DIE FALLEN IM NETZ: WIE SIE PHISHING UND ANDERE METHODEN ZUVERLÄSSIG ERKENNEN

Achtung, Köder im Netz:
Durch diverse Tricks versuchen Betrüger an Ihr Geld und an Ihr Konto zu kommen.

Vorwort

Liebe Anwenderinnen und Anwender,

Cyberkriminalität hat sich zu einer der größten Bedrohungen für Einzelpersonen und Unternehmen entwickelt. Das Jahr 2023 war geprägt von einer deutlichen Zunahme an Cyberangriffen, sowohl in ihrer Häufigkeit als auch in ihrer Komplexität. Und der Schaden für die deutsche Wirtschaft ist enorm: 148 Milliarden Euro alleine in Deutschland haben Hacker und Trojaner durch das Ausspähen und Stehlen von Daten und durch das Lahmlegen von wichtigen Systemen in Unternehmen verursacht.

Besonders besorgniserregend ist die steigende Anzahl an Angriffen aus dem Ausland, die zunehmend auch Auswirkungen auf Deutschland haben.

Phishing ist weit verbreitet und die Betrüger lassen sich, auch dank künstlicher Intelligenz, immer wieder neue Tricks einfallen. Hier zeige ich Ihnen wichtige Tipps, worauf Sie achten müssen.

Ihr Kaner Etem

Phishing und Smishing: Der Köder im Netz

Phishing und Smishing sind weit verbreitete Methoden, um an persönliche Daten und Zugangsdaten zu gelangen. Beim Phishing werden betrügerische E-Mails, Nachrichten oder Webseiten genutzt, die täuschend echt aussehen und von vertrauenswürdigen Unternehmen oder Institutionen zu stammen scheinen. Das Ziel ist es, die Empfänger dazu zu bringen, ihre sensiblen Daten wie Passwörter, Kreditkartennummern oder PINs preiszugeben.

Smishing ist eine Variante des Phishings, bei der SMS (Kurznachrichten) anstelle von E-Mails verwendet werden. Oftmals werden die Opfer mit vermeintlichen Gewinnen, dringenden Warnungen oder angeblichen Problemen mit ihrem Konto oder ihrer Bestellung in die Falle gelockt.

Ransomware: Die digitale Geiselnahme

Eine der größten Bedrohungen im Bereich der Cyberkriminalität bleibt Ransomware. Diese Schadprogramme verschlüsseln die Dateien ihrer Opfer und machen sie unzugänglich. Die Kriminellen fordern dann ein Lösegeld für die Entschlüsselung, oft in Kryptowährungen, um ihre Spuren zu verwischen.

Die Verbreitung von Ransomware erfolgt häufig über Phishing-E-Mails oder schädliche Webseiten. Ein unbedachter Klick auf einen infizierten Link oder das Öffnen eines schädlichen Anhangs kann ausreichen, um die Schadsoftware auf dem eigenen Computer zu installieren. Einmal infiziert, verschlüsselt die Ransomware die Dateien des Opfers und zeigt eine Lösegeldforderung an.

Die Folgen einer Ransomware-Infektion können verheerend sein. Neben dem Verlust wichtiger Daten, der auch nach Zahlung des Lösegelds nicht ausgeschlossen ist, entstehen oft hohe finanzielle Schäden durch die Lösegeldzahlung selbst und die Kosten für die Wiederherstellung der Systeme. Für Unternehmen können Ransomware-Angriffe zu erheblichen Betriebsunterbrechungen führen.

Künstliche Intelligenz: Ein zweischneidiges Schwert

Künstliche Intelligenz (KI) spielt eine immer größere Rolle in der Cyberkriminalität. Während KI das Potenzial hat, die Cybersicherheit zu stärken, nutzen Kriminelle sie auch, um ihre Angriffe zu optimieren und effektiver zu gestalten.

KI senkt die Einstiegshürde für Menschen mit geringen IT-Kenntnissen, indem sie komplexe Angriffe vereinfacht. Gleichzeitig verstärkt sie die Fähigkeiten erfahrener Cyberkrimineller, indem sie ihnen neue Werkzeuge und Methoden zur Verfügung stellt.

Zudem ermöglicht KI die Erstellung professionellerer und authentischerer Phishing-Mails, die von legitimen Nachrichten kaum noch zu unterscheiden sind.

