Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Mehr als ein sicheres Passwort“

Eine der häufigsten Methoden, wie sich Kriminelle Zugriff auf Ihre Konten, Ihr Netzwerk und Ihre Daten verschaffen, ist die Anmeldung unter falscher Identität. Sie sollten unbedingt einzigartige, sichere Passwörter (oder Passphrasen) für alle Ihre Konten verwenden und diese Passwörter geheim halten, schützen und niemals wiederverwenden.

- Wenn Sie dasselbe Passwort für mehrere Konten verwenden, kann ein Krimineller, der eines Ihrer Passwörter erlangt hat, im Prinzip auf alle Ihre Konten zugreifen.
    - *Er wird denselben Benutzernamen und dasselbe Passwort bei vielen häufig genutzten Anwendungen ausprobieren.*

Um sich Zugriff auf Ihre Passwörter zu verschaffen, setzen Kriminelle verschiedene Techniken ein. Im Internet (dem sogenannten „Darknet“) gibt es einen sehr aktiven Markt, auf dem diese personenbezogenen Informationen gekauft und verkauft werden, sollte eines der Unternehmen, bei dem Sie ein Konto besitzen, betroffen sein.

Unter anderem werden folgende Methoden verwendet:

- **Brute-Force-Angriff**: Nutzung von Rechenleistung, um automatisch alle möglichen Kombinationen einzugeben.
    - *Verwenden Sie lange Passwörter oder Passphrasen sowie Sonderzeichen, um dies zu erschweren.*
- **Wörterbuch-Angriff**: Eine Form des Brute-Force-Angriffs, bei der bekannte Wörter/Phrasen aus dem Wörterbuch oder häufige Passwörter verwendet werden.
    - *Verwenden Sie einprägsame Wörter/Passwörter. Diese sollten jedoch nicht aus dem Wörterbuch stammen, keine häufig genutzten Passwörter sein und keine Wörter, die mit Ihnen in Verbindung gebracht werden.*
- **Credential stuffing**: Sobald ein Konto kompromittiert wurde, werden die Angreifer dieselbe Kombination aus Benutzername/Passwort an anderer Stelle ausprobieren.
    - *Verwenden Sie für jedes Konto ein anderes Passwort sowie zusätzlichen Schutz (2-Faktor-Authentifizierung – 2FA) für Konten mit dieser Option.*

- **Phishing-E-Mails:** D. h. Sie erhalten eine Nachricht mit der Aufforderung, Ihr Passwort zurückzusetzen. Diese enthält Links zu einer bösartigen Website oder einen Keylogger, der installiert wird, wenn Sie einen schädlichen Anhang öffnen (ein Keylogger zeichnet Ihre Tastatureingaben auf).

    - *Seien Sie wachsam, wenn Sie E-Mails öffnen, darin auf Links klicken oder Inhalte herunterladen, selbst wenn diese scheinbar von Ihnen bekannten Personen oder Unternehmen stammen.*

- **Social Engineering**: Profis sind sehr geschickt darin, Kommunikation über verschiedenste Medien zu manipulieren (Telefonate, SMS oder soziale Medien), damit Sie Ihre Passwörter und andere personenbezogenen Informationen offenlegen, indem sie legitim Zwecke vortäuschen.

    - *Verraten Sie niemals Ihr Passwort oder Teile davon. Ein seriöses Unternehmen wird Sie nie darum bitten.*

- **Manuelles Raten**: Personenbezogene Daten, d. h. es wird ausprobiert, ob Namen und Geburtsdaten als Teil Ihres Passworts verwendet werden.

    - *Verwenden Sie keine zu persönlichen Informationen in Passwörtern. Überlegen Sie, was das Internet und soziale Medien über Sie verraten könnten, und vermeiden Sie es, diese Informationen in Ihren Passwörtern zu verwenden.*

- **Schulter-Surfen**: An öffentlichen Orten und sogar an Ihrem Schreibtisch kann es passieren, dass jemand Ihre Aktivitäten ausspioniert.

