Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Verhindern von Phishing und Malware“

Mehr als 90 % der Cyberangriffe beginnen mit einer Phishing-E-Mail. Beim Phishing soll Menschen der Eindruck vermittelt werden, dass sie es mit einer vertrauenswürdigen Entität zu tun haben. So wollen sich Kriminelle Zugriff auf sensible Daten oder Geld verschaffen.

Phishing bezieht sich in der Regel auf Kommunikation per E-Mail, Smishing auf SMS und Vishing auf Anrufe. Es gibt viele verschiedene Arten von Phishing, beispielsweise:

- **Phishing**: Dies ist in der Regel nicht zielgerichtet. Es werden Massen-E-Mails versendet, die den Anschein erwecken, von seriösen Organisationen zu stammen. Sie können sich auf aktuelle Nachrichten oder das Steuerjahr beziehen oder den Anschein erwecken, von bekannten, häufig genutzten Anbietern zu stammen, in der Hoffnung, dass viele Empfänger antworten.
- **Spear-Phishing**: Dies erfolgt gezielter. Die E-Mail ist so gestaltet, als ob sie von einer Person oder Organisation stammt, die dem Opfer bekannt ist. Dazu ist etwas Recherche über das beabsichtigte Opfer nötig. Häufig verfolgt der Angreifer ein spezielles Ziel.
- **Whaling**: Dies erfolgt ganz gezielt, oft gegen sehr hochrangige Personen innerhalb einer Organisation. Dazu müssen die Kriminellen das Opfer in aller Regel auskundschaften und dabei über Monate Bewegungsmuster nachverfolgen und Daten sammeln, bevor sie den Angriff starten. Üblicherweise haben sie dabei ein ganz konkretes Ziel.

Sobald sich die Nachricht in Ihrem Posteingang befindet, hofft der Angreifer darauf, dass Sie auf einen Link klicken oder den Anhang öffnen, wodurch die beabsichtigte Aktivität ermöglicht wird:

- **Malware**: Ein allgemeiner Begriff für verschiedene Arten von bösartiger Software:
    - **Virus**: Vermehrt und verbreitet sich selbst über einen Host. Er kann sich an ein legitimes Programm oder eine legitime Datei anhängen und wird aktiviert, sobald das Programm das nächste Mal ausgeführt wird.
    - **Wurm**: Vermehrt und verbreitet sich selbst über Netzwerkverbindungen. Er kann sich z. B. in einem Anhang verstecken und sich dann selbst per E-Mail an alle Kontakte in Ihrem E-Mail-Adressbuch versenden.
    - **Trojaner**: Vermehrt sich nicht. Er tarnt sich als nützliches, legitimes Programm (z. B. als Bildschirmschoner) und verursacht währenddessen Schäden im Hintergrund.

Beispielsweise kann eine **Hintertür** geschaffen werden (ein geheimer Zutrittspunkt zum Computer für die spätere Verwendung), Daten können beschädigt und **Spyware** (zur Nachverfolgung Ihrer Aktivitäten und zum Abrufen personenbezogener Informationen) oder **Ransomware** (zum Sperren Ihrer Daten, die Sie nur gegen Zahlung eines Lösegelds zurückerhalten) installiert werden.

Phishing-E-Mails sind NICHT leicht zu erkennen.

- Sie können aussehen, als stammten sie von jemandem, den Sie kennen.
- Sie nutzen möglicherweise genau dieselbe E-Mail-Adresse wie jemand, den Sie kennen.
- Sie können die Logos und das Format von E-Mails von bekannten Unternehmen imitieren.
- Sie können sich auf aktuelle Nachrichten oder einen Auftrag beziehen, den Sie gerade ausgeführt haben.
- Der Angreifer hat möglicherweise bei Ihrem Unternehmen angerufen oder online nachgesehen, um die E-Mail zu personalisieren und sie noch „legitimer“ wirken zu lassen.

Angreifer werden alles versuchen, damit E-Mails echt und ansprechend aussehen – sie sind sehr geübt darin.

Die Folgen sind für Einzelpersonen und Unternehmen gleichermaßen schwerwiegend. Mehrere Studien zeigen, dass kleine Unternehmen sehr gefährdet sind. Mehr als 60 % der KMU wurden mit großer Wahrscheinlichkeit im vorangegangenen Jahr Opfer eines Cyberangriffs, wobei E-Mails der am häufigsten verwendete Initiator (Angriffsvektor) sind.

Antiviren-Software
Schützt vor einer Infektion, indem nach charakteristischen Merkmalen von Viren gesucht wird (auch als Signaturen bezeichnet). Wenn ein Virus erkannt wird, wird er blockiert und die Datei bereinigt. Angreifer entwickeln kontinuierlich neue Virenstämme, um Antiviren-Software zu umgehen. Wenn neue Viren veröffentlicht werden, dauert es eine Weile, bis die Merkmale identifiziert und die Viren blockiert werden können. Angriffe mithilfe neuer Viren, für die es noch keine Abwehrmaßnahmen gibt, werden als Zero-Day-Angriffe bezeichnet.

