CYBERANGRIFFE IN ÖSTERREICH

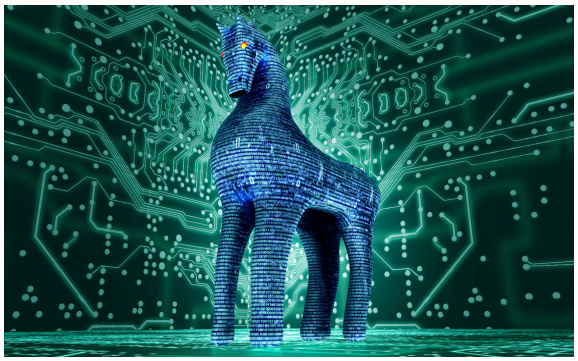
CERT - das österreichische IT-Notfallteam

Das nationale Notfallteam CERT (Computer Emergency Response Team) ist gerüstet. Das Team ist die Anlaufstelle für Computer-Sicherheit. Als österreichische IT-Feuerwehr kann sie nicht nur Bedrohungen erkennen, sondern auch Cyberattacken vorbeugen und im Notfall zu Hilfe kommen. Gegründet wurde CERT im Jahr 2008. Dass es dieses Team braucht um kritische Infrastrukturen und Firmen zu schützen, zeigen die Berichte und Meldungen, die CERT veröffentlicht.

Cyberangriffe mit Ransomware

Ransomware sind Schadprogramme, die in ein Computersystem eindringen, und Daten verschlüsseln. Ziel der Attacke ist die Erpressung von Lösegeld. Vergleichbar ist dieser Vorgang mit dem Trojanischen Pferd, in dessen Bauch die Griechen ungesehen in die Stadt Troja gelangten und diese besiegen konnten.

Getarnte Programme, die gezielt in IT-Systeme eingeschleust werden, werden deshalb auch Trojaner genannt. So gut sichtbar wie das hölzerne Pferd sind die Trojaner leider nicht.



SalzburgMilch stand nach einem solchen Angriff still. Nichts ging mehr. Mit der Botschaft "SalzburgMilch, you are fucked" forderten die Kriminellen eine erhebliche Summe in Form von Bitcoins. Die Verfolgung der Angreifer führte ins Darknet, aber nicht zum Erfolg.

Phishing

Auch mit vermeintlich echten Accounts gelangen Kriminelle in die IT-Infrastruktur der Unternehmen. Online-Banking, vermeintliche Shopping-Angebote öffnen so die PC-Tür für den Angriff.

Hier heißt es vor allem für die Anwender:innen vorsichtig zu sein. Kontodaten und Passwörter dürfen niemals bekannt gegeben werden, unbekannte Links sollten ungeöffnet bleiben.

DDoS-Angriff auf Kärnten

Etwas anders lief es in Kärnten. Hier war war es DDoS (Distributed Denial of Services). Ein DDoS-Angriff wird auch als "Überlastungsangriff" bezeichnet. Dabei werden so lange Anfragen an den Server geschickt, bis dieser zusammenbricht. Das Bundesland Kärnten sah sich 2022 mit einem solchen Angriff konfrontiert. Eine Hacker-Gruppe, die sich Black Cat nennt, hatte sich Zugang zum System verschafft und angeblich Lösegeld in Höhe von fünf Millionen US-Dollar gefordert.

Palfinger: Lösegeld bezahlt

Während das Land Kärnten auf die Forderungen der Verbrecher nicht eingegangen ist, hat sich der Kranarmhersteller Palfinger nach einer weltweiten Cyberattacke zur Zahlung entschieden.

Rund zwei Wochen lang gelang es den Hackern zuvor den Großteil der weltweiten Standorte lahmzulegen. Der Schaden des entstandenen Betriebsausfalls sei beträchtlich, so der Konzern. Still gestanden sind auch die Kassen des Großhändlers METRO. Vom Ausfall des IT-Systems waren einige Standorte und zahlreiche Kunden betroffen. Somit konnten keine Verkäufe abgewickelt werden, Online-Bestellungen waren nicht mehr möglich.

Schaden enorm

Die Liste der geschädigten Firmen und Institutionen ließe sich fortsetzen. Betroffen sind große und kleine Betriebe, keiner scheint sicher. Doch eines ist gewiss: es geht immer um sehr viel Geld. Bankraub war gestern, heute ist IT-Kriminalität angesagt. Das zeigen viele erfolgreiche Hacking-Angriffe. Durch die zunehmende Digitalisierung werden immer mehr Bereiche ins Netz verlagert. Die Bedrohungslage für Unternehmen steigt dadurch weiter. Experten sprechen von einem weltweiten Schaden von mindestens 20 Milliarden Euro. Die Dunkelziffer dürfte aber weitaus höher sein.