Der monatliche Security Awareness Newsletter für Jedermann

Personalisierte Betrügereien

Übersicht

Cyberkriminelle entwickeln immer wieder neue und kreative Wege um Menschen zu täuschen. Eine neue Masche gewinnt dabei an Popularität - personalisierte Betrügereien. Cyberkriminelle finden oder kaufen Informationen über Millionen von Menschen und verwenden diese Informationen, um ihre Angriffe zu personalisieren. Unten zeigen wir Ihnen, wie diese Betrügereien funktionieren und führen Sie durch ein gängiges Beispiel. Je mehr Sie über diese Betrügereien wissen, desto einfacher ist es für Sie, sie zu erkennen und zu stoppen.

Wie funktioniert es?

E-Mail- oder Telefonbetrug ist nicht neu, Cyberkriminelle versuchen seit Jahren Menschen zu täuschen. Beispiele dafür sind die “Sie haben in der Lotterie gewonnen” oder die berüchtigten “Nigerianischer Prinz”-Betrügereien. Bei diesen traditionellen Vorgehensweisen wissen Cyberkriminelle jedoch nicht, wen sie ins Visier nehmen. Sie erstellen einfach eine allgemein gehaltene Nachricht und senden sie an Millionen von Menschen. Da diese Betrügereien so allgemein gehalten sind, sind sie in der Regel leicht zu erkennen. Ein personalisierter Betrug ist anders, die Cyberkriminellen recherchieren zunächst und erstellen dann eine individuelle Nachricht für jedes beabsichtigte Opfer. Sie tun dies, indem sie eine Datenbank mit den Namen, Passwörtern, Telefonnummern oder anderen Details von Personen finden oder kaufen. Diese Art von Informationen sind, aufgrund der Vielzahl in der Vergangenheit gehackter Webseiten, leicht zugänglich. Auch in Sozialen Netzen und im Internet zugänglichen Behördeninformationen sind derartige Daten abrufbar. Die Kriminellen zielen dann auf jeden, über den sie passende Informationen haben.

Ein gängiger Trick von Cyberkriminellen ist, Ihnen Angst zu machen oder Sie zu erpressen, um Sie zu zwingen, ihnen Geld zu zahlen. Der Angriff funktioniert so: Die Angreifer finden oder kaufen Informationen wie Benutzernamen und Passwörter, die von gehackten Webseiten extrahiert wurden. Sie finden Ihre Benutzerdaten in einer solchen Datenbank und senden Ihnen (und allen anderen in der Datenbank) eine E-Mail mit einigen persönlichen Daten über Sie, einschließlich des ursprünglichen Passworts, das Sie auf der gehackten Webseite verwendet haben. Die Verbrecher bezeichnen Ihr Passwort als “Beweis” dafür, dass Sie Ihren eigenen Computer oder Ihr eigenes Gerät gehackt haben, was natürlich nicht wahr ist. Die Verbrecher behaupten dann, dass, während sie Ihren Computer gehackt haben, sie Sie auch dabei erwischt haben, wie Sie sich online Pornografie ansehen. Die E-Mail droht dann, dass die Angreifer, wenn Sie die geforderte Erpressersumme nicht zahlen, die Beweise für die peinlichen Online-Aktivitäten mit Ihrer Familie und Ihren Freunden teilen.

Der Clou ist, dass die Cyberkriminellen in fast jeder Situation wie dieser gar nicht Ihr System gehackt haben. Sie wissen nicht einmal, wer Sie sind oder welche Webseiten Sie besucht haben. Die Betrüger versuchen einfach die wenigen persönlichen Daten, die sie über Sie haben, zu verwenden um Sie zu erschrecken. Sie sollen glauben, dass sie Ihren Computer oder Ihr Gerät gehackt haben, und um Sie dazu zu bringen, ihnen Geld zu zahlen. Bedenken Sie, dass böse Jungs die gleichen Techniken auch für betrügerische Telefonanrufe verwenden können.

Was soll ich tun?

Erkennen Sie, dass E-Mails oder Telefonate wie diese ein Betrug sind. Es ist ganz natürlich, Angst zu haben, wenn jemand persönliche Informationen über Sie hat. Rufen Sie sich jedoch ins Gedächtnis, dass der Absender lügt. Der Angriff ist Teil einer automatisierten Massenkampagne und kein Versuch, Sie direkt anzusprechen. Es wird für Cyberkriminelle heute viel einfacher, persönliche Informationen zu finden oder zu kaufen, also erwarten Sie in Zukunft mehr personalisierte Betrügereien wie diese. Einige Hinweise, nach denen man suchen sollte:

- **Wann immer Sie eine sehr dringende E-Mail, Nachricht oder einen Telefonanruf erhalten, seien Sie sehr misstrauisch. Wenn jemand Emotionen wie Angst oder Dringlichkeit benutzt, versucht er, Sie dazu zu bringen, einen Fehler zu machen.**
- **Wenn jemand Zahlung in BitCoin, Geschenkkarten oder anderen nicht nachvollziehbaren Methoden verlangt.**
- **Wenn Sie eine verdächtige E-Mail erhalten, suchen Sie bei Google nach dem Absender, dem Betreff oder prägnanten Teilen des E-Mail-Texts, um zu sehen, ob andere Personen ähnliche Angriffe gemeldet haben.**

Letztendlich ist der gesunde Menschenverstand Ihre beste Verteidigung. Wir empfehlen Ihnen jedoch auch, für jedes Ihrer Online-Konten immer ein eindeutiges, langes Passwort zu verwenden. Sie können sich nicht an all Ihre Passwörter erinnern? Verwenden Sie einen Passwort-Manager. Aktivieren Sie außerdem nach Möglichkeit eine zweistufige Authentisierung.

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 Sicherheit spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gast-Autor

Lenny Zeltser *ist ein Veteran der Cybersicherheit. Er entwickelt Anti-Malware-Lösungen in den Minerva Labs und leitet verschiedene Kurse für das SANS Institute. Seine Erfahrung umfasst auch Managed Security Services und Consulting. Folgen Sie ihm auf* zeltser.com/blog *und auf Twitter* @lennyzeltser.

Weiterführende Informationen

Social Engineering:	https://www.sans.org/u/MUU
Stopp den Phishzug:	https://www.sans.org/u/MUZ
Suchen Sie sich selbst online:	https://www.sans.org/u/MV4
Passwort-Manager:	https://www.sans.org/u/MV9