# Die INTARGIA Tipps zur Prävention von Cyber-Attacken:

## Für Unternehmen:

**Verringern Sie die Wahrscheinlichkeit eines Cyber-Angriffs**

- Überprüfen Sie, ob für den gesamten Remotezugriff auf das Netzwerk der Organisation und für privilegierte oder administrative Zugriffe eine mehrstufige Authentifizierung erforderlich ist.
- Stellen Sie sicher, dass die Software auf dem neuesten Stand ist, und priorisieren Sie Updates, die bekannte ausgenutzte Schwachstellen beheben.
- Vergewissern Sie sich, dass das IT-Personal der Organisation alle Ports und Protokolle deaktiviert hat, die für geschäftliche Zwecke nicht unbedingt erforderlich sind.

**Ergreifen Sie Maßnahmen, um ein potenzielles Eindringen schnell zu erkennen**

- Stellen Sie sicher, dass sich das Cybersicherheits-/IT-Personal darauf konzentriert, unerwartetes oder ungewöhnliches Netzwerkverhalten zu erkennen und schnell zu bewerten. Aktivieren Sie die Protokollierung, um Probleme oder Ereignisse besser untersuchen zu können.
- Vergewissern Sie sich, dass das gesamte Netzwerk der Organisation durch Antiviren-/Antimalwaresoftware geschützt ist und dass die Signaturen in diesen Tools aktualisiert werden.
- Wenn Sie mit ukrainischen Organisationen zusammenarbeiten, achten Sie besonders darauf, den Datenverkehr von diesen Organisationen zu überwachen, zu inspizieren und zu isolieren. Überprüfen Sie die Zugriffskontrollen für diesen Datenverkehr genau.

**Stellen Sie sicher, dass die Organisation darauf vorbereitet ist, im Falle eines Eindringens zu reagieren**

- Benennen Sie ein Krisenreaktionsteam mit Hauptansprechpartnern für einen vermuteten Cybersicherheitsvorfall und Rollen/Verantwortlichkeiten innerhalb der Organisation, einschließlich IT, Kommunikation, Recht und Business Continuity.
- Sicherstellung der Verfügbarkeit von Schlüsselpersonal; Identifizierung von Mitteln zur Bereitstellung von Support für die Reaktion auf einen Vorfall.
- Führen Sie eine kurzfristige Übung durch, um sicherzustellen, dass alle Teilnehmer ihre Rollen während eines Vorfalls kennen und verstehen.

**Maximieren Sie die Widerstandsfähigkeit des Unternehmens gegenüber einem zerstörerischen Cyber-Vorfall**

- **Testen Sie Backup-Verfahren**, um sicherzustellen, dass kritische Daten schnell wiederhergestellt werden können, wenn das Unternehmen von Ransomware oder einem zerstörerischen Cyberangriff betroffen ist.
- **Stellen Sie sicher, dass Sicherungen von Netzwerkverbindungen getrennt vorhanden sind.**
- Wenn Sie industrielle Steuerungssysteme oder Betriebstechnologie verwenden, führen Sie einen Test der manuellen Kontrollen durch, um sicherzustellen, dass kritische Funktionen funktionsfähig bleiben, wenn das Netzwerk des Unternehmens nicht verfügbar oder nicht vertrauenswürdig ist.

## Für Nutzer (dienstlich und privat):

Jeder Einzelne kann einfache Schritte unternehmen, um seine Cyber-Hygiene zu verbessern und sich zu schützen. Folgendes sollten Sie tun:

- **Implementieren Sie die Multi-Faktor-Authentifizierung für Ihre Konten**.

Ein Passwort reicht nicht aus, um Sie online zu schützen. Durch die Implementierung einer zweiten Identifikationsebene, wie eine Bestätigungs-SMS oder E-Mail, einen Code von einer Authentifizierungs-App, einen Fingerabdruck oder eine Face ID oder ähnliches, geben Sie Ihrer Bank, Ihrem E-Mail-Anbieter oder einer anderen Website, auf der Sie sich anmelden, das Vertrauen, dass Sie es wirklich sind. Multi-Faktor-Authentifizierung kann dazu führen, dass Sie 99% weniger wahrscheinlich gehackt werden. Aktivieren Sie also die Multi-Faktor-Authentifizierung für Ihre E-Mail-, Social-Media-, Online-Shopping- und Finanzdienstleistungskonten. Und vergessen Sie nicht Ihre Gaming- und Streaming-Entertainment-Dienste!

- **Aktualisieren Sie Ihre Software. Aktivieren Sie automatische Updates**.

Hacker werden Fehler im System ausnutzen. Aktualisieren Sie das Betriebssystem auf Ihren Mobiltelefonen, Tablets und Laptops. Und aktualisieren Sie Ihre Anwendungen – insbesondere die Webbrowser – auch auf all Ihren Geräten. Nutzen Sie automatische Updates für alle Geräte, Anwendungen und Betriebssysteme.

- **Denken Sie nach, bevor Sie klicken**.

Mehr als 90% der erfolgreichen Cyberangriffe beginnen mit einer Phishing-E-Mail. Wenn Sie einen Link sehen, den Sie nicht kennen, vertrauen Sie Ihren Instinkten und denken Sie nach, bevor Sie klicken. Das gilt derzeit insbesondere für E-Mails mit Bezug zur aktuellen Situation (wie bspw. Ukraine-Hilfen etc.).

- **Verwenden Sie starke Passwörter.**

  Und idealerweise einen Passwort-Manager, um sichere Passwörter zu generieren und zu speichern. Unsere Welt ist zunehmend digital und zunehmend vernetzt. Während wir uns also schützen müssen, wird es uns alle brauchen, um die Systeme, auf die wir uns alle verlassen, wirklich zu schützen.

Haben Sie Fragen? Kontaktieren Sie uns, wir helfen Ihnen gerne weiter:


Ihr Ansprechpartner

Thomas Lang

Geschäftsführender Partner

Phone: +49 6103 5086 0
Mail: thomas.lang@intargia.com