Studie

Cyber-Angriffe auf die Verwaltung

[27.04.2022] Das Software-Beratungsunternehmen KonBriefing Research hat die zugänglichen Informationen zu weltweiten Cyber-Attacken auf die öffentliche Verwaltung im ersten Quartal 2022 ausgewertet. Deutsche Verwaltungen seien demnach wenig betroffen, dennoch gelte es, wachsam zu bleiben.

Wie ist es um die Cyber-Sicherheit in öffentlichen Institutionen bestellt? Wie stehen die Länder im internationalen Vergleich? Das Software-Beratungsunternehmen KonBriefing Research, das sich vor allem mit IT-Sicherheit befasst, hat von Januar bis März 2022 durchgeführte Cyber-Angriffe weltweit analysiert und stellt nun die Ergebnisse vor. Für den Zeitraum haben die Analysten von KonBriefing Research 61 erfolgreiche Cyber-Angriffe auf Einrichtungen der öffentlichen Verwaltung gezählt. Ziele waren vor allem Gemeinden, aber auch Regierungsinstitutionen und Justizbehörden. In vielen Fällen kam es zu erheblichen Störungen des Betriebs und zur Offenlegung von Daten.

Ransom-Attacken als häufigste Angriffsart

Die Angriffsarten waren vielfältig, besonders häufig waren jedoch Ransomware-Angriffe, mit denen Daten verschlüsselt und vorgeblich nur gegen Zahlung eines Lösegelds (ransom) freigegeben werden. Wird nicht gezahlt, werden die gestohlenen Daten im Darknet veröffentlicht. Durch die Verschlüsselung und den notwendigen Neuaufbau der IT ist der Betrieb in betroffenen Institutionen oft für längere Zeit stark beeinträchtigt. Andere Einrichtungen waren von Denial-of-Service(DDoS)-Attacken betroffen, welche die Verfügbarkeit von Internet-Diensten reduzieren.
Angriffe auf Einrichtungen in der Ukraine konnten in der Regel nicht einzelnen Organisationen zugeordnet werden, hier wurde nur übergreifend gezählt. Dabei wurde vor allem so genannte Wiper-Schad-Software in Stellung gebracht, die Daten auf den betroffenen Systemen löscht. In umgekehrter Richtung seien im Februar und März 2022 auch erste öffentliche Einrichtungen in Russland von Cyber-Angriffen betroffen gewesen, berichtet KonBriefing. Hier seien Angehörige des Anonymous-Kollektivs verantwortlich, die damit gegen den Krieg in der Ukraine protestieren wollten.

Behörden sollten wachsam bleiben

In Deutschland haben vor allem die erfolgreichen Cyber-Attacken auf die Städte Suhl in Thüringen und Dingolfing in Bayern Schlagzeilen gemacht. In deren Folge kam es zu wesentlichen Beeinträchtigungen der Dienste. Viele Angriffe hätten mit Phishing begonnen, so KonBriefing. Deshalb sei es wichtig, dass Behörden neben technischen und organisatorischen Schutzmaßnahmen auch das Bewusstsein ihrer Mitarbeitenden schärfen. Das sollte regelmäßig und „am besten verbunden mit praktischen Übungsangriffen erfolgen“, so der Rat der IT-Sicherheitsexperten.
Bisher sind die Verwaltungen in Deutschland im ersten Quartal 2022 offenbar glimpflich davongekommen. Dennoch belegten die Zahlen aus anderen Ländern wie etwa Frankreich, dass eine anhaltend hohen Bedrohung bestehe, mahnt der Geschäftsführer von KonBriefing Research, Bert Kondruß. Behörden müssten weiterhin sehr wachsam sein und kontinuierlich in die IT-Sicherheit investieren.

(sib)

Zur statistischen Auswertung der Cyber-Angriffe auf die Verwaltung

Stichwörter: IT-Sicherheit, KonBriefing Research, Cyber-Sicherheit