Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Schutz Ihrer E-Mails und Ihrer Marke“

E-Mails werden sehr häufig als Initiator für einen Cyberangriff verwendet. Es geht extrem schnell und ist kostengünstig, Tausende von E-Mails an ahnungslose Empfänger zu versenden, in der Hoffnung, dass zumindest einige von ihnen diese als echt erachten und auf den schädlichen Website-Link klicken oder den bösartigen Anhang herunterladen.

Dies kann dazu führen, dass Ihr Computersystem mit einer Form von Malware oder Ransomware infiziert wird, sodass der Kriminelle Zugriff erhält und wertvolle Daten stehlen oder Ihr Geld auf betrügerische Konten überweisen kann. Außerdem kann der Kriminelle möglicherweise die Kontrolle über Ihre Systeme übernehmen und Ihre Bankdaten manipulieren, sodass Kunden Zahlungen unbemerkt auf andere Konten vornehmen.

Die Verwendung von Phishing-E-Mails ist für Kriminelle extrem effektiv, denn sie können Tausende von potenziellen Opfern sehr schnell erreichen. Damit sie erfolgreich sind, muss die E-Mail jedoch so aussehen, als ob sie von einer legitimen Quelle stammt.

Es gibt mehrere Möglichkeiten, wie Kriminelle dies erreichen:

- **Anzeigenamen-Spoofing**
  - Angezeigter Name im Absenderfeld: ***„Unternehmen“***
  - E-Mail-Adresse: „<person@yahoo.com>“
    - *Zeigen Sie mit der Maus auf den Anzeigenamen, um die tatsächliche Adresse zu überprüfen, bevor Sie fortfahren.*

- **Spoofing durch gleich aussehende Domäne**
  - Angezeigter Name im Absenderfeld: ***„Unternehmen“***
  - E-Mail-Adresse: „<person@c**0rn**pany.com>“
    - *Überprüfen Sie die E-Mail-Adresse sorgfältig, bevor Sie fortfahren.*

- **Domänennamen-Spoofing**
  - Angezeigter Name im Absenderfeld: ***„Unternehmen“***
  - E-Mail-Adresse: „<person**@company.com**>“
    - *Verwenden Sie DMARC, um sich vor Domänennamen-Spoofing zu schützen.*

Bleiben Sie auch nach doppelter Überprüfung wachsam und nutzen Sie im Zweifelsfall alternative Methoden, um die Rechtmäßigkeit zu prüfen (rufen Sie den Absender beispielsweise an, um nachzufragen, ob er die E-Mail wirklich gesendet hat).

Wenn Sie keine Abwehr gegen Domänennamen-Spoofing haben, bedeutet das:

- Angreifer können vorgeben, Sie oder Ihr Lieferant/Kunde zu sein, um Zahlungen anzufordern oder Bestellungen aufzugeben.
- Angreifer können auch vorgeben, eine Person aus Ihrem eigenen Unternehmen zu sein.

Möglicherweise nutzen sie:

- **CEO-Betrug**, wobei eine E-Mail gesendet wird, die vorgibt, vom CEO oder einer befugten Führungskraft zu stammen. Darin werden häufig Kollegen angewiesen, sofort eine Zahlung vorzunehmen.

    - *Führen Sie ein Vier-Augen-Prinzip ein. In Familienunternehmen gilt häufig die Vertrauensbasis und es werden keine Gegenprüfungen durchgeführt. Angreifer nutzen das aus.*

- **Business Email Compromise (BEC)** bedeutet, dass eine E-Mail von einem bereits kompromittierten E-Mail-Konto gesendet wird, die „innerhalb des Unternehmens“ versendet wurde oder bei der die betrügerische E-Mail einen legitimen Domänennamen verwendet (Domänennamen-Spoofing). Diese können an Lieferanten oder Kunden gesendet werden und Zahlungen anfordern, die jedoch an geänderte Bankdaten erfolgen sollen. Da der Angreifer scheinbar aus demselben Unternehmen stammt, erscheint er vertrauenswürdiger. Durch bestimmte Authentifizierungstechniken wird der Absender bestätigt und ist dann schwerer als Angreifer zu erkennen. Der Angreifer hat möglicherweise die Kommunikation überwacht und befindet sich bereits seit einer Weile im System, sodass er kompetent wirkt.

    - *Verwenden Sie DMARC, um Beeinträchtigungen von Anfang an zu vermeiden, wenn Domänennamen-Spoofing eingesetzt wird.*
    - *Verwenden Sie sichere Passwörter und Multi-Faktor-Authentifizierungsmechanismen, um die Wahrscheinlichkeit von Kontobeeinträchtigungen zu verringern.*
    - *Überprüfen Sie regelmäßig Ihre E-Mail-Kontoeinstellungen, um sicherzustellen, dass E-Mails nicht an eine unbekannte E-Mail-Adresse weitergeleitet werden.*
    - *Implementieren Sie eine Richtlinie, damit alle Details für neue Lieferanten und Kunden mit mindestens zwei verschiedenen Methoden überprüft werden. Wenn Änderungen vorgenommen werden, prüfen Sie dies immer über eine bekannte alternative Methode (z. B. telefonisch unter einer bekanntermaßen richtigen Nummer/aus der Telefonzentrale, nicht nur anhand von eventuell in der Signatur enthaltenen Informationen, da diese ebenfalls geändert worden sein könnten).*

DMARC (Domain-based Message Authentication Reporting and Conformance)
Eine DMARC-Richtlinie ermöglicht es einem Absender, anzugeben, dass seine Nachrichten geschützt sind, und teilt dem Empfänger mit, was zu tun ist, wenn eine der Authentifizierungsmethoden erfolgreich ist oder fehlschlägt.

DMARC:

- Verhindert, dass eine andere Person in einer E-Mail Ihre Identität annimmt.
- Verhindert, dass Sie E-Mails von einem Betrüger erhalten.
- Bietet Einblicke in Spam-, Phishing- oder Spear-Phishing-Versuche mithilfe der E-Mail-Domäne Ihres Unternehmens durch Berichterstellung.
- Schafft Vertrauen bei Kunden und der Lieferkette.

Aber:

- Sowohl der Absender als auch der Empfänger müssen über eine gültige DMARC-Richtlinie und eine DMARC-Verifizierung verfügen, damit DMARC wirksam ist.
- Wenn Kunde und Lieferant DMARC nutzen, sind ***beide*** vor E-Mail-Domänen-Spoofing GESCHÜTZT. Wenn nur einer DMARC nutzt, ist keiner von beiden sicher.
- Was mit der E-Mail geschieht, sobald sie empfangen wird, hängt von der DMARC-Richtlinieneinstellung des Absenders ab.

Verwenden Sie die Tools in der Toolbox „Schutz Ihrer E-Mails und Ihrer Marke“, um mehr über DMARC zu erfahren und es in Ihrer E-Mail-Domäne zu konfigurieren.

https://gcatoolkit.org/de/kmu/schutz-ihrer-e-mails-und-ihrer-marke/