Cyber-Sicherheit

Hacker in digitaler Quarantäne

[14.12.2022] Städte, Gemeinden und Kreise werden immer öfter Opfer von Cyber-Angriffen. Veraltete IT-Lösungen machen es den Hackern zum Teil leicht, an sensible Daten zu kommen. Kommen können sich unter anderem mit virtuellen Browsern schützen.

Diesmal traf es die Verwaltung des Rhein-Pfalz-Kreises. Kriminelle Hacker hatten am 11. November 2022 deren IT lahmgelegt und zahlreiche Daten kopiert (wir berichteten). Schlimmste Befürchtungen wurden wahr als die Kommune der Lösegeldforderung nicht nachkam: Die Daten wurden im Darknet hochgeladen. Namen, Anschriften und Geburtsdaten von ukrainischen Geflüchteten, die in dem Landkreis untergebracht wurden, waren einsehbar. Auch war die Website der Kreisverwaltung mehrere Tage nicht vollumfänglich erreichbar. Ein Einzelfall ist das nicht. Im Oktober 2021 erbeuteten kriminelle Hacker Daten der Stadt Witten und veröffentlichten diese im Netz. Vielen ist außerdem der schwere Angriff auf die Kreisverwaltung Anhalt-Bitterfeld in Erinnerung. Die Bereitstellung öffentlicher Dienstleistungen war dort im Sommer 2021 so nachhaltig eingeschränkt, dass der Landkreis den Katastrophenfall ausrief. Auch nach Monaten war noch kein Regelbetrieb möglich. Für Kommunen und deren Bürgerinnen und Bürger haben solche Angriffe tiefgreifende Folgen. Sie reichen von der Einstellung von Sozialleistungen bis hin zum Leak ihrer persönlichen Daten.

Die Attacken nehmen zu

Erpressungsangriffe – in der Fachsprache als Ransomware-Attacken bezeichnet – nehmen laut Bundeskriminalamt (BKA) zu. Rasant ist der dadurch entstandene jährliche Schaden gestiegen: auf circa 24,3 Milliarden Euro im Jahr 2021. 2019 waren es noch 5,3 Milliarden Euro. Der durchschnittliche Schaden pro Attacke hat um 21 Prozent zugelegt. Und auch die Kommunen werden immer öfter Opfer solcher Angriffe. Zum einen sind die IT-Strukturen in Städten und Gemeinden häufig veraltet und nicht ausreichend geschützt. Zum anderen liegen durch die Digitalisierung der Behörden immer mehr persönliche Daten auf den Servern.
Bei den Angreifern handelt es sich laut BKA um eine hoch professionelle und organisierte Gruppe, die aus Cyber-Angriffen ein regelrechtes Geschäftsmodell gemacht habe. Das Einfallstor ist das Internet. Links werden über Phishing-E-Mails versendet, die vertrauenswürdig aussehen, deren Aktivierung jedoch einen Angriff initiiert. Mitarbeiterschulungen reichen als Schutz nicht mehr aus, da Phishing immer professioneller und authentischer wird. Eine Antiviren-Software ist auch keine Lösung, da sie nur bereits bekannte Malware erkennen kann. Bleibt der Weg, den Internet-Zugang vollständig einzuschränken. In Zeiten des Onlinezugangsgesetzes (OZG) und der digitalen Bürgerservices wäre das ein fataler Rückschritt.

Wie sich Kommunen wappnen können

Die gute Nachricht ist: Kommunen können sich vor Ransomware schützen und die Gefahr eines Angriffs minimieren. Durch Programmkorrekturen – so genannte Patches – lassen sich bekannte Fehler in Programmen ausbessern oder Sicherheitslücken schließen. Patches sollten regelmäßig und zeitnah auf alle Geräte im IT-Netzwerk aufgespielt werden.
Veraltete Systeme mit nicht mehr unterstützten Betriebssystemen, wie Windows XP, sollten keinesfalls in

einem mit dem Internet verbundenen Netzwerk laufen. Des Weiteren sollten Anhänge oder Links, die nicht zweifelsfrei sicherer Herkunft sind, ungeöffnet bleiben. Die Mitarbeitenden müssen entsprechend geschult werden. Sie sollten auch niemals Programme aus dem Internet herunterladen, die nicht von verifizierten Stellen angeboten werden. Regelmäßige Back-ups auf externen Datenträgern sichern wiederum den Zugang zu unternehmenskritischen Daten.
Zusätzlich gibt es sehr wirksame IT-Sicherheitstechnologien, mit denen sich Ransomware-Angriffe abwehren lassen. Der wichtigste Schutz ist die Absicherung des Internet-Zugangs. Am konsequentesten wird das durch eine Trennung von Internet und internem Netzwerk realisiert, denn dann kann Schad-Software nicht in das Basisbetriebssystem eindringen.

Cyber-Kriminellen den Zugriff verwehren

Praktisch umsetzen lässt sich das mit einem virtuellen Browser: Die Nutzer arbeiten mit einer vom Betriebssystem separierten Maschine. Entscheidend ist, dass es sich dabei um eine vollvirtualisierte Surf-Umgebung handelt. Dabei wird zusätzlich auf der Netzwerkebene der Zugang zum Internet vom Intranet getrennt. Ein solcher Browser ist beispielsweise der R&S Browser in the Box von Rohde & Schwarz Cybersecurity. Er schließt die Sicherheitslücke Internet sozusagen mit der digitalen Quarantäne für Hacker-Angriffe: Die Lösung ermöglicht eine konsequente Netzwerktrennung und schützt auch vor Angriffen über E-Mail-Anhänge oder bei Web-Konferenzen mit Mikrofonnutzung und Webcam-Unterstützung. Anstatt – wie bei Antivirenprogrammen – Schad-Codes zu erkennen, werden alle potenziell gefährlichen Aktivitäten in diesem virtuellen Browser isoliert. Jeder Browser-Start beseitigt die Schädlinge und versetzt den Browser in seinen Ausgangszustand. Kommt ein virtueller Browser zum Einsatz, haben Cyber-Kriminelle keine Chance.

()

Stichwörter: IT-Sicherheit, Ransomware, Phishing, Cyber-Sicherheit, Rohde & Schwarz Cybersecurity