OUCH! | September 2019

OUCH!

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Sie

Betrügereien über Soziale Medien

Übersicht

Viele von uns waren bereits von Phishing-E-Mail-Angriffen betroffen, entweder am Arbeitsplatz oder zu Hause. Es handelt sich hierbei um E-Mails, die legitim aussehen, wie z.B. von Ihrer Bank, Ihrem Chef oder Ihrem bevorzugten Online-Shop. Diese sind jedoch ein Angriff, der versucht, Sie zu täuschen und zu überstürzten Handlungen zu bewegen, die Sie nicht ergreifen sollten - wie das Öffnen eines infizierten E-Mail-Anhangs, das Teilen Ihres Passworts oder das Überweisen von Geld. Je besser wir diese E-Mail-Angriffe erkennen und stoppen, umso mehr beschreiten Cyberkriminelle andere Wege der Kontaktaufnahme und des Betrugs.

Versuche, Sie zu betrügen oder zu täuschen, können über fast jede Form von Kommunikation erfolgen, von Skype, WhatsApp und Slack bis hin zu Twitter, Facebook, Snapchat, Instagram oder sogar über Spiele-Apps. Die Kommunikation über diese Plattformen oder Kanäle fühlt sich informeller oder vertrauenswürdiger an, weshalb Angreifer sie gerade deshalb nutzen, um andere zu täuschen. Darüber hinaus ist es mit den heutigen Technologien für jeden Angreifer auf der ganzen Welt viel einfacher geworden, vorzutäuschen jemand anderes zu sein. Es ist wichtig sich im Klaren zu sein, dass jede Konversation möglicherweise nicht das ist, wonach sie aussieht, und die Personen nicht die sind, die sie vorgeben zu sein.

Das sollten Sie sich merken

Hier sind die häufigsten Indizien dafür, dass die gerade erhaltene Nachricht oder der gerade gelesene Beitrag ein Angriff sein kann.

Dringlichkeit: Eine Nachricht, die ein Gefühl der Dringlichkeit erzeugt, die "sofortiges Handeln" fordert, bevor etwas Schlimmes passiert, wie z.B. die Drohung, ein Konto zu schließen oder Sie ins Gefängnis zu schicken. Der Angreifer will SIe dazu bringen, übereilt einen Fehler zu machen.

Druck: Sie werden unter Druck gesetzt, um Richtlinien oder Verfahren Ihrer Organisation zu umgehen oder zu ignorieren.

Neugierde: Ein starkes Gefühl der Neugierde wird erzeugt oder etwas versprochen, das zu gut ist um wahr zu sein. Nein, Sie haben nicht in der Lotterie gewonnen.

Sensibel: Eine Anfrage nach hochsensiblen Informationen, wie z.B. Ihrer Kreditkartennummer oder Ihrem Passwort, oder nach Informationen, die Sie nicht einfach so mit anderen teilen möchten.

Offizielle Mitteilungen: Die Nachricht gibt vor, von einer offiziellen Organisation zu stammen, hat aber eine schlechte Grammatik oder Rechtschreibung. Die meisten Regierungsorganisationen werden keine offizielle Kommunikation über soziale Medien mit Ihnen führen. Wenn Sie sich nicht sicher sind, ob die Nachricht legitim ist, rufen Sie die Organisation zurück, verwenden Sie aber eine vertrauenswürdige Telefonnummer, z.B. von deren Webseite.

Nachahmung: Sie erhalten eine Nachricht von einem Freund oder Mitarbeiter, aber der Ton oder die Formulierungen klingen einfach nicht nach ihm. Wenn Sie misstrauisch sind, rufen Sie den Absender per Telefon an, um zu überprüfen, ob er die Nachricht gesendet hat. Es ist einfach für einen Cyber-Angreifer, Nachrichten zu erstellen, die scheinbar von jemandem stammen, den man kennt. In einigen Fällen können die Angreifer das Benutzerkonto Ihres Freundes übernehmen und dann vorgeben Ihr Freund zu sein und Sie kontaktieren. Beachten Sie, dass es insbesondere bei Nachrichten via SMS, Twitter und anderen Kurznachrichtendiensten schwierig ist, die Identität des Absender zu erkennen.

Sie sind die beste Verteidigung gegen Betrügereien und Angriffe wie diese. Wenn Beiträge oder Nachrichten seltsam oder verdächtig erscheinen, ignorieren oder löschen Sie diese einfach. Wenn diese von jemandem stammen, den Sie persönlich kennen, rufen Sie die Person zur Bestätigung per Telefon an.

Gastredakteur

Dr. Jessica Barker *(@drjessicabarker) ist führend auf dem menschlichen Gebiet der Cybersicherheit. Sie ist Co-CEO von Cygenta, wo sie ihrer Leidenschaft folgt, das Bewusstsein, das Verhalten und die Kultur der Cybersicherheit weltweit positiv zu beeinflussen. Sie ist Vorsitzende des ClubCISO und eine beliebte Rednerin auf Konferenzen.*

Weiterführende Informationen

Social Engineering:	https://www.sans.org/u/Uz6
Angriffe & Betrügereien mittels Telefon:	https://www.sans.org/u/Uzb
Stopp Den Phishzug:	https://www.sans.org/u/Uzg
Personalisierte Betrügereien:	https://www.sans.org/u/Uzl