Cyber-Kriminalität

Es kann jeden treffen

[17.03.2022] Cyber-Kriminalität verspricht große Gewinne, während das Risiko, entdeckt zu werden, gering ist. Im Interview spricht Thomas Stasch, Leiter des KomCERT der regio iT, über die aktuellen IT-Gefahren für Kommunen und wie sich diese davor schützen können.

Herr Stasch, Cyber-Angriffe haben sich deutlich gehäuft. Entspricht das den Tatsachen oder werden einfach mehr IT-Sicherheitsvorfälle gemeldet?

Cyber-Kriminalität ist in der Tat stark angestiegen. Das zeigen auch die Statistiken der Ermittlungsbehörden. Die ‚dunkle Seite der Macht' entdeckt immer mehr Einnahmemöglichkeiten, und die Geldsummen sind ja ziemlich gigantisch. Cybercrime ‚lohnt sich' quasi und verspricht große Margen, während das Risiko, entdeckt zu werden, gering ist. Zudem gibt es sozusagen auch Verbrechen on demand: Kriminelle können sich Ransomware-Trojaner kaufen, mieten sich eine Infrastruktur im Hintergrund as-a-Service dazu, sind dann nur noch für die Verteilung zuständig und kassieren einen Teil des Lösegelds. Es wird immer einfacher.

Es gab immer die Tendenz, Sicherheitsvorfälle zu verschweigen und auszusitzen. Hat sich daran etwas geändert?

Das kommt vor allem auf die Beteiligten an. Uns wird tatsächlich manchmal nahegelegt, dass der Vorfall geheim bleiben muss. Das bringt aber wenig, denn wenn es herauskommt, sind der Ärger und Vertrauensverlust umso größer. Es ist besser, gleich offen zu kommunizieren.

Im vergangenen Jahr gab es massive Cyber-Angriffe mit immensen Schäden. Lohnen sich professionelle IT-Sicherheitsmaßnahmen überhaupt?

Es kann wirklich jeden treffen, egal ob BSI-zertifiziert nach ISO 27001 oder nicht. Die Frage lautet: Wie interessant ist man für Angreifer? Viele Cyber-Attacken sind immer noch Zufallstreffer. Grundsätzlich gibt es Angriffe auf IT-Schwachstellen über das Internet oder Phishing-Attacken per E-Mail. Hier ist allerdings eine Verschiebung zu beobachten. Vor zwei Jahren kamen 95 Prozent der Angriffe über E-Mail, jetzt sind es grob geschätzt noch 70 Prozent. Immer häufiger werden Sicherheitslücken aufgespürt, wie unlängst die Exchange-Schwachstelle oder Log4j. Wenn die Betreiber dann nicht schnell genug im Umgang mit dem Patch-Management sind, platzieren Angreifer eine Hintertür und planen in aller Ruhe den Cyber-Angriff, indem sie das System ausspionieren und sondieren, ob sich Aufwand und Nutzen lohnen. Eine große Rolle spielt allerdings, wie man im operativen Bereich bei der IT-Sicherheit aufgestellt ist. In der Industrie sind so genannte Security Operation Center (SOC) längst verbreitet, wo Leute sitzen, die nichts anderes tun, als nach dem Feind im Netz zu suchen – nach einer irgendwo schlummernden Software oder einem aktiven Angreifer.

Was macht eine Kommune attraktiv für einen Angreifer?

Attraktiv ist eine Kommune, wenn der Angreifer glaubt, Gewinn erzielen zu können. Denn wenn er es schafft, eine Kommune oder ein Unternehmen lahmzulegen, sodass sie nicht mehr handlungsfähig sind, steht häufig eine Lösegeldzahlung an. Während früher Daten von Angreifern verschlüsselt und eine

Zahlung für den Schlüssel verlangt wurde, werden heute Daten häufig noch kopiert. Wenn die Opfer dann nicht für die Entschlüsselung zahlen wollen, drohen Angreifer mit der Veröffentlichung der Daten. Das ist kein schönes Szenario bei personengebundenen Daten in Kommunen.

„Cybercrime ‚lohnt sich' quasi und verspricht große Margen. Das Risiko, entdeckt zu werden, ist gering." Im Dezember vergangenen Jahres kam es zum Log4j-Vorfall. Wie verbreitet ist die Software in Kommunen?

Es gibt keinen großen Unterschied zwischen der kommunalen Welt und der Industrie. Jeder, der Java entwickelt und mit dem Logging von Informationen befasst war, hat in der Regel Log4j als eine der Standardbibliotheken eingebunden. Entsprechend groß war auch die Verbreitung. Wir haben allerdings bemerkt, dass häufig noch die Version 1.x im Einsatz war, und die war vom Vorfall nicht betroffen. Sich dann aber zurückzulehnen und zu glauben, alles wäre gut, unterschlägt die Tatsache, dass diese Version seit 2015 gar nicht mehr gepflegt wurde. Inzwischen gibt es Update-Patches für Log4j, man muss aber parallel die Software aktualisieren, welche die Bibliotheken verwenden.

Gerade im öffentlichen Sektor soll vermehrt Open Source Software eingesetzt werden. Ist deren professionelle Pflege in jedem Fall gewährleistet?

Die Schwachstelle, die wir beim Open-Source-Produkt Log4j beobachtet haben, kann genauso bei jedem kommerziellen Produkt auftreten. Das ist ja auch kürzlich bei der Schwachstelle in Exchange geschehen. Microsoft reagiert dann natürlich sehr schnell mit Patches. Aber auch bei Log4j ist die Schwachstelle schnell angegangen worden.

Wie müssen Kommunen ihre IT-Infrastrukturen schützen?

Kommunen müssen in der Lage sein, ein vernünftiges Patch-Management zu betreiben. Sie müssen die entsprechenden Sicherheitsexperten im Haus haben oder sich das Know-how extern einkaufen. Eine Situation wie mit Log4j wird eine kleine Kommune selbst kaum bewerten können. Wichtig ist, seine Systeme im Griff zu haben und genau zu wissen, was man selbst betreibt. Indem wir uns mit anderen Diensten koppeln, in die Cloud gehen, die städtische Infrastruktur digitalisieren und Sensorennetze für die Smart City aufbauen, werden wir immer vernetzter. Solche Netze müssen sauber von den inneren Netzen getrennt werden. Zudem müssen sich Kommunen Gedanken darüber machen, wie sie die Infrastruktur überwachen wollen.

Können kleinere Kommunen das überhaupt leisten und worauf müssen sie sich einstellen?

Darauf, dass sie irgendwann einen Sicherheitsvorfall haben. Das Problem ist, dass Kommunen nicht überall den Druck haben, Informationssicherheit umzusetzen. Das ist Ländersache und je nach Bundesland unterschiedlich. Es gibt Länder, die das per Gesetz festschreiben, und andere, die sich wegen des Konnexitätsprinzips