    - *Geben Sie Acht, wer sich hinter oder neben Ihnen befindet oder ob eine Kamera vorhanden ist, insbesondere bei der Eingabe vertraulicher Daten.*

- **Abfangen**: Passwörter können bei der Übertragung über ein Netzwerk abgefangen werden.

    - *Prüfen Sie Websites auf das https-Symbol (Vorhängeschloss) und seien Sie bei der Nutzung von WLAN-Netzen an öffentlichen Orten wachsam. Diese können unsicher oder „gekapert“ sein, das bedeutet, sie sehen aus wie das Original, doch andere können die übertragenen Daten auslesen.*

Ebenso wie unsere Nutzung des Internets und der sozialen Medien hat sich auch Leistung von Computern im Laufe der Zeit exponentiell zugenommen. All das führt dazu, dass sich Kriminelle schneller und einfacher Zugriff auf Ihre Informationen verschaffen können:

	Apple MacIntosh, 1984:	iMac „Core i5“ (Standard), 2019:	Unterschied:
RAM:	128 K	8 G	Anstieg um 64.500.000 %
Verarbeitungs-geschwindigkeit:	8 MHz	3 GHz	37.400 % schneller
Kosten:	2.500 $	1.500 $	40 % günstiger

- Der rasante technische Fortschritt kommt Hackern sehr entgegen, denn ein moderner Laptop und ein modernes Programm können ein Passwort schneller als je zuvor knacken.

    - *Die Notwendigkeit, mithilfe von längeren, komplexeren Passwörtern und zusätzlichen Schutzmaßnahmen mit der Entwicklung Schritt zu halten, geht Hand in Hand mit dem technologischen Fortschritt.*

Zwei-Faktor-Authentifizierung (2FA)
2FA bietet eine zweite Sicherheitsebene, die es einem Angreifer deutlich schwerer macht, sich Zugriff auf Ihre Konten zu verschaffen, da sie auf folgenden Informationen beruht:

- Etwas, das Sie kennen:
    - Ein Passwort

- Und/oder etwas, das Sie haben:
    - Ein Token (Google Authenticator, Okta, RSA)
    - Ein an Ihr Telefon gesendeter Verifizierungscode (SMS)

- Oder etwas, das Sie sind:
    - Ein Fingerabdruck oder Ihr Gesicht (Biometrie)

2FA fragt dies ab, bevor Zugriff gewährt wird, was eine zusätzliche Abwehrebene bietet.

Es gibt viele Tipps für das Erstellen langer, sicherer Passwörter oder Passphrasen. Welche Tipps Sie auch befolgen, Folgendes sollte gewährleistet sein:

- Implementieren Sie eine sichere unternehmensweite Richtlinie und ein System, das die Verwendung unsicherer Passwörter untersagt.
- Vermeiden Sie Kosenamen oder Passwörter, die anhand von Informationen in sozialen Medien erraten werden könnten.
- Verwenden Sie für jedes Konto ein anderes Kennwort.
- Erwägen Sie die Verwendung eines Passwort-Managers, um Ihre Passwörter zu speichern, wenn Sie dies wünschen.

Zusätzlich:

- Aktualisieren Sie Ihre Passwörter für alle Konten, die kompromittiert wurden (Sie können dies über das Tool „Have I Been Pwned“ in der Toolbox überprüfen).
- Löschen Sie Konten und deinstallieren Sie Anwendungen, die Sie nicht mehr verwenden.
- Verwenden Sie sichere und einzigartige Passwörter für alle Ihre Konten.
- Aktivieren Sie 2FA für alle Ihre Konten (sofern 2FA unterstützt wird).
- Überprüfen Sie Ihre remote zugänglichen Geräte auf Admin/Admin-Standardeinstellungen. Ändern Sie Standardpasswörter, die leicht zu erraten sind, immer vor der ersten Verwendung.

Verwenden Sie die Tools in der Toolbox „Mehr als ein sicheres Passwort“ als Anleitung, um zu überprüfen, ob Ihre Konten nachweislich kompromittiert wurden, und um Verbesserungen zu implementieren.

https://gcatoolkit.org/de/kmu/mehr-als-ein-sicheres-passwort/