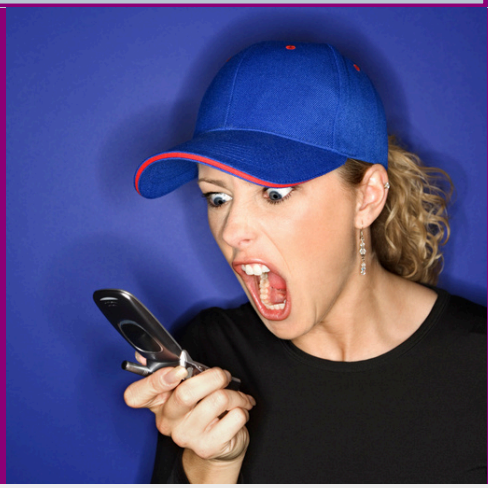
SECURITY TAKE AWAY

powered by S@ND

Was ist schlimmer als Phishing? Smishing!
Gefahr für Mobilgerätenutzer - Was steckt dahinter?

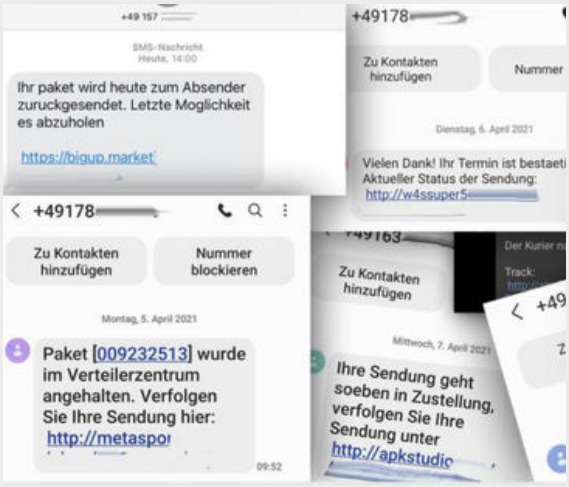
Unser heutiges Thema zeigt, wie wir einigen perfiden Angriffsvarianten ausgeliefert sind. Cyberkriminelle haben es in diesem Fall darauf abgesehen, Ihre persönlichen Daten zu stehlen. Technische Schutzmöglichkeiten? Fehlanzeige!

Wenn man sich technisch also nicht schützen kann - WIE DANN?



Erfahren Sie in diesem TAKE AWAY mehr darüber, wie Sie selbst den entscheidenden Unterschied machen und was unser Bauch damit zu tun hat.

SMISHING - WAS IST DAS NUN?



Smishing ist eine Abwandlung des herkömmlichen Phishings und zielt auf die Textnachrichten mobiler Nutzer. Der Name setzt sich aus **SM**S und Ph**ishing** zusammen. Dabei wird die persönliche und unmittelbare Natur von SMS ausgenutzt.

Insbesondere 3 Faktoren bringen den Erfolg:

1. **Vertrauen**
2. **Kontext** und
3. **Emotion**

Cyberkriminelle missbrauchen Ihr **Vertrauen**, indem sie sich als vertrauenswürdige Akteure ausgeben. Sie erzeugen durch einen realistischen und relevanten **Kontext** eine persönliche Ansprache und appellieren mit **emotionalen** Nachrichten an die Impulsivität der Empfänger, um schnelle, unreflektierte Handlungen zu erzwingen. Der Empfänger soll dazu verleitet werden, einen URL-Link in der Nachricht zu öffnen, der ihn auf eine Phishing-Seite führt. Dort wird er aufgefordert persönliche Daten einzugeben. Diese Eingabemaske befindet sich oft auf einer gefälschten Webseite oder App, die täuschend echt einem seriösen Original nachempfunden ist.

Da die Abwehrmaßnahmen gegen E-Mail-Betrug immer besser werden, weichen die Cyberkriminellen auf diesen weniger geschützten Kommunikationskanal aus. Der Wechsel stellt eine moderne Variante einer uralten Täuschung da, die für eine digitale, vernetzte Welt optimiert wurde.

Quellen:
Verbraucherzentrale, Paketdienst-SMS: Vorsicht, Abzocke! in Verbraucherzentrale.de, https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/paketdienstsms-vorsicht-abzocke-58988, letzter Zugriff: 11.12.2024
SANS, A Tale of the Three *ishings: Part 02 – What is Smishing? in sans.org, https://www.sans.org/blog/a-tale-of-the-three-ishings-part-02-what-is-smishing/, letzter Zugriff: 11.12.2024
FORTRA, 7 smishing examples and how to protect yoursef in terranovasecurity.com, https://www.terranovasecurity.com/blog/smishing-examples, letzter Zugriff: 11.12.2024

SMISHING - WARUM WIRD ES IMMER POPULÄRER?

Ein Smishing-Angriff ist dann erfolgreich, wenn der Angreifer Ihre Daten für den ursprünglich beabsichtigten Diebstahl verwenden konnte. Das Ziel kann dabei beispielsweise sein, Ihr Bankkonto zu leeren, Ihre Identität zu stehlen, um illegal ein Kreditkartenkonto zu eröffnen, oder vertrauliche Unternehmensinformationen zu veröffentlichen.

Für Unternehmen ist es schwierig, mobile Geräte zu sichern. Die Sicherheitsteams haben durch Policies wie BYOD oft keine Kontrolle über die mobilen Endgeräte der Mitarbeiter. Hinzu kommt, dass Privatpersonen eine unglaublich große Angriffsfläche für Smishing bieten. Darunter fallen z. B. Nachrichten von Paketzustellern, Banken oder anderen wohlbekannten Diensten.