KI-Enkeltrick: Die neue Generation des Betrugs

Eine besonders perfide Betrugsmasche, die an Bedeutung gewonnen hat, ist der sogenannte KI-Enkeltrick. Dabei nutzen Betrüger Künstliche Intelligenz, um die Stimmen von Verwandten, wie Kindern oder Enkeln, täuschend echt zu imitieren. Heutzutage reichen lediglich 2 Minuten Sprachmaterial aus, um die KI auf eine Stimme zu trainieren und dann mit Hilfe von Texten beliebige Inhalte vorlesen zu lassen!

In einem typischen Szenario täuschen die Kriminellen einen Notfall vor, wie einen Unfall oder eine Festnahme, und bitten ihre Opfer dringend um Geld. Die emotionale Belastung und der Zeitdruck, der durch den vorgetäuschten Notfall erzeugt wird, machen es den Opfern schwer, den Betrug zu erkennen.

Schutzmaßnahmen und Handlungsempfehlungen

Prävention:

- **Misstrauen:** Seien Sie misstrauisch gegenüber unerwarteten E-Mails, Nachrichten oder Anrufen, insbesondere wenn sie Geldforderungen oder dringende Aufforderungen enthalten. Bei Zweifeln an der Dringlichkeit einer Nachricht, rufen Sie das Unternehmen über die offizielle Hotline an (nicht die Telefonnummer aus der Phishing-Nachricht verwenden!)
- **Vorsicht bei Links und Anhängen:** Klicken Sie nicht auf Links oder öffnen Sie keine Anhänge von unbekannten Absendern.
- **Starke Passwörter verwenden:** Verwenden Sie komplexe Passwörter
- **Nutzen Sie die Zwei-Faktor-Authentifizierung:** Viele Internetdienste bieten die Zwei-Faktor-Authtentifizierung (2FA), bei der Sie einen Login zusätzlich durch ein zweites Gerät, typischerweise Ihrem Smartphone, bestätigen müssen. So haben dritte Personen auch dann keinen Zugriff auf Ihr Konto, wenn sie das richtige Passwort kennen.
- **Software aktuell halten:** Installieren Sie regelmäßig Updates für Ihre Betriebssysteme und Anwendungen, um Sicherheitslücken zu schließen.
- **Am allerbesten: E-Mails und SMS mit „dringenden“ Aufforderungen oder Geldforderungen einfach ignorieren!**

Im Ernstfall:

- **Bei Schaden:** Anzeige bei der Polizei. Zwar ist die Aufklärungschance bei Cyber-Kriminalität verschwindend gering, aber Ihr Fall ist aktenkundig.
- **Bei Online-Banking-Schäden:** In den meisten Fällen zahlt die Bank diese Schäden zurück – außer die Bank kann nachweisen, dass Sie grob fahrlässig gehandelt haben. Als grob fahrlässig gilt zum Beispiel, dass Sie PIN- oder TAN-Nummern freiwillig an dritte Personen übergeben oder sehr große Summen (z. B. 8000 Euro) einfach ins Ausland überweisen (OLG Oldenburg, 21.08.2018 - 8 U 163/17).
- Haben Sie eine **Rechtsschutzversicherung**? Wenn nein, dann sollten Sie eine abschließen, damit Sie Ihr Recht durchsetzen können. Denn oft versuchen Versicherungen die Schuld Ihnen zu geben.
- Viele **Hausratversicherungen** beinhalten auch die Schadensregulierung bei Cyberkriminalität. Machen Sie sich schlau, ob Ihre Hausratversicherung diese miteinschließt oder man sie als weiteren Baustein hinzufügen kann.

Fazit

Cyberkriminalität ist eine ernstzunehmende Bedrohung, die sich ständig weiterentwickelt. Seien Sie im Internet und vor allem bei eingehenden Nachrichten (E-Mail / SMS) ruhig misstrauisch, wenn Sie auf einmal zu Aktionen gedrängt werden oder hohe Geldsummen gefordert werden. KI macht es mittlerweile sogar möglich, die Stimmen unserer Liebsten zu imitieren – seien Sie daher besonders auf der Hut!

Impressum: Computerwissen, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2-4, 53177 Bonn, Vorstand: Richard Rentrop, Bonn, Redaktionell Verantwortlicher: Sven Udert, VNR Verlag für die Deutsche Wirtschaft AG, Redaktion, Satz & Layout: Kaner Etem, München