OUCH!

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

Stopp den Phishzug

Überblick

E-Mail und Nachrichtendienste (wie z.B. Skype, Twitter oder Snapchat) gehören heute zu unseren Hauptkommunikationswegen. Wir nutzen diese Technologien nicht nur beruflich jeden Tag, sondern auch um mit Freunden und Familie in Kontakt zu bleiben. Viele Menschen auf der ganzen Welt sind von diesen Technologien abhängig, daher haben Cyberangreifer Methoden entwickelt um hierüber Angriffe zu starten – das sogenannte Phishing. Sie lernen in diesem Newsletter, was Phishing ist und wie Sie diese Angriffe aufhalten können – sowohl privat wie auch beruflich.

Was ist Phishing

Bei Phishing handelt es sich um eine Form des Angriffs, die E-Mail oder einen Nachrichtendienst nutzt, um Sie dazu zu bewegen etwas zu tun, was Sie besser nicht tun sollten, wie z.B. einen bösartigen Link anzuklicken, Ihr Passwort weiterzugeben oder einen infizierten E-Mail Anhang zu öffnen. Angreifer geben sich viel Mühe, die Nachrichten überzeugend aussehen zu lassen und Ihre emotionalen Seiten anzusprechen, wie z.B. durch Dringlichkeit oder Erwecken von Neugier. Der Angriff kann so gestaltet sein, dass er aussieht als käme er von jemandem den Sie kennen, wie ein Freund oder ein vertrauenswürdiges Unternehmen. Vielleicht fügen die Angreifer auch das Logo Ihrer Bank ein oder fälschen eine E-Mail-Adresse, so dass die Nachricht noch echter wirkt. Eine solche Nachricht wird dann an Millionen Empfänger gesendet. Wer letztendlich darauf hereinfällt ist den Angreifern egal, sicher ist aber, dass um so mehr Menschen darauf hereinfallen, je mehr derartige Nachrichten versendet werden.

Schützen Sie sich

In fast allen Fällen ist das bloße Öffnen und Lesen einer E-Mail oder Nachricht in Ordnung. Damit ein Phishing-Angriff funktioniert, müssen die Angreifer Sie überlisten etwas zu tun. Glücklicherweise gibt es eine Vielzahl von Anzeichen für derartige Angriffe, nachfolgend finden Sie die gängigsten:

- Eine große Dringlichkeit, anfordern von „unmittelbaren Handlungen“ bevor etwas Schlimmes geschieht, wie z.B. eine drohende Kontoschließung oder gar ein Gefängnisaufenthalt. Der Angreifer will, dass Sie durch eine übereilte Reaktion Fehler machen.
- Druck, dass Sie Richtlinien und Abläufe Ihres Arbeitgebers ignorieren oder übergehen.
- Man weckt Ihre Neugier oder die Nachricht erscheint zu gut, um wahr zu sein (nein, Sie haben nicht in der Lotterie gewonnen!).

- Eine allgemein gehaltene Anrede wie „Sehr geehrter Kunde“. Die meisten Unternehmen und Freunde, die Sie kontaktieren, kennen Ihren Namen.
- Anforderung hochsensibler Informationen, wie z.B. Ihrer Kreditkartennummer, Ihres Passworts oder irgendwelcher Informationen die der Anfordernde bereits haben sollte.
- Die Nachricht wirkt als käme sie von einer offiziellen Stelle, weißt aber schlechte Grammatik oder Rechtschreibung auf oder kommt von einer privaten E-Mail-Adresse wie @gmx.de.
- Die Nachricht kommt von einer offiziellen Adresse (z.B. Ihrem Vorgesetzten), nutzt aber eine private Antwort-Adresse (Reply-To).
- Sie erhalten eine Nachricht von jemandem, den Sie kennen, aber der Tonfall klingt einfach ungewohnt. Wenn Sie einen Verdacht haben, rufen Sie den Absender auf einer Ihnen bekannten Nummer an, um zu überprüfen, ob die Nachricht von ihm oder ihr stammt. Es ist für Cyberangreifer sehr leicht, eine Nachricht so wirken zu lassen, als käme sie von einem Freund oder Kollegen.

Gesunder Menschenverstand ist letztendlich Ihre beste Verteidigung. Wenn eine E-Mail oder Nachricht zu gut aussieht um wahr zu sein, könnte es sich um eine Phishing-Nachricht handeln.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gastautor

Tonia Dudley entwickelt und betreibt Security Awareness Programme seit 2011, darunter auch ein preisgekröntes Phishing-Lernprogramm. Sie können sie auf www.linkedin.com/in/toniadudley finden.

Weiterführende Informationen

Social Engineering:	https://www.sans.org/u/Cb1
Hilfe zur Selbsthilfe:	https://www.sans.org/u/Cb6
E-Mail Verhaltensregeln:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
OUCH! Übersetzungen und Archive:	https://www.sans.org/u/Cbq

License

Redaktionsleitung: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley