Phishing und Spam

Definition Phishing

- Phishing (Neologismus „fishing“, engl. Für „Angeln“), „ph“ stammt vom damaligen Begriff „phreaking“ (Hacker Subkultur, die sich mit Sicherheitsmechanismen der Telefonsysteme beschäftigte)
- Definition nach APWG:
  - Phishing ist eine kriminelle Handlung, bei der sowohl Social Engineering als auch technische Tricks eingesetzt werden, um personenbezogene Daten und Zugangsdaten für Finanzkonten zu stehlen.
  - Phishing nutzt unvorsichtige Opfer aus, indem sie diese glauben lässt, dass sie es mit einer vertrauenswürdigen und legitimen Partei zu tun haben. Z.b. durch die Verwendung von irreführenden E-Mail-Adressen und Nachrichten.
  - Diese Nachrichten führen den Verbraucher jedoch zu gefälschten Websites, die den Empfänger zur Preisgabe von Informationen, so wie Benutzernamen und Passwörtern auffordern.
  - Technische Täuschungsmanöver können Malware auf den Computer einschleusen, um Anmeldedaten direkt zu stehlen. Häufig werden Systeme eingesetzt, die Benutzernamen und Passwörter von Verbraucherkonten abfangen oder den Vebraucher auf gefälschte Websiten umleiten.

Definition Social Engineering

- Wikipedia: „**Social Engineering** [ˈsəʊʃl̩ ˌɛndʒɪˈnɪəɹɪŋ] (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. “

Definition Spam

- Wikipedia: „Als **Spam** […]werden unerwünschte, in der Regel auf elektronischem Weg übertragene massenhafte Nachrichten (Informationen) bezeichnet, die dem Empfänger unverlangt zugestellt werden, ihn oft belästigen und auch häufig werbenden Inhalt enthalten.“

Phishing

- Hat 3 Bestandteile:
  - Medium
  - Vektor
  - Technischer Ansatz
- Medium: Internet, Voice oder „short messaging services“ SMS
- Vektor:
  - Fürs Internet: E-Mail, Webseiten oder Social Media
  - Für Voice: Anrufe
- Technischer Ansatz:
  - Social Engineering
  - Malware basiertes Phishing

Phishing

- Täuschung durch: E-Mail Spoofing, Webseiten Spoofing und Nachbildung der E-Mail/Webseite
- E-Mail Spoofing:
  - Manipulation des „Von“-Feldes
  - Ausnutzung offener SMTP-Server, einige überprüfen Sender und E-Mail nicht
- Webseiten Spoofing:
  - Verwendung ähnlicher Zeichen z.B lateinisches „a“ und kyrillisches „a “
  - Nutzung von Subdomains: echter Domainname als Subdomain einer anderen
  - Verwendung von URL-Verkürzern
  - Tippfehler ausnutzen
- Nachbildung:
  - Durch Verwendung des HTML-Source Codes und mit Tools wie GoPhish können E-Mail-Formate und Webseiten einfach geklont werden

Phishing Life cycle

- Phisher erstellt phishing Webseite, imitiert die legitime Webseite
- Phisher versendet phishing Link an Opfer via Spam
- Opfer verwendet den Link und gibt seine Daten ein
- Phisher erhält Zugangsdaten des Opfers
- Phisher verwendet diese für eigene Zwecke

Arten von Phishing

- „normales“ Phishing
- Spear Phishing
- Whaling

„normales“ Phishing

- Typischerweise ist die Zielgruppe sehr groß, Ziele: Kunden großer Unternehmen
- Imitation z.B. von Google, PayPal oder Banken
- Opfer erhalten Mails, dass sofort über einen gegebenen Link oder Anhang Aktionen durchgeführt werden müssen
- Anderer Ansatz: Opfer erhält eine positive Mail, wie eine Paketzustellung oder Überweisung

Spear Phishing

- Personalisierte Phishing Angriffe
- Meist auf ein Unternehmen oder spezifische Person im Unternehmen
- Verlangt eine gründliche Recherche über Unternehmen und Ziel
- Meist erfolgreicher als „normales Phishing“, Aufwand aber größer

Whaling

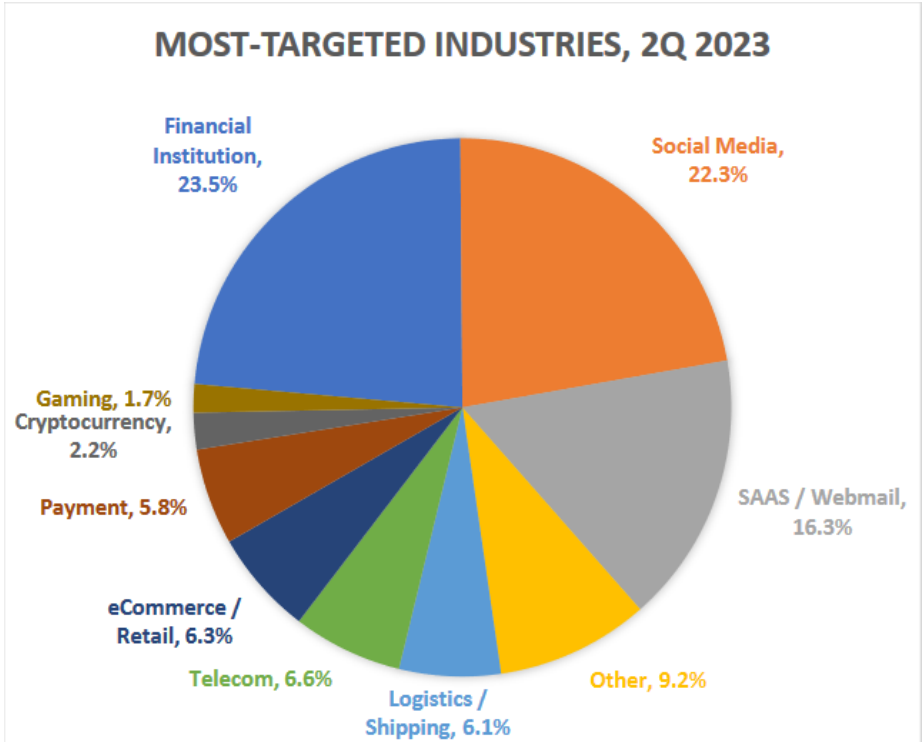
- Ziele sind hochrangige oder einflussreiche Person in einem Unternehmen („große Fische“, „Wale“)
- Phisher gibt sich als andere hochrangige Person aus
- Dadurch entsteht Druck für das Opfer

Weitere Konzepte

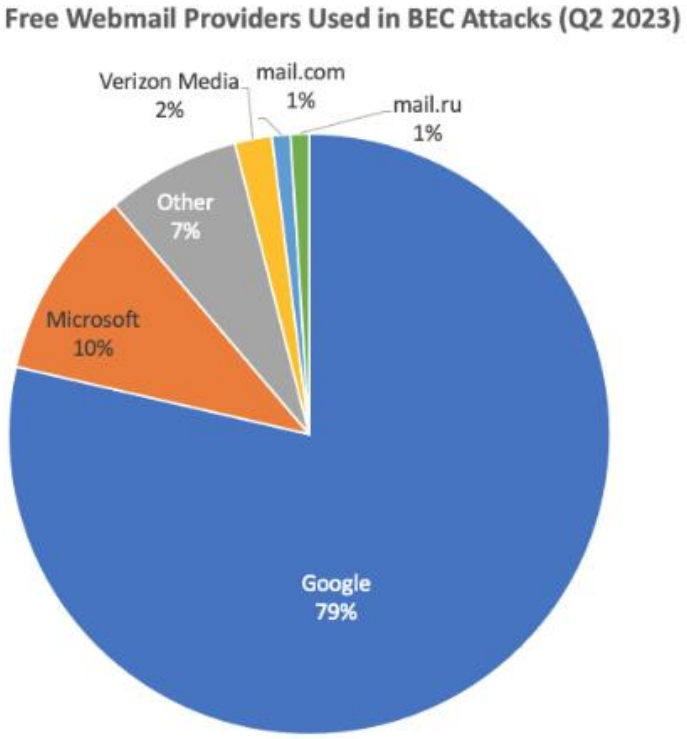
- Vishing oder Voice Phishing: Opfer wird via Telefonat aufgefordert sensible Daten preiszugeben oder direkt veranlasst bestimmte Aktionen wie Überweisung durchzuführen
- Phishing via SMS: Betrüger senden automatisiert SMS an große Gruppen von Zielen
  - Ziele werden aufgefordert einen Link anzuklicken
  - Link führt entweder zu Phishing Webseiten oder dubiosen Downloads
  - Wird oft verwendet für das Phishing nach Homebanking Daten

Trends

- Dienste im Finanziellen Bereich, z.B PayPal oder Banken sind beliebte Ziele



Phishing Activity Trends Report
2nd Quarter 2023
w w w . a p w g . o r g



Free Webmail Providers Used in BEC Attacks (Q2 2023)

Trends

- Analyse Statistik von IT-Sicherheitsunternehmen Checkpoint

Platz	Marke	Anteil in %
1	DHL	22
2	Microsoft	16
3	LinkedIn	11
4	Google	6
5	Netflix	5
6	WeTransfer	5
7	Walmart	5
8	WhatsApp	4
9	Bank HSBC	4
10	Instagram	3

Top 10 Unternehmensziele 2022
https://www.heise.de/news/DHL-ist-Phishers-Liebling-7321731.html

1 Microsoft (29%)
2 Google (19.5%)
3 Apple (5.2%)
4 Wells Fargo (4.2%)
5 Amazon (4%)
6 Walmart (3.9%)
7 Roblox (3.8%)
8 LinkedIn (3%)
9 Home Depot (2.5%)
10 Facebook (2.1%)

Top 10 Unternehmensziele 2023
https://www.checkpoint.com/press-releases/microsoft-dominates-as-the-most-impersonated-brand-for-phishing-scams-in-q2-2023/

Maßnahmen gegen Phishing

- E-Mail-Clients:
  - Spamfilter: viele E-Mail-Provider filtern die meisten Spam E-Mails raus
  - Blacklists: Verwendung von Listen bekannter Phishing Quellen z.B PhishTank
  - Domain-Authentifizierung
  - Link- und Anhang-Analyse: scannen nach potenziellen Bedrohungen
- Schulung und Sensibilisierung: regelmäßige Tests durch interne oder externen Phishing Kampagnen

Übung

- Unter https://github.com/daigiat/Phishing-Uebung.git können Sie sich die Übung und benötigte Dateien auf die Kali VM herunterladen.

Quellenverzeichnis

- https://apwg.org/trendsreports/
- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/E-Mail-Phishing-Bankbetrug/email-phishing-bankbetrug_node.html
- https://www.checkpoint.com/press-releases/microsoft-dominates-as-the-most-impersonated-brand-for-phishing-scams-in-q2-2023/
- https://www.fortinet.com/resources/cyberglossary/email-spoofing
- https://getgophish.com/documentation/
- https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/pdf
- https://www.heise.de/news/DHL-ist-Phishers-Liebling-7321731.html
- http://www.ijarcs.info/index.php/Ijarcs/article/view/2706/2694
- https://www.kaspersky.de/resource-center/definitions/spear-phishing#:~:text=Die%20Antwort%20lautet%20Spear%2DPhishing,bestimmte%20Personen%20oder%20Unternehmen%20abzielen
- https://de.wikipedia.org/wiki/Vishing