2024-02-25 Betrug – Scam

Der böse Betrug über das Internet, meist fängt es mit einer E-Mail an. Aber auch über die sozialen Medien bleiben solche Versuche nicht lange aus. Je geschickter das ganze angelegt wird, umso größer die Erfolgswahrscheinlichkeit. Erst wenn solche Betrügereien nicht mehr funktionieren, dann hört es auf. Eher unwahrscheinlich. (JDH)

Was ist Scam?

Scam ist das englische Wort für Betrug. Im IT-Bereich wird Scam vorwiegend im Zusammenhang mit Vorschussbetrug verwendet. Ein Scam-Opfer soll eine Vorleistung erbringen, um an Geld, Informationen oder Waren zu gelangen. Ein bekanntes Scam-Beispiel ist die E-Mail von einem vermeintlichen nigerianischen Prinzen oder Geschäftsmann, der ein großes Erbe verspricht – natürlich erst nach Zahlung von Gebühren. Ferner gibt es auch den Romance-Scam, der in Verbindung mit Dating-Plattformen eingesetzt wird. Nach anfänglichem Romantik-Versprechen wird um finanzielle Unterstützung gebeten. Wenn man darauf nicht eingeht, wird der Kontakt zumeist sofort abgebrochen und aus ist es mit der Romantik.

Wie erkenne ich Scam?

E-Mail-Betrüger verwenden verschiedene Strategien, um die E-Mail-Abwehr zu umgehen und Benutzer dazu zu bringen, Informationen preiszugeben oder bösartigen Code auszuführen. Einige betrügerische E-Mails enthalten einen Link zu einer vom Angreifer kontrollierten Website, auf der der Angreifer sensible Daten von den Opfern sammelt.

Klare Anzeichen für eine Scam-Mail liegen vor, wenn der Absender einer E-Mail:

- behauptet, dass Sie sich bei einer Website anmelden müssen, da ansonsten Ihr Konto geschlossen wird. Meistens ein Link zu einer vom Angreifer kontrollierten Website.
- behauptet, dass Ihre Zahlungsinformationen ungültig sind und Sie sich bei Ihrem Konto anmelden und diese Informationen ändern müssen, um das Konto aktiv zu halten.
- Sie darauf hinweist, dass Ihre persönlichen Daten nicht korrekt sind und dass sie entweder in einer Antwortnachricht oder auf einer Website an den Angreifer gesendet werden müssen.
- eine Rechnung zur Zahlung anhängt.
- ein Gefühl der Dringlichkeit oder Vertraulichkeit vermittelt.
- behauptet, dass Sie eine staatliche Rückerstattung erhalten könnten und nach sensiblen Daten wie der Sozialversicherungsnummer fragt.
- Sie auffordert, private Daten einzugeben, um kostenlose Produkte, Gutscheine oder Geld zu erhalten.

Aber immer häufiger weisen betrügerische E-Mails erst einmal keines der typischen Anzeichen auf. Die Scam-E-Mails enthalten keine Anhänge oder URLs. Und sie verstecken sich geschickt, indem sie sich als normale Alltagsgeschäfte tarnen. Diese Angriffe werden manchmal als Business Email Compromise (BEC) oder Email Account Compromise (EAC) bezeichnet. Sie beginnen in der Regel damit, dass sich der Angreifer als jemand ausgibt, dem der Empfänger vertraut – vielleicht ein Chef, Kollege oder Geschäftspartner – und um etwas bittet, das wie eine normale geschäftliche Anfrage aussieht. Dabei kann es sich um eine Überweisung oder die Änderung von Zahlungsdaten handeln, also um Dinge, die im alltäglichen Geschäftsablauf ständig vorkommen. Wenn das Unternehmen merkt, dass etwas nicht stimmt, hat der E-Mail-Betrüger das Geld bereits gestohlen.

Bei E-Mail-Scams gibt es einige Faktoren, die häufig auftreten. Die E-Mails:

- Verwenden ein vertrauenswürdiges Unternehmen (wie FedEx, Netflix, PayPal, Ihre Bank usw.).
- Vermitteln Dringlichkeit, wie z. B. den Verlust eines Kontos oder Produkts, wenn der angesprochene Nutzer nicht reagiert.
- Enthalten eine generische Begrüßung ohne Namen.
- Enthalten eine praktische Schaltfläche, auf die der Zielbenutzer klicken kann, um dann auf die bösartige Website zu gelangen.
- Nutzen eine E-Mail-Adresse, die nicht mit dem offiziellen Unternehmen verbunden ist, ihm aber täuschend ähnlich sieht. Der Absender könnte z. B. die Domain fedexx.com verwenden und Nutzer auf diese Weise täuschen, denn die meisten Anwender schenken der Absenderadresse nicht viel Beachtung.

Was muss ich tun, wenn ich Opfer von Scamming wurde?

- Schnell handeln
- Andere warnen
- Nicht auf Forderungen eingehen
- Anzeige erstatten
- Beweise sammeln
- Kontakt mit dem Betrüger abbrechen

Jochen D. Hohenwald