Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Kennen Sie Ihre eigene IT-Umgebung“

Es ist entscheidend, dass Sie Ihre eigene IT-Umgebung kennen, damit Sie diese richtig schützen können. Wenn Sie Ihre eigene IT-Umgebung kennen, können Sie:

- Potenzielle Risiken erkennen und etwas dagegen unternehmen
- Verstehen, dass Sie niemals alle Risiken beheben werden, aber sie reduzieren können
- Die Cyber-Sicherheit und das Bewusstsein dafür verbessern, wodurch Sie Ihr Risiko für häufige Bedrohungen um bis zu 80 % senken

Cybersecurity ist der Weg, nicht das Ziel. Beginnen Sie also noch heute, sie in Ihren Alltag zu integrieren.

Kennen Sie Ihre eigene IT-Umgebung – Checkliste

<u>Erstellen Sie eine Inventarliste:</u>

- Was ist in Ihrer IT-Umgebung vorhanden?
    - *Ihre Geräte – Desktop-PCs, Server, Laptops, Smartphones, Tablets, POS, IoT, Videoüberwachung...*
    - *Ihre Anwendungen – Microsoft Office, Adobe, POS-Anwendungen, Chrome...*
    - *Ihre Online-Konten – E-Mail, Amazon, iCloud, Facebook, Online-Banking, Kreditkarten...*

- Was ist über das Internet oder in Ihrem internen Netzwerk zugänglich?
    - *Ein IoT-Gerät, das Ihr internes Netzwerk nutzt, aber über das Internet gesteuert werden kann, stellt potenziell ein Risiko dar*
    - *Ein altes Gerät, das nicht mehr verwendet und nicht mehr gepatcht wird, aber immer noch eingeschaltet ist, kann eine Angriffsfläche bieten*
    - *Jedes Gerät, das noch ein unverändertes Standardpasswort verwendet, öffnet Eindringlingen die Tür (z. B. ein Videoüberwachungssystem mit einem einfachen Admin/Admin-Passwort oder ein älterer Router)*
    - *Ein altes Online-Konto, das Sie nicht verwenden, das aber immer noch Ihre Daten gespeichert hat, kann kompromittiert werden und Sie (und andere verbundene Geräte) gefährden*
    - *Software auf Ihrem Computer, die Sie nicht mehr verwenden oder pflegen, aber nicht entfernt haben, kann zum Angriffsziel werden*

- Welche Art von Zugriff ist nötig, damit alles reibungslos funktioniert?
    - Wurde der Zugriff für Personen, die keinen Zugriff mehr benötigen, entfernt
        - *Beziehungen mit Drittauftragnehmern, die beendet wurden?*
        - *Lieferkettenunternehmen, die es nicht mehr gibt?*
        - *Mitarbeiter, die das Unternehmen verlassen haben, versetzt wurden oder längere Zeit abwesend sind?*
    - Wurden Systeme und Anwendungen entfernt, die nicht mehr relevant sind oder nicht mehr verwendet werden?
    - Beschränken Sie die Anzahl der Benutzer mit Administratorrechten. Administrator-Zugriff auf Systeme oder Anwendungen sollte Administratoren vorbehalten sein und nicht für normale Benutzer gelten.

- Beschränken Sie den Zugriff auf Systeme und Anwendungen, um potenzielle Schäden durch Folgendes zu verringern:
    - Vorsätzliche und versehentliche Insider-Bedrohungen, verursacht durch:
        - *Vorsätzliches Handeln eines verärgerten Mitarbeiters*
        - *Einen Mitarbeiter, der erpresst wird, auf vertrauliche Informationen zuzugreifen*
        - *Die Auswirkungen und Folgen des Öffnens einer Phishing-E-Mail*
        - *Versehentliches Löschen oder Beschädigen von Daten*

Berücksichtigen Sie bei der Erstellung der Inventarliste auch, ob Anforderungen für sichere Passwörter durchsetzbar sind und ob die Zwei-Faktor-Authentifizierung (2FA) aktiviert ist. (2FA ist eine zusätzliche Schutzebene für Ihre Passwörter.)

- Erstellen Sie separate Netzwerke und eingeschränkte Zugriffsrechte (Administrator / Benutzer / keiner), damit vertrauliche Informationen schwerer auszulesen sind und wichtige Systeme sich nicht im selben Netzwerk wie weniger sichere Geräte befinden. Dies kann die Auswirkungen eines Angriffs möglicherweise verringern, denn:
    - Viele IoT-Geräte von Verbrauchern verfügen über keine oder nur minimale integrierte Sicherheit
    - Ältere Geräte unterliegen möglicherweise nicht mehr der Garantie und bieten keinen Schutz vor neuen Sicherheitslücken
    - Dritte mit Netzwerkzugriffsrechten bieten Angreifern einen Eintrittspunkt
        - *Falls Dritte Zugriff auf Ihr Netzwerk haben, verfügen diese über eine Richtlinie, um Passwortänderungen zu erzwingen, wenn wichtige Mitarbeiter ausscheiden?*

- Stellen Sie sicher, dass Ihre Inventarliste immer auf dem neuesten Stand ist, besonders, wenn Sie neue Geräte, Konten oder wichtige Daten hinzufügen oder löschen.

Verwenden Sie die Tools in der Toolbox „Kennen Sie Ihre eigene IT-Umgebung“ als Unterstützung oder um ein alternatives System zu entwickeln, das für Sie funktioniert.

https://gcatoolkit.org/de/kmu/kennen-sie-ihre-eigene-it-umgebung/