SANS SECURITY AWARENESS

OUCH!

Der monatliche Security Awareness Newsletter für Jedermann

Angriffe & Betrügereien mittels Telefon

Überblick

Wenn Sie an Cyberkriminelle denken, denken Sie wahrscheinlich an ein böses Superhirn, das hinter einem Computer sitzt und raffinierte Angriffe über das Internet startet. Viele Cyberkriminelle nutzen heutzutage neben E-Mail und Kurznachrichten aber auch ganz einfach das Telefon, um ihre Opfer auszutricksen. Es gibt zwei große Vorteile bei der Benutzung eines Telefons. Erstens gibt es im Gegensatz zu E-Mail weniger Sicherheitstechnologien, die Telefonate überwachen und einen Angriff erkennen und stoppen können. Zweitens ist es für Bösewichte viel einfacher, Emotionen über das Telefon zu vermitteln, was es wahrscheinlicher macht, dass sie ihre Opfer austricksen können. Lassen Sie uns lernen, wie man diese Angriffe erkennt und stoppt.

Wie funktionieren betrügerische Telefonanrufe?

Zuerst sollten Sie verstehen, was diese Angreifer wollen. Sie wollen normalerweise Ihr Geld, Informationen oder Zugang zu Ihrem Computer (oder alles drei). Sie tun das, indem sie Sie dazu bringen, das zu tun, was sie wollen. Die Kriminellen rufen Menschen auf der ganzen Welt an und schaffen Situationen, die sehr dringend erscheinen. Sie wollen Sie aus dem Gleichgewicht bringen, indem sie Sie erschrecken, damit Sie nicht klar denken, und Sie dann in einen Fehler stürzen. Einige der häufigsten Beispiele sind:

Der Anrufer gibt vor, dass er vom Finanzamt oder einem Inkassounternehmen kommt und dass Sie unbezahlte Steuern oder Rechnungen haben. Sie erklären, dass Ihnen eine Gefängnisstrafe droht, wenn Sie Ihre fälligen Steuern oder Rechnungen nicht sofort zahlen, und bauen Druck auf, damit Sie mit Ihrer Kreditkarte über das Telefon bezahlen. Dies ist ein Betrug, das Finanzamt würde nie anrufen oder einzelne Personen per E-Mail kontaktieren. Alle offiziellen Steuerbescheide werden per Post verschickt.

Der Anrufer gibt vor, von der Microsoft Kundenbetreuung zu sein und erklärt, dass Ihr Computer infiziert ist. Sobald der Angreifer Sie überzeugt hat, dass Sie infiziert sind, drängt er Sie dazu, Schadsoftware zu kaufen oder ihm Fernzugriff auf Ihren Computer zu gewähren. Microsoft wird Sie niemals zu Hause anrufen.

Sie erhalten eine automatische Mailbox-Nachricht, dass Ihr Bankkonto gekündigt wurde und Sie eine Nummer zurückrufen müssen, um sie wieder zu aktivieren. Wenn Sie anrufen erreichen Sie nur ein automatisiertes System, das Sie zur Bestätigung Ihrer Identität auffordert und Ihnen alle möglichen privaten Fragen stellt. Dabei handelt es sich jedoch gar nicht wirklich um Ihre Bank, die Angreifer notieren einfach all Ihre Informationen für einen späteren Identitätsbetrug.

Sich selbst schützen

Die größte Verteidigung, die Sie gegen betrügerische Telefonanrufe haben, sind Sie selbst. Behalten Sie diese Dinge im Hinterkopf.

Jedes Mal, wenn Sie jemand anruft und ein enormes Gefühl der Dringlichkeit erzeugt und Sie unter Druck setzt, etwas zu tun, seien Sie extrem misstrauisch. Auch wenn der Anruf zunächst in Ordnung erscheint, sich dann aber merkwürdig anfühlt, können Sie jederzeit unterbrechen und "Nein" sagen.

Wenn Sie glauben, dass ein Anruf ein Angriff ist, legen Sie einfach auf. Wenn Sie bestätigen möchten, ob der Anruf legitim war, gehen Sie auf die Website der Organisation (z.B. Ihrer Bank), holen sich die Telefonnummer des Kundensupports und rufen diese direkt an. So wissen Sie wirklich, dass Sie mit der richtigen Organisation sprechen.

Vertrauen Sie niemals der Anruferkennung, böse Jungs werden oft die Nummer des Anrufers fälschen, so dass es so aussieht, als käme sie von einer legitimen Organisation oder aus Ihrem lokalen Vorwahlbereich.

Lassen Sie niemals zu, dass ein unbekannter Anrufer vorübergehend die Kontrolle über Ihren Computer übernimmt oder Sie zum Herunterladen von Software verleitet. So können Kriminelle Ihren Computer infizieren.

Wenn ein Anruf von jemandem kommt, den Sie nicht persönlich kennen, lassen Sie den Anruf direkt auf den Anrufbeantworter gehen. Auf diese Weise können Sie unbekannte Anrufe in Ihrer Freizeit überprüfen. Noch besser, auf vielen Telefonen können Sie dies standardmäßig mit der Funktion "Nicht stören" aktivieren.

Betrügereien und Angriffe über das Telefon nehmen zu. Sie sind die beste Verteidigung, die Sie haben, um diese Art Angriffe zu erkennen und zu stoppen.

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.

Gast-Autor

Jen Fox *bietet als Sen. Security Consultant bei All Covered Dienstleistungen in den Bereichen Security Awareness, Social Engineering und Risk Assessment an. Sie finden sie auf Twitter als* @j_fox.

Ressourcen

Verbraucherinformationen zu Identität, Datenschutz und Online-Sicherheit:	https://www.bsi-fuer-buerger.de
Melden Sie einen Telefonbetrug:	https://www.bsi-fuer-buerger.de
Social Engineering:	https://www.sans.org/u/Fi5