Auch für gemanagte Geräte gilt: **Es gibt wenige bis keine technischen Sicherheitskontrollen, die Smishing-Angriffe effektiv erkennen und filtern.** Wenn ein Cyberangreifer eine Smishing-SMS an seine Opfer sendet, ist es sehr wahrscheinlich, dass diese Nachricht ankommt und nicht gefiltert wird.
Textnachrichten sind in der Regel viel informeller als E-Mails. Somit neigen Menschen dazu, Textnachrichten zu vertrauen und darauf zu reagieren.

Zusammengefasst:
SMS ist kaum kontrollierbar und Angreifer sind nur schwer erkennbar. Die Gefahr, Opfer eines Smishing Angriffs zu werden ist deutlich erhöht.

SMISHING - EIN LUKRATIVES GESCHÄFTSMODELL

Laut einer gemeinsamen Umfrage von Enea und GSMA's Mobile World Live mit dem Titel „Mobile Network Security: Bridging the Gap Between Enterprise Needs and CSP Capabilities“ (Überbrückung der Kluft zwischen den Bedürfnissen der Unternehmen und den Fähigkeiten der Netzbetreiber), halten fast zwei Drittel (61 %) der Unternehmen die Kosten des Mobilfunkbetrugs für ‚erheblich‘.

Einem Bericht der U.S. Federal Trade Commission zufolge kosteten Smishing-Betrügereien die US-Verbraucher im Jahr 2022 mehr als 330 Millionen Dollar. Oft decken die Unternehmen einige, wenn nicht sogar alle dieser Verluste.
Dies gilt auch für viele andere Gebiete. So musste beispielsweise die Bank OCBC in Singapur im Jahr 2022 13,7 Mio. S$ (10,2 Mio. US$) an über 790 Opfer eines Smishing-Angriffs zahlen und die Zentralbank von Singapur forderte das Unternehmen auf, 330 Mio. S$ (240 Mio. US$) an Kapital für operationelle Risiken bereitzustellen.

Der gesamte Bereich des Telefonbetrugs (Spam und Scam Anrufe) hat in den USA einen Schaden von unglaublichen 25,4 Milliarden $ verursacht!

Quellen:
ENEA, How are Leading CSPs Turning the Need for Security Into a Revenue Opportunity? in enea.com, https://www.enea.com/insights/two-thirds-of-enterprises-endure-significant-losses-to-mobile-fraud-in-2024/, letzter Zugriff 11.12.2024
truecaller, The True Cost of Spam and Scam Calls in America in truecaller.com, https://www.truecaller.com/blog/insights/the-true-cost-of-spam-and-scam-calls-in-america, letzter Zugriff: 11.12.2024

NICHTS HILFT?AUFMERKSAMKEIT HILFT IMMER!

Wenn man sich technisch nicht schützen kann, wie dann?

Awareness, wie in diesem Fall durch unseren TAKE AWAY, ist das A und O. Ein Angreifer kann nur dann Schaden anrichten, wenn Sie den Köder schlucken. Das heißt, der beste Schutz besteht darin, aufmerksam zu sein und sich nicht zu einer spontanen Reaktion hinreißen zu lassen.

Jeder von Ihnen hat bereits, wenn auch nur unterbewusst, jahrelange Erfahrung mit diesem Thema durch Phishingmails. Hier verwenden die Angreifer die selben Tricks.
Denken Sie immer daran, dass es darum geht, Sie hinters Licht zu führen. Kriminelle verlassen sich darauf, dass Sie mitspielen und auf einen Link klicken oder Informationen preisgeben.

Das sollten Sie beachten:

- Der Angreifer wird versuchen, **Zeitdruck** zu vermitteln. Lassen Sie sich Zeit!
- Vertrauen Sie keinen **unbekannten Nummern**, vor allem aus dem Ausland.
- Falls Sie aufgefordert werden zu antworten, kann dies ein Versuch des Angreifers sein, Ihre Nummer zu verifizieren.
- Vertrauen Sie keinen **verkürzten URLs** wie z. B. bit.ly/xyz. Falls Sie sich unsicher sind, besuchen Sie die **Webseite** der Firma **manuell über den Browser**, anstatt über den angebotenen Link.
- Verwenden Sie **MFA** wenn möglich, auch privat. Wir haben darüber in unserem letzten NetDescribe Security TAKE AWAY #2 - Passwörter und Multi-Faktor-Authentifizierung berichtet.
- **Zu schön, um wahr zu sein?** Leider haben Sie keine Tickets fürs Champions League Finale bei einem Ihnen unbekannten Gewinnspiel gewonnen 😢 Finger weg!
- Und damit wären wir bei Ihrem **Bauchgefühl**. Hören Sie darauf!
- Speichern Sie möglichst **keine Kreditkarteninformationen** auf Ihrem Telefon. Was nicht da ist, kann auch nicht gestohlen werden.
- Geben Sie **niemals** ein **Passwort oder** einen **Wiederherstellungscode** für Ihr Konto weiter.

WAS TUN, WENN SIE DOCH ZUM OPFER WERDEN?

1. **Melden** Sie den eventuellen Angriff an die zuständigen Behörden.
2. **Sperren** Sie die möglicherweise betroffenen Karten.
3. **Ändern** Sie alle vielleicht betroffenen Passwörter und Konto PINs.
4. **Kontrollieren** Sie, ob es ungewöhnliche Anmeldungen oder Aktivitäten gibt.

Sie wollen mehr zum Thema IT Security wissen? Kontaktieren Sie uns. Wir freuen uns darauf, Sie persönlich zu beraten.

NETDESCRIBE
Member of xantaro group

CALL FOR APPOINTMENT

089 215 48 68 0

info@netdescribe.com