programm unter „Ansicht" oder unter „Optionen" anzeigen lassen.

Der Empfänger

Neben der Absender- kann auch die **Empfänger-Adresse** Aufschluss über die Vertrauenswürdigkeit einer E-Mail geben. Hat sich ein Nutzer beispielsweise bei PayPal mit einem Google-Mail-Konto angemeldet, aber eine E-Mail von PayPal auf eine GMX-Adresse empfangen, handelt es sich möglicherweise um Phishing. Dies ist selbstverständlich nur ein Indikator, wenn der Nutzer auch mehrere E-Mail-Adressen verwendet.

Die Anrede

Bei großangelegten Phishing-Kampagnen versenden Cyberkriminelle ihre gefälschten Nachrichten an Hunderte, teilweise auch Tausende Empfänger. Oft bleibt dabei **die richtige Anrede des Empfängers** auf der Strecke. Besonders wenn ein vermeintlicher Vertragspartner plötzlich nicht mehr den Namen des Empfängers kennt und stattdessen allgemeine Anreden verwendet, ist Vorsicht geboten.

Layout, Rechtschreibung und Grammatik

Cyberkriminelle aus dem Ausland nutzen häufig Rechtschreibprogramme zum Verfassen ihrer gefälschten E-Mails. Je nach Komplexität der Themen und Sätze, entstehen dabei oftmals mehr oder minder schwerwiegende Fehler. Auch die **Zeichensetzung** spielt eine Rolle beim Erkennen einer Phishing-E-Mail: Neben **falsch gesetzten Kommata und Bindestrichen** können auch **fremde Zeichen** in einer gefälschten E-Mail auftauchen. Die Experten vom Hornetsecurity Security Lab empfehlen außerdem, auf die **Qualität des Layouts** der E-Mail zu achten. Oft deuten auch grafische Fehler auf einen Phishing-Angriff hin.

Psychologischer Druck

Das Ausüben von Druck spielt eine maßgebliche Rolle beim Verfassen von Phishing-E-Mails. Cyberkriminelle üben **Druck auf den Empfänger einer E-Mail aus, um so das „kritische Denken" außer Gefecht zu setzen.** Oft werden dem Empfänger folgenschwere Konsequenzen und Strafen bei Nichthandeln angedroht und bringen ihn so dazu, schnell und unüberlegt zu handeln.

Auch **vermeintliches Detailwissen** soll das Opfer dazu bringen, dem Sender zu glauben. Ein Beispiel dafür ist die „Sextortion"-Masche. Der Cyberkriminelle gibt vor im Besitz von Videomaterial zu sein, das über die gehackte Webcam aufgenommen wurde und den Empfänger bei sexuellen Handlungen oder Ähnlichem zeigt.

Um zu beweisen, dass der Cyberkriminelle den Rechner des Opfers wirklich gehackt hat, werden teilweise sogar korrekte Passwörter aufgeführt, die allerdings aus alten Datenlecks stammen. Cyberkriminelle erpressen ihre Opfer mit diesen Aufnahmen und fordern sie zu einer **Zahlung auf, die meist in Form von Bitcoins oder anderen Kryptowährungen** erbracht werden soll.

Links, Phishing-Seiten und Anhänge

Oft versuchen Cyberkriminelle den Empfänger dazu zu bringen, eine URL zu öffnen. Der ahnungslose **Nutzer wird auf eine Fake-Website** geleitet, auf der er personenbezogene Daten eingibt und unwissend mit dem Hacker teilt. Um schadhafte oder gefälschte Links zu identifizieren, sollte unter anderem geprüft werden, ob der Link zum Absender passt, der ihn versendet hat. Links, die **neben dem Namen der jeweiligen Institution auch Nummern enthalten,** sind dabei besonders zu beachten.

Einige Links verstecken sich hinter einer vertrauenswürdig wirkenden URL. Um das tatsächliche Ziel des Links zu sehen, können Nutzer den Mauszeiger, ohne zu klicken auf die URL setzen (hovern), um sich den Hover-Text anzeigen zu lassen. Der **Hover-Text zeigt die gesamte Ziel-URL.** Oft nutzen Cyberkriminelle Subdomains und eine Erweiterung des Links durch weitere Zeichen, um die Domain, auf die der User tatsächlich geführt wird, zu verstecken.