Antiviren-Software kann auch nach ungewöhnlichem Benutzerverhalten Ausschau halten (bekannt als Heuristik). Die Software lernt Ihre üblichen Verhaltensmuster kennen und wird misstrauisch, wenn außergewöhnliche Aktivitäten stattfinden (z. B. wenn Sie sich zu einem ungewöhnlichen Zeitpunkt an einem System anmelden).

Es ist wichtig, Antiviren-Software auf dem neuesten Stand zu halten. Angreifer entwickeln kontinuierlich neue Viren.

- *Sorgen Sie dafür, dass auf allen Computern und Mobilgeräten Echtzeit-Antiviren-Software installiert ist.*
- *Führen Sie regelmäßige Scans aller Systeme durch.*

DNS-Filtering (Domain Name Filtering)
Bei der Einrichtung neuer Websites gelten allgemeine Geschäftsbedingungen, die sicherstellen sollen, dass diese für legitime Zwecke genutzt werden. Kriminelle ignorieren diese Bestimmungen und es ist schwierig, die wahren Absichten zu identifizieren, bevor eine Website live geht.

- Von den mehr als 200.000 neuen Domänen, die täglich weltweit registriert werden, könnten schätzungsweise bis zu 70 % für schädliche Aktivitäten vorgesehen sein.
    - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Viele spezialisierte Cybersecurity-Unternehmen überwachen die Nutzung von Websites sowie andere Informationen, um verdächtige Aktivitäten zu identifizieren. Threat Intelligence (TI) wird erstellt, die nach einmaliger Analyse verwendet wird, um böswillige Absichten zu bestätigen. Domain Name Filtering nutzt diese TI (aus mehreren Quellen), um den Zugriff auf schädliche Websites zu blockieren und so den beabsichtigten Schaden zu verhindern.

- **Quad9** ist ein DNS-Filtering-Dienst, der von der Global Cyber Alliance in Zusammenarbeit mit IBM und Packet Clearing House entwickelt wurde. Er verfügt über 19 verschiedene Threat Intelligence-Feeds und blockiert den Zugriff auf bekannte schädliche Websites nahezu in Echtzeit. Dazu verweigert er die Umwandlung und das Routing von Traffic an die IP-Adresse, die mit dem in den Browser eingegebenen Website-Domänennamen verknüpft ist. Außerdem kann es IP-Adressen blockieren, mit denen sich Ihre IoT-Geräte oder Computer möglicherweise automatisch verbinden (ohne dass Sie es wissen).

Domain Name Filtering kann eine Website erst dann blockieren, wenn ein Schwellenwert für schädliche Aktivität identifiziert wurde.

DNS: Domain Name System

- Das DNS (Domain Name System) ist das Äquivalent zu einem Telefonbuch im Internet.
- Ein eindeutiger Website-Name oder eine einzigartige Domäne in einem für uns verständlichen Textformat (d. h. globalcyberalliance.org) wird von Domänennamen-Servern in eine einzigartige Zahlenfolge (die IP-Adresse – 192.124.249.5) umgewandelt, die Computer verstehen.
- Es werden kontinuierlich neue Websites und Domänen erstellt und von Domänennamen-Registraren registriert, die die zugehörige IP-Adresse zuweisen und protokollieren (GoDaddy ist ein Beispiel für einen Domänennamen-Registrar).

Die Registrare müssen sicherstellen, dass jeder Website-Domänenname und jede IP-Adresse einzigartig ist. Viele Betrüger nutzen gleich aussehende Website-Domänennamen, um Opfern den Eindruck zu vermitteln, sich mit einer legitimen Website zu verbinden. Diese Websites tragen scheinbar den echten Website-Namen, aber bei näherer Betrachtung fallen Unterschiede auf (z. B. „rn“ anstelle von „m“ in der Website-Adresse).

Anzeigenblocker
Einige Anzeigen oder Nachrichten, die während des Surfens eingeblendet werden, sind nützlich. Viele sind es jedoch nicht und viele enthalten schädlichen Code. Um zu verhindern, dass während des Surfens Werbeanzeigen auf Websites eingeblendet werden, kann ein Anzeigenblocker eingesetzt werden. Er bietet eine zusätzliche Abwehrlinie gegen Angriffe.

Verwenden Sie die Tools in der Toolbox „Verhindern von Phishing und Malware“, um zu verhindern, dass Sie Phishing und Malware zum Opfer fallen.

https://gcatoolkit.org/de/kmu/verhindern-von-phishing-und-malware/