GU Sicherheit & Krisenmanagement

Weihnachtstage – ein idealer Zeitpunkt für Cyberangriffe

Weihnachten steht vor der Tür und wir haben vielleicht schon viele Pläne. Noch schnell etwas fertigstellen im Geschäft, den Computer herunterfahren und ein paar wohlverdiente Feiertage geniessen. Damit Sie dies tun können, lohnt es sich, ein paar Dinge im Bereich IT-Sicherheit zu berücksichtigen.

Ein Beitrag von Priska Schwander

Angriffe nehmen zu

In den Medien lesen und hören wir fast täglich, dass Cyberangriffe auf Unternehmen weiter zunehmen. Aber auch Privatpersonen sind nicht vor einem Angriff gefeit. Trotz grosser Bemühungen und Vorsichtsmassnahmen finden Cyberkriminelle immer wieder Mittel und Möglichkeiten die vorhandenen Sicherheitsmassnahmen zu umgehen.

Dem Nationalen Zentrum für Cybersicherheit NCSC (früher MELANI) wurden in der Zeit vom 01.01. – 12.11.2022 wöchentlich zwischen 408 und 954 Vorfälle gemeldet. Dabei ist zu bedenken, dass nicht alle Cybervorfälle beim NCSC deklariert werden.

Swisscom hat beispielsweise veröffentlicht, dass sie bis zu 6,5 Mio. Cyberangriffe pro Monat abwehren müssen. Die Zahlen für 2022 sind erschreckend, doch Fachleute gehen davon aus, dass die Anzahl der Cyberangriffe im Jahr 2023 noch ansteigen wird.

Erhöhtes Risiko an Feiertagen

Gerade vor speziellen Anlässen oder Feiertagen ist das Risiko eines Angriffs zusätzlich erhöht. Beispielsweise am «Black Friday» stehen Hackern Tür und Tor offen, da viele Leute die großartigen Angebote sehen möchten, um vielleicht noch ein Schnäppchen zu ergattern. Praktischerweise ist in der E-Mail gleich ein Link vorhanden, welcher rasch angeklickt werden kann...

Ein weiteres Risiko sind sogenannte Fernwartungszugänge, bei welchen sich eine externe Firma mit Ihrer Unternehmens-IT verbinden kann. Wie praktisch ist es doch, wenn der Spezialist nicht immer ins Haus kommen muss, sondern sich direkt verbinden kann? Oder wenn die Daten direkt im Internet gespeichert werden, anstatt auf einer lokalen Komponente? Viele Komponenten der IT-Landschaft haben Abhängigkeiten und jede davon bietet Raum für eine weitere Schwachstelle. Cyberkriminelle finden immer wieder neue Wege, um an ihr Ziel zu kommen, denn für sie ist es ein lukratives Business-Modell. Art und Dauer des Angriffs können dabei variieren. Sind die Cyberkriminellen einmal im System, können sie mit verschiedenen Hilfsmitteln Informationen abgreifen, Prozesse verändern, Daten verschlüsseln oder mittels gezielter Sabotage des Unternehmens die Reputation längerfristig schädigen.

Einige Tipps zum optimalen Schutz Ihrer Daten:

- ☐ Updates und Sicherheits-Patches sofort installieren
- ☐ Steigern Sie die Awareness der Mitarbeitenden und von sich selber
- ☐ IT-Notfallpläne erstellen (Notbesetzung, Einsatzplanung, Pikett-Organisation)
- ☐ Computer mit aktuellen Virenschutzprogrammen und Firewalls schützen
- ☐ Cookies regelmässig löschen
- ☐ Verschiedene Passwörter verwenden und regelmässig ändern
- ☐ Persönliche Angaben aufs Nötigste reduzieren
- ☐ Absender und Anhänge bei E-Mails genau prüfen
- ☐ E-Mails, in welchen Daten verlangt werden sehr kritisch betrachten – ev. beim Sender nachfragen
- ☐ Link auf Websites genau prüfen
- ☐ Vorsicht mit Downloads aus dem Internet
- ☐ Privatsphäre-Einstellungen anpassen
- ☐ Berechtigungen von Apps so weit wie möglich beschränken

Wappnen Sie sich für den Ernstfall. Wir sind für Sie da. Mit Sicherheit.

Über die Autorin

Priska Schwander ist seit November 2021 bei der GU Sicherheit & Partner AG. Sie ist eidg. dipl. Berufsoffizier mit «Diploma of Advanced Studies in Militärwissenschaften» der ETH Zürich. Ausserdem war sie Projektleiterin in der Medizin-Informatik.

Priska Schwander
Consultant