Anfrage der SPD-Ratsfraktion vom 24.07.2023
Hackerangriffe auf die städtische IT

Frage 1:
Wie hat sich die Zahl der Hackerangriffe auf die städtische IT in den letzten 12 Monaten im Vergleich zu den Vorjahren entwickelt und über welche Einfallstore finden Angriffe dieser Art statt?

Antwort:
Angriffe finden täglich in unterschiedlichen Ausprägungen statt, die Anzahl nimmt dabei weiter zu. Alleine im Monat Juli 2023 wurden vom System für den Zweckverband der ITK insgesamt 6,2 Millionen E-Mails als potentiell schädlich erkannt und abgewiesen und 1,1 Millionen E-Mails als potentiell unschädlich erkannt und zugestellt.

Ein Hackerangriff von außen findet häufiger und professioneller statt, läuft aber eher in Angriffswellen und ist breiter gestreut.

Weniger häufig, aber leider sehr gefährlich sind Angriffe, die es durch die unterschiedliche Awareness bei den Anwendern und Anwenderinnen, bis nach innen geschafft haben.

Einfallstore sind zum Beispiel:
- bösartige E-Mails mit Links zu kompromittierten Webseiten und anschließende Schadcode-Download
- Download / Installation von Software durch Anwender und Anwenderinnen
- gezielte Phishing-Mails (CEO-Fraud u.ä.)
- Besuchen von NSFW-Websites (not-safe-for-work)
- Verwendung von USB-Sticks (insbesondere bei gleichzeitiger privater Nutzung)

Frage 2:
Welche Maßnahmen zum Schutz vor Hackerangriffen und Ransomware verfolgt die Stadt Düsseldorf und wie werden diese Sicherheitsvorkehrungen weiterentwickelt?

Antwort:
Die wichtigsten Infektionsvektoren von Ransomware sind hauptsächlich Spam-Mails mit schadhaften Anhängen oder verlinkter Schadsoftware, sowie Schwachstellen auf Systemen.

Eine Maßnahme zum Schutz vor Ransomware und anderer Schadsoftware ist die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter sowie der Führungskräfte in den Fachbereichen.

Im technischen Bereich richtet sich die ITK Rheinland als IT Dienstleister der LHD bei der Informationssicherheit nach den aktuellen Sicherheitsstandards und setzt dabei verschiedene Endpoint Detection und Endpoint Protection Lösungen ein. U.a. wurden die möglichen E-Mail Anhänge –(Dateitypen) eingeschränkt und nicht jede/r Mitarbeitende kann Anhänge aus dem Internet runterladen. Ein Patch Management wurde etabliert, so dass Updates schnell und regelmäßig erfolgen und es erfolgen wiederkehrende Penetrationstestungen.

Dabei ist ein gutes Zusammenspiel von technischen und organisatorischen Maßnahmen wichtig, um bei neuen und bisher unbekannter Malware oder Zero Day Lücken schnell reagieren zu können.

Frage 3:
Welche Schäden sind bereits durch Hackerangriffe entstanden?

Antwort:
Laut Dienstleister gab einige Distributed Denial-of-Service (DDoS) Angriffe auf Webseiten, durch die bisher aber keine nennenswerten Schäden entstanden sind.