Hintergrund zum GCA Cybersecurity Toolkit: Toolbox „Backup und Wiederherstellung“

Da immer mehr Informationen online gespeichert werden, sollten Sie unbedingt ein Backup von geschäftlichen und privaten Daten erstellen. Dies ist von entscheidender Bedeutung für die Geschäftskontinuität.

Es gibt viele Gründe, warum der Zugriff auf Ihre Daten verloren gehen kann. In diesem Fall gehen wir von Datenverlusten oder -beschädigungen aufgrund eines Cyberangriffs aus, doch Backups ermöglichen auch die Wiederherstellung nach Festplattenausfall, Gerätediebstahl, menschlichen Fehlern, versehentlicher Beschädigung, Wasserschaden usw.

Die starke Abhängigkeit von Computern und der Online-Welt bedeutet, dass die Auswirkungen von Datenverlusten oder Ausfallzeiten die Produktivität und Rentabilität eines Unternehmens ernsthaft beeinträchtigen können. Der Verlust wertvoller Fotos auf einem Heimcomputer beispielsweise kann ebenso für Ärger sorgen.

Welche Auswirkungen hätte es auf Ihre Finanzen und Ihre Reputation, wenn Ihr Unternehmen:

- Einen Tag lang keinen Handel treiben/die IT-Systeme nicht nutzen könnte?
- Ein wichtiges Angebot verlöre, das zum nächsten großen Vertragsabschluss hätte führen können?
- Nicht mehr auf Kundendaten zugreifen könnte oder diese beschädigt wären?
- Aufgefordert würde, Lösegeld zu bezahlen, um wieder Zugriff auf seine Daten zu erhalten?

Backups sind entscheidend, um Daten schnell wiederherzustellen und den Betrieb wieder aufnehmen zu können!

Ransomware
Ransomware ist eine Art von Malware, die den Zugriff auf ein System, Gerät oder eine Datei blockiert, bis ein Lösegeld bezahlt wird – in der Regel in einer Kryptowährung (d. h. Bitcoin), die weniger leicht nachzuverfolgen ist als herkömmliche Überweisungen.

Sie hat an Popularität gewonnen und wurde für eine Reihe von hochkarätigen Angriffen eingesetzt. Beispiele für Ransomware-Angriffe:

- WannaCry: WannaCry nutzte 2017 eine Sicherheitslücke im Windows-Betriebssystem aus. NHS, Renault und FedEx waren betroffen.

- Petya (2016) und NotPetya (2017): Petya verbreitete sich versteckt in einer PDF-Datei, die an eine E-Mail angehängt war (d. h. ein schädlicher Lebenslauf, der an eine Personalabteilung gesendet wurde). Diese Ransomware entwickelte sich weiter zu NotPetya, die teilweise dieselbe Sicherheitslücke ausnutzte wie WannaCry.
- Anfang 2020 fiel TravelEx, ein globaler Dienstleister für den Währungsumtausch, einem Ransomware-Angriff zum Opfer. Dadurch war das Unternehmen über zwei Wochen lang offline, was Chaos für Millionen von Reisenden verursachte.

Es mag verlockend sein, das Lösegeld zu zahlen, der allgemeine Ratschlag lautet jedoch, dies NICHT zu tun.

Schutz vor Ransomware:

- **Stellen Sie sicher, dass alle Systeme auf dem neuesten Stand sind** – eine gute Cyber-Sicherheit, Patching, automatische Updates und Echtzeit-Antiviren-Software können dazu beitragen, einen Ransomware-Angriff zu verhindern.
- **Verhindern Sie Phishing-/Spam-Nachrichten,** indem Sie die entsprechenden Filter aktivieren und Benutzer darüber aufklären, dass sie nicht auf Links klicken und keine Anhänge von nicht vertrauenswürdigen Quellen öffnen sollen.
- **Regelmäßige und externe Backups** helfen bei der Wiederherstellung, falls Sie Opfer eines Ransomware-Angriffs (oder Malware/anderer Ursache für Datenverlust/-beschädigung) werden.

Es gibt verschiedene Backup-Möglichkeiten:

- **Offline-Backups** werden lokal und offline gespeichert, z. B. auf einer externen Festplatte, einem USB-Laufwerk, einer Speicherkarte oder einem anderen Gerät. Diese Geräte sollten getrennt und separat vom Gerät aufbewahrt werden.
- **Online-Backups** oder Cloud-Backups erzeugen Kopien Ihrer wichtigen Daten und speichern sie extern auf sicheren Servern in der Cloud.

  Online-Backups können so eingestellt werden, dass sie in regelmäßigen Abständen automatisch erfolgen, und bieten in vielen Fällen eine gute Wiederherstellung (z. B. bei Diebstahl und Wasserschäden). Bei der Wiederherstellung nach einem Cyber-/Ransomware-Angriff sollten Sie jedoch vorsichtig sein und darauf achten, ob nicht auch das Backup betroffen ist. Es empfiehlt sich, eine Richtlinie zu implementieren, die sowohl Online- als auch Offline-Backups umfasst.

Überlegen Sie, welche Auswirkungen der Verlust Ihrer Daten hätte, und berücksichtigen Sie dies bei der Erstellung einer Backup-Richtlinie. Zum Schutz vertraulicher Informationen sollte Verschlüsselung genutzt werden.

- Implementieren Sie einen sinnvollen Ansatz (Richtlinie) für das Backup Ihrer Daten, indem Sie die verschiedenen Datentypen, über die Sie verfügen, kategorisieren.
- Berücksichtigen Sie die wichtigen und sensiblen Daten – wie regelmäßig sollte ein Backup durchgeführt und wie/wo sollte es gespeichert werden?

Verwenden Sie die Tools in der Toolbox „Backup und Wiederherstellung“, um Backups für alle Systeme zu konfigurieren. Verwenden Sie ein externes Laufwerk/Gerät, um Offline-Backups durchzuführen.

https://gcatoolkit.org/de/kmu/backup-und-wiederherstellung/