# Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Updates zur Abwehr“

Cyberkriminelle sind ständig auf der Suche nach Möglichkeiten, Zugriff auf Systeme und Daten zu erhalten. Eine Möglichkeit dabei ist, Schwachstellen in einer Konfiguration oder einem Entwicklercode aufzudecken, die für alle Benutzer repliziert und von Cyberkriminellen zu ihrem eigenen Vorteil ausgenutzt werden können.

Hersteller und Softwareentwickler veröffentlichen regelmäßig Updates für ihre Betriebssysteme und Anwendungen, um neu entdeckte Schwachstellen oder Sicherheitslücken zu beheben.

- Diese Korrekturen werden in der Regel als Patches bezeichnet, der Prozess heißt Patching.

**Es ist von entscheidender Bedeutung, dass Patches schnell und wenn möglich automatisch angewendet werden, um zu vermeiden, dass die Schwachstellen bei einem Cyberangriff ausgenutzt werden.**

- Beim WannaCry Ransomware-Angriff im Mai 2017 wurde eine Sicherheitslücke im Windows-Betriebssystem ausgenutzt. Der Angriff hatte verheerende globale Folgen.
    - Er zielte nicht auf bestimmte Sektoren ab, sondern auf die Art der verwendeten Geräte.
        - Betroffen waren Einzelpersonen,
        - KMU und große Konzerne,
        - die Polizei, das Gesundheits- und Transportwesen, die Telekommunikation, Banking-Dienste usw.
    - Innerhalb von 24 Stunden wurden schätzungsweise 230.000 Computersysteme in 150 Ländern zum Ziel des Angriffs. Die Verluste lagen im Milliardenbereich.
- Im März 2017 hatte Microsoft Patches für alle unterstützten Geräte veröffentlicht.
    - Jeder, der das Patch vor Beginn des Angriffs nicht angewendet hatte, war gefährdet.
    - Diejenigen, die das Patch (manuell oder automatisch) angewendet hatten, waren nicht gefährdet.

- Auch Verwender von Windows XP waren gefährdet, da es für Windows XP keine Updates mehr gab („Lebensende“ – aufgrund der Schwere des WannaCry-Angriffs wurde jedoch schnell ein Patch entwickelt).

**Lebensende**
Alle Geräte und Betriebssysteme haben ein „Lebensende“. Wenn sie dieses erreicht haben, gibt es keinen Support und keine weiteren Patches mehr und sie werden zum unmittelbaren, ständigen Risiko bei neu entdeckten Sicherheitslücken. Dies kann auch passieren, wenn ein Hersteller den Betrieb einstellt und niemand die Entwicklung seiner Produkte übernimmt.

- Windows 7 erreichte im Januar 2020 sein Lebensende.
- Windows XP erreichte im April 2014 sein Lebensende.
- *Nicht unterstützte Systeme sollten aus dem Netzwerk entfernt, aktualisiert oder ersetzt werden.*

**IoT-Geräte**
Die Zunahme von IoT-Geräten (Internet of Things), insbesondere auf dem Verbrauchermarkt, wo Kaufentscheidungen häufig auf Preis, Benutzerfreundlichkeit und Funktionalität, jedoch weniger auf Sicherheit basieren, kann potenzielle Zugriffspunkte für Angreifer schaffen. Viele davon bieten nur eingeschränkte Sicherheitsfunktionen und keine Patching-Optionen. Wenn also eine Schwachstelle vorhanden wäre, würde diese Ihr Netzwerk angreifbar machen, bis das Gerät physisch entfernt wird oder entsprechende Abwehrmaßnahmen implementiert werden. Um dieses Risiko zu umgehen, gäbe es –wenn überhaupt– nur minimale Präventivmaßnahmen.

Alte Anwendungen, die nicht mehr verwendet werden, und ältere Geräte (alte Geräte, die für die Verwendung im Netzwerk oder über das Internet „angepasst“ wurden) sollten am besten entfernt werden. Idealerweise wurden diese im Rahmen der Toolbox „Kennen Sie Ihre eigene IT-Umgebung“ identifiziert und entfernt/aktualisiert, sodass für geschäftliche Funktionen nur die minimal erforderliche Zugriffsebene gewährt wird.

Zusammenfassung:

- Patches/Updates enthalten wichtige Sicherheitskorrekturen zum Schutz vor neu entdeckten Sicherheitslücken und sollten sofort implementiert werden, idealerweise über eine automatische Update-Option, falls vorhanden.
    - *Wenn Sie Patches nicht rechtzeitig anwenden, gefährden Sie Ihre Computersysteme – und damit auch Ihr Unternehmen.*
- Entfernen Sie Geräte, die nicht gepatcht werden können (d. h. viele IoT-Geräte für Verbraucher), und alle Geräte oder Anwendungen, die nicht mehr unterstützt werden – diese können andernfalls Ihr Unternehmen gefährden.
    - *Wenn das Gerät für geschäftliche Abläufe erforderlich ist, isolieren Sie das Gerät so gut wie möglich und verhindern Sie jeglichen Internetzugang und Zugriff auf andere Geräte.*

- Stellen Sie für geschäftliche Funktionen die minimal erforderliche Zugriffsebene sicher und deaktivieren Sie umgehend den Zugriff für Mitarbeiter, die das Unternehmen verlassen haben, oder Drittunternehmen, die keine Dienste (oder Kunden) mehr bereitstellen.
- Stellen Sie sicher, dass jegliche Software und Systeme auf dem neuesten Stand sind, also über die neueste Patch-Version verfügen und regelmäßig überprüft werden.

**Verwenden Sie die Tools in der Toolbox „Updates zur Abwehr“ als Unterstützung. Implementieren Sie eine Richtlinie, die regelmäßige Überprüfungen Ihres Inventars, Ihrer Lieferkette und Ihrer Updates sicherstellt.**

**https://gcatoolkit.org/de/kmu/updates-zur-abwehr/**