OUCH!

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

# Ja, Sie sind ein Ziel

## Übersicht

Viele Menschen glauben fälschlicherweise, dass sie kein Ziel von Cyber-Angreifern sind: dass sie, Ihre Systeme oder Konten keinen Wert haben. Das könnte nicht weiter von der Wahrheit entfernt sein. Wenn Sie Technologie in irgendeiner Weise einsetzen - ganz gleich ob am Arbeitsplatz oder zu Hause, glauben Sie uns - Sie haben Wert für Kriminelle. Aber das Glück ist auf Ihrer Seite: Sie haben bereits die beste Verteidigung, die es gegen diese Cyberangriffe gibt - Sich selbst.

## Warum Sie ein Ziel sind

Es gibt heutzutage viele Cyber-Angreifer im Internet, und sie alle haben unterschiedliche Motive. Warum sollte einer von ihnen ausgerechnet Sie angreifen wollen? Weil sie ihrem Ziel näher kommen, indem sie Sie hacken. Hier sind zwei gängige Beispiele für Cyber-Angreifer und warum sie Sie ins Visier nehmen würden:

⚠ **Cyberkriminelle:** Diese Typen sind darauf aus, so viel Geld wie möglich zu verdienen. Das Internet ist für sie so wertvoll, da sie jetzt mit nur einem Knopfdruck Opfer auf der ganzen Welt erreichen können. Und es gibt VIELE Möglichkeiten, wie sie mit Ihnen Geld verdienen können. Beispiele dafür sind der Diebstahl von Bank- oder Rentenkonten, die Erstellung einer Kreditkarte in Ihrem Namen und auf Ihre Rechnung, die Verwendung Ihres Computers zum Hacken anderer Personen oder das Hacken Ihrer Social Media- oder Spielekonten und deren Verkauf an andere Kriminelle. Die Liste ist fast endlos, wie böse Jungs mit Ihnen Geld verdienen können. Es gibt Hunderttausende davon, die jeden Morgen mit dem Ziel aufwachen, so viele Menschen wie möglich zu hacken, Sie eingeschlossen.

☆ **Gezielte Angreifer:** Dies sind hochqualifizierte Cyber-Angreifer, die oft für Regierungen, Verbrechersyndikate oder Konkurrenten arbeiten, und die Sie beruflich ins Visier nehmen. Sie werden vielleicht das Gefühl haben, dass Ihr Job nicht viel Interesse erregen würde, aber Sie werden sehr überrascht sein.

- Die Informationen, mit denen Sie beruflich zu tun haben, stellen einen enormen Wert für gezielte Angreifer.
- Die Daten, mit denen Sie arbeiten, können Sie im beruflichen Umfeld angreifen, nicht weil sie Sie hacken wollen, sondern um Sie zu benutzen, um einen Ihrer Kollegen oder andere Systeme zu hacken.
- Berufliche Beziehungen zu anderen Unternehmen machen Sie zu einem attraktiven Ziel!

## Ich nutze Anti-Virus, ich bin sicher.

Okay, also bin ich ein Ziel, kein Problem. Ich installiere einfach einen Virenschutz und eine Firewall auf meinem Computer und bin geschützt, richtig? Nun, leider nicht. Viele Menschen haben das Gefühl sicher zu sein, wenn sie nur einige Sicherheitswerkzeuge installieren. Leider ist das nicht ganz richtig. Cyber-Angreifer werden immer besser, und viele ihrer Angriffsmethoden umgehen heute problemlos Sicherheitstechnologien. Beispielsweise erstellen sie oft spezielle Schadprogramme, die Ihr Antivirus nicht erkennen kann. Sie umgehen Ihre E-Mail-Filter mit einem individuellen Phishing-Angriff oder rufen Sie am Telefon an und überlisten Sie oder entlocken Ihnen Ihre Kreditkarte, Ihr Geld oder Ihr Passwort. Technologie spielt für Ihren Schutz eine wichtige Rolle, aber letztendlich sind Sie die beste Verteidigung.

Glücklicherweise ist es nicht so schwer, sicher zu sein, denn letztendlich sind gesunder Menschenverstand und einige grundlegende Verhaltensweisen Ihr zuverlässigster Schutz. Wenn Sie eine E-Mail, Nachricht oder einen Anruf erhalten, die extrem dringend, seltsam oder verdächtig klingt, kann es sich um einen Angriff handeln. Um sicherzustellen, dass Ihre Computer und Geräte sicher sind, halten Sie sie auf dem neuesten Stand, und aktivieren Sie die automatische Aktualisierung. Verwenden Sie eine starke, eindeutige Passphrase für jedes Ihrer Konten. Sicherheitsbewusst zu bleiben, ist letztendlich Ihre beste Verteidigung. Sie sind sich nicht sicher, wo Sie anfangen sollen? Erwägen Sie, den monatlichen OUCH! Newsletter unter sans.org/ouch zu abonnieren.

## 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

***Matt Bromiley*** *(@mbromileyDFIR) ist ein Incident Responder und Experte für Digitale Forensik mit über 8 Jahren Erfahrung und hat mit Organisationen in Vorfällen auf der ganzen Welt zusammengearbeitet. Matt ist auch Trainer für Digital Forensic und Incident Response und unterrichtet die SANS Kurse FOR508 sowie FOR572.*

## Ressourcen

| | |
|---|---|
| Stoppen Sie Malware: | https://www.sans.org/u/L1J |
| Social Engineering: | https://www.sans.org/u/L1O |
| Angriffe & Betrügereien mittels Telefon: | https://www.sans.org/u/L1T |
| Passphrasen: | https://www.sans.org/u/L1Y |
| Poster - Sie sind ein Ziel (englisch): | https://www.sans.org/u/L23 |