Ob eine Website echt oder gefälscht ist, lässt sich oft nur schwer erkennen. Die Abkürzung https:// galt einst als Zeichen für eine sichere Verbindung, allerdings bedeutet dies nur, dass der Betreiber der Website ein SSL-Zertifikat erworben hat. Auch Cyberkriminelle können dieses Zertifikat für ihre Website erwerben – die Abkürzung bedeutet also nicht zwingend eine Entwarnung. Ein Indiz für eine Phishing-Website könnte allerdings die **Abfrage einer Transaktionsnummer sein, ohne dass vorher eine Transaktion vorgenommen wurde.** Vorsicht ist außerdem geboten, wenn beispielsweise nach der Anmeldung im Online-Banking eigentlich bekannte Daten, wie Name und Adresse oder die IBAN, eingegeben werden sollen. Ist man nicht sicher, ob die in der E-Mail angegebene URL wirklich zur richtigen Website führt, sollten Nutzer die ihnen bekannte Website-Adresse direkt im Browser aufrufen und dort die Account-Daten eingeben.

Auch E-Mail-Anlagen können Risiken in sich bergen. Insbesondere bei **Angriffen auf Unternehmen verwenden Hacker häufig schadhafte Anhänge.** Sie versenden vermeintliche Rechnungen, Kontoauszüge oder Geschäftsbriefe in Formaten wie *.xls, *.doc oder *.pdf. Diese enthalten beispielsweise Trojaner, die Dateneingaben protokollieren und die Informationen an den Cyberkriminellen weitergeben. Vor dem Öffnen eines Anhangs sollte der Empfänger der Nachricht stets den Absender überprüfen, zum Beispiel mit der Detailansicht des E-Mail-Headers (Kapitel: Der Absender) oder telefonisch nachhaken.

Abfrage von vertraulichen Daten

Besonders bei E-Mails, die von Unternehmen aus dem Finanzsektor stammen, müssen Nutzer wachsam sein. Wenn in einer E-Mail nach **persönlichen Informationen oder Geheimnummern und Passwörtern** gefragt wird, ist dies ein Indiz für Phishing. Seriöse Banken erfragen sensible Daten, wie zum Beispiel PIN-Nummern, im Regelfall schriftlich in Briefform.

SICHERHEITSMASSNAHMEN

Um sich vor Phishing-Angriffen zu schützen, können Nutzer einige **Sicherheitsvorkehrungen treffen,** die Accounts im Ernstfall schützen können. Auch nachdem ein User einer Attacke zum Opfer gefallen ist, kann das richtige Handeln danach nicht nur zur Schadensbegrenzung dienen, sondern **auch andere vor den perfiden Angriffen schützen.**

Passwortsicherheit

Der verantwortungsvolle Umgang mit Passwörtern kann **im Fall eines erfolgreichen Phishing-Angriffs weitere Folgeschäden eingrenzen.** Nutzer sollten für jeden Online-Account ein einzigartiges Passwort verwenden. Gelangt ein Hacker an Log-in-Daten, die mehrfach genutzt werden, sind **im Worst Case alle Accounts in Gefahr.**

Zwei-Faktor-Authentifizierung

Mit der Zwei-Faktor-Authentifizierung ist es dem Nutzer möglich, eine weitere Sicherheitsstufe zu erzeugen. Ein gängiges Zwei-Faktor-System ist das **Senden eines Bestätigungscodes an ein weiteres Gerät.** So sind die sensiblen Daten des Nutzerkontos sicher – selbst, wenn ein Hacker bereits die Zugangsdaten dafür erbeutet hat.

Awareness

Es ist wichtig, sich mit den **Taktiken und Maschen von Betrügern auseinanderzusetzen** – so ist man in der Lage, diese schneller zu erkennen oder ähnliche Taktiken zu identifizieren. Neben einem technischen Schutz ist es essenziell, sich für die perfiden Betrugsmaschen zu sensibilisieren. Die Kreativität der Cyberkriminellen ist grenzenlos: Oft greifen sie aktuelle Ereignisse auf und nutzen emotional behaftete Themen, um ihren Nachrichten Glaubwürdigkeit zu verleihen.

Besonders Bankkunden fallen Maschen wie dieser zum Opfer. So versendeten Cyberkriminelle gefälschte E-Mails im Namen von PayPal, die sich auf die damals kürzlich in Kraft getretene DSGVO bezogen. Es gibt **Internetseiten, wie die der Verbraucherzentrale, auf der aktuelle Phishing-Methoden gelistet sind.** Ein Blick auf die Liste kann oft Aufschluss darüber geben, ob man Opfer einer betrügerischen E-Mail geworden ist.

Notfall-Maßnahmen

Haben es die Cyberkriminellen doch geschafft über eine Phishing-E-Mail an Zugangsdaten eines Nutzers zu gelangen, kann sich dieser trotzdem schützen. Falls es noch möglich ist, sollte sich der User schnellstmöglich bei dem **betroffenen Account anmelden, um das Passwort zu ändern.** Außerdem sollte kontrolliert werden, ob bereits Änderungen im Konto vorgenommen oder sogar Transaktionen, wie zum Beispiel eine Überweisung, getätigt wurden. In diesem Fall empfiehlt es sich das betroffene Konto schnellstmöglich zu sperren.

Phishing-Angriffe melden

Phishing-E-Mails und Phishing-Websites können bei dem Absender gemeldet werden, von dem die E-Mails angeblich stammen soll. Auch eine Information an das Phishing-Radar der Verbraucherzentrale ist sinnvoll. Die gefälschten E-Mails werden hier gelistet und sind so auch für andere User zu finden. Arbeitnehmer können potenzielle Phishing-Angriffe bei dem firmenintern Beauftragten für IT-Sicherheit melden, damit das Unternehmen entsprechend reagieren kann. Bei der Nutzung eines E-Mail-Security-Services sollten Auffälligkeiten, die auf einen Phishing-Angriff hinweisen, dem zuständigen Provider gemeldet werden.

Checkliste

- **Absender überprüfen:** Kenne ich den Absender? Sind kryptische Zahlen oder Buchstabendreher in der Absender-Adresse? Welche IP-Adresse wird im Header angezeigt?
- **Empfänger:** Bei der Nutzung unterschiedlicher E-Mail-Konten auf die richtige Adresse achten: Habe ich mich mit meinem GMX- oder meinem Google-Mail-Account bei PayPal angemeldet?
- **Layout, Rechtschreibung und Grammatik:** Ist die Anzahl von Rechtschreib- und Grammatikfehlern auffällig? Gibt es unbekannte Zeichen in der E-Mail? Macht das Layout allgemein einen qualitativ hochwertigen Eindruck?
- **Anrede:** Wurde ich mit meinem richtigen Namen angesprochen?
- **Psychologischer Druck:** Droht der Absender mit der Veröffentlichung von Videoaufnahmen, rechtlichen Schritten oder Ähnlichem? Fordert der Absender zu schnellem Handeln auf?
- **Links, Anhänge und Websites prüfen:** Ist die URL die originale Website-Adresse des vermeintlichen Absenders? Um welche Dateiformate handelt es sich bei den Anhängen? Werden auf der Phishing-Website Daten abgefragt, die dem Betreiber eigentlich bekannt sein müssten?
- **Abfrage vertraulicher Daten:** Wird der Empfänger zum Eingeben von Passwörtern oder PIN-Nummern aufgefordert?
- **Sicherheitsmaßnahmen:**
  - Verwende ich bei jedem Account unterschiedliche und sichere Passwörter? Nutze ich die Zwei-Faktor-Authentifizierung? Kenne ich mich mit den typischen Phishing-Maschen aus?
  - Notfall-Maßnahmen: Passwörter ändern, Konten sperren lassen, Phishing-Angriffe bei Unternehmen und der Verbraucherzentrale melden

Grundsätzlich sind all die genannten Indikatoren und Tipps bei der **Erkennung und Prävention von Phishing-Angriffen** hilfreich, doch um sich zuverlässig abzusichern, **empfiehlt Hornetsecurity die Nutzung von E-Mail-Security-Services**, die Phishing-Angriffe bereits im Voraus erkennen.