proofpoint™

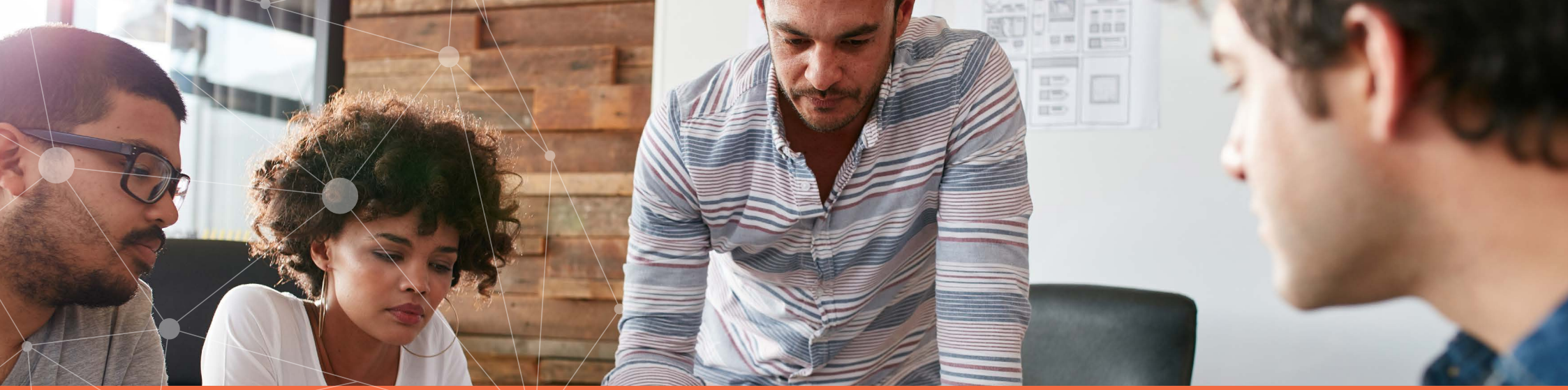
DAS CREDENTIAL-PHISHING-HANDBUCH:

Warum Phishing immer noch funktioniert und wie man es mit 4 Schritten verhindern kann

EINFÜHRUNG

Phishing gibt es zwar schon seit über 20 Jahren, aber noch heute macht es mehr als 90 % aller gezielten Angriffe aus. Der Grund ist einfach: es funktioniert.

Einer von etwa vier Benutzern öffnet eine empfangene Phishing-E-Mail. Was noch alarmierender ist: Mehr als 10 % klicken auf einen schädlichen Link oder öffnen einen gefährlichen Anhang in der Phishing-E-Mail. Das bedeutet, dass ein Hacker nur 10 Nachrichten verschicken muss, um mit 90-%iger Wahrscheinlichkeit einen Anwender an den Haken zu kriegen und zu schädigen. Laut Ponemon-Institut verlieren Organisationen mittlerer Größe jedes Jahr im Schnitt 3,7 Millionen USD durch Phishing-Betrügereien. Und das sind nur die materiellen Kosten.



WIE PHISHING FUNKTIONIERT: TRENDS UND TAKTIKEN

Während andere Cyberattacken technisch gesehen fortschrittlicher geworden sind, ist das Phishing heute erwachsener in der Art und Weise, wie es das menschliche Verhalten ausnutzt. Die Angriffe überwinden herkömmliche Filter und gelangen in die Posteingänge von Unternehmen. Und ganz gleich, ob die Anwender in Aufmerksamkeitstrainings geschult wurden – geklickt wird immer. Wir beobachten vier wesentliche Trends bei Phishing-Angriffen:

GETARNT ALS IT-ABTEILUNG DES ZIELANWENDERS

BESTIMMTE ANWENDER UND ABTEILUNGEN IM VISIER

DOKUMENTE MIT EINGEBETTETEN SCHÄDLICHEN MAKROS

ZUSAMMENWIRKEN MIT WATERING-HOLE-ATTACKEN

ZIELPERSONEN: BEWEGLICHE ZIELE

Hacker sind auf Profit aus: Zahlungs- und Finanzdienstleister machen 40 % der Opfer gezielter Phishing-Angriffe aus. Internet-Dienstanbieter gehören ebenfalls zu den beliebteren Zielen, da manipulierte Domain-Namen und Hosting-Services für künftige Attacken genutzt werden können.

Wenngleich ein Angreifer Phishing-E-Mails zu allen möglichen Adressen einer Organisation verschickt, schwankt die Kick-Rate je nach Abteilung und Posten. Überraschenderweise gehören einige der pflichtbewusstesten Angestellten mit zu den klickfreudigsten – insbesondere dann, wenn die Phishing-E-Mail an ihren Sinn für Dringlichkeit, Effizienz und Ordnung appelliert.

Die „Angler“ verdienen auf verschiedene Art und Weise am Phishing. Manche verkaufen gestohlene Anmeldedaten. Andere handeln mit vertraulichen Dokumenten. Und es gibt Hacker, die gestohlene Anmeldedaten für betrügerische Finanztransaktionen missbrauchen.

GRÜNDE FÜR DEN ERFOLG VON PHISHING-ATTACKEN: IRREN IST MENSCHLICH

Angreifer arbeiten mit allen möglichen Tricks, um ihre schadhaften Links und Dokumente durch die Filter und Firewalls zu schleusen, die sie vom Zugang abhalten sollen. Hier sind einige Beispiele:

ÜBERWINDEN DER FILTER MIT SCHNELL VERÄNDERLICHEN URLS UND DOMAINS

sowie erheblich kleineren Kampagnen, die keine Spam-Kontrollen auslösen

NACHAHMUNG VON FREUNDEN UND KOLLEGEN

GROSS ANGELEGTE SOCIAL-ENGINEERING-RECHERCHE UNTER RÜCKGRIFF

auf öffentliche Informationen, um überzeugende E-Mails zu erstellen

NACHAHMUNG VON URLS UND WEBSITES

SO STOPPEN SIE PHISHING-ATTACKEN: EMPFEHLUNGEN

Ihre Mitarbeiter sind jetzt das primäre Ziel der Exploits. Sie müssen sie in der Art und Weise schützen, in der sie arbeiten. Und Sie müssen Ressourcen und Risiken erkennen, bevor es sie trifft. Hier einige Empfehlungen zur Bekämpfung von Phishing-Attacken:

REDUZIEREN SIE DIE ANGRIFFSFLÄCHE.

Stellen Sie Tools bereit, die Nachrichten, URLs, Anhänge und Anwender-klicks mithilfe statischer Codes und dynamischer Verhaltenstechniken überwachen und analysieren.

BAUEN SIE IHRE ABWEHR

mit cloudbasierten Abwehrmechanismen aus, die Ihre Mitarbeiter schützen – wo immer sie arbeiten.

NUTZEN SIE DIE VORTEILE VON BIG DATA UND MASCHINELLEN LERNTECHNIKEN,

um aufkommende und bis dato unbekannte Attacken vorbeugend abzufangen – bevor der Benutzer klickt.

SCHAFFEN SIE SICH TRANS-PARENTERE EINBLICKE

Einblicke in Ihre Umgebung und in die Bedrohungslage als Ganzes. Mit Threat Intelligence in Echtzeit und einer Sicht auf die Aktivitäten, von denen Ihre Systeme bedroht sind, können Sie schneller reagieren und die Betriebsbereitschaft wiederherstellen. Stellen Sie Tools bereit, die Ihnen vermitteln, wer durch welche Bedrohung gefährdet ist, welche Bedrohungen Ihre Abwehr überwunden haben und wer davon betroffen ist.

MODERNER E-MAIL-SCHUTZ MUSS AUF IHRE ARBEITS-PROZESSE ABGESTIMMT SEIN

Bei der steigenden Menge sensibler und vertraulicher Informationen – und der expandierenden Angriffsfläche der Geräte, Cloud-Apps und mobiler Standorte – können Sie es sich nicht mehr leisten, sich auf herkömmliche Abwehrmechanismen zu verlassen. Innovative, neue Tools operieren inmitten des Workflows, wo sie URLs und Anhänge überwachen, Threat Intelligence-Informationen in Echtzeit teilen und Benutzeraktivitäten innerhalb wie außerhalb Ihres Firmennetzes beobachten.

Mit Targeted Attack Protection können Sie diese Bedrohungen erkennen, sie abschwächen und darauf reagieren, bevor sie zu einer Gefahr werden.

Um mehr darüber zu erfahren, wie Proofpoint Ihnen dabei helfen kann, Credential-Phishing zu unterbinden, laden Sie unser Whitepaper, Haken, Leine und Senkblei: Neue Strategien der Credential-Phisher – und wie Sie sich wehren können auf www.proofpoint.com/de herunter.

ÜBER PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führender Sicherheits- und Compliance-Anbieter der nächsten Generation, der cloudbasierte Lösungen zum Schutz vor Bedrohungen sowie für Compliance, Archivverwaltung und sichere Kommunikation vertreibt. Unternehmen in aller Welt verlassen sich auf die umfangreichen Kenntnisse, patentierten Technologien und On-Demand-Bereitstellungssysteme von Proofpoint. Proofpoint schützt vor Phishing, Malware und Spam und unterstützt gleichzeitig die Datensicherheit, die Verschlüsselung sensibler Daten sowie die Archivierung und Verwaltung von Nachrichten und wichtigen Unternehmensdaten.

Weitere Informationen finden Sie unter www.proofpoint.com/de

© Proofpoint, Inc., 2016. Proofpoint ist eine Marke der Proofpoint, Inc. in den USA und anderen Ländern. Alle anderen aufgeführten Produkt- und Firmennamen sind Eigentum ihrer jeweiligen Inhaber.