Claudia Plattner, Präsidentin des Bundesamtes für Sicherheit (BSI), warnt vor einer neuen Welle von Cyberangriffen mit einem markanten Satz:

"Die Frage ist nicht, ob ein Angriff erfolgreich ist, sondern nur, wann."

Zur Lage in Kürze:

66% aller Spam E-Mails sind Cyberangriffe
250.000 neue Schadprogramme pro Tag
21.000 infizierte Systeme werden jeden Tag vom BSI gemeldet

83% aller Cybervorfälle betreffen Unternehmen und Organisationen mit weniger als 1000 Mitarbeiter

Jedes dritte deutsche Unternehmen wurde bereits gehackt.

Trend 2023/2024: Ausnutzen von Schwachstellen sinkt von 37% auf 23% und Kompromittieren von Zugangsdaten steigt stark von 29% auf 50%

91% aller Angriffe erfolgen außerhalb der normalen Geschäftszeiten (Mo-Fr 8-18)

Angriffe werden schneller, die Verweildauer sinkt:
2021 11 Tage (Erpressung)
2022 9 Tage (Exfiltration)
2023 5 Tage (Ransomare / kompromittierte Zugangsdaten)

Durch ständig optimierte Angriffstechniken, gelingt es Angreifern immer häufiger die Schutzsysteme zu deaktivieren:
2021 21%
2022 36%
2023 43% (!)

In 82% aller erfolgreichen Angriffe werden Beweise vernichtet.

>> WAS IST ZU TUN?

1) Machen Sie es den Angreifern so schwer wie möglich:
   Halten Sie Ihre Systeme auf dem **aktuellen Stand**
   Nutzen Sie nur aktuelle und **professionelle Schutzsysteme**
   Schließen Sie sofort bekannte Schwachstellen
   Nutzen Sie MFA (**Multi Faktor Authentifizierung**) wo es nur geht

2) **Sichern Sie Ihre Daten täglich**, automatisiert im und außer Haus.
   Verwenden Sie unterschiedliche Zugangsdaten für das Backup
   Buchen Sie immuntable cloud backups (unveränderbare Datenspeicherung)
   Überprüfen Sie regelmäßig mit Nachweis, ob und wie Ihre Backups funktionieren (per DSGVO gesetzlich vorgeschrieben)

3) Nutzen Sie „**E-Mail Gateway Protection**": ein System das den gesamten E-Mail Verkehr überwacht und alle Links vor Weitergabe prüft und bei Gefahr löscht.

4) Buchen Sie ein **kontinuierliches Awareness Training** (digitale Achtsamkeit) für alle Mitarbeiter mit harmlosen Fake Phishing Mails gegen die „**Schwachstelle Mensch**". Diese sporadisch absolvierten Trainings dienen als Schulungsnachweise (per DSGVO gesetzlich vorgeschrieben)

5) Erstellen Sie einen **Notfallplan** (Desaster Plan) für den Moment nach dem erfolgreichen Angriff und eine **aktuelle Dokumentation** für die Wiederherstellung der Systeme.

Wir unterstützen Sie gerne bei der Umsetzung.

Peter Grünewald
Evidenta GmbH

https://evidenta.de
Tel. +491715607720

März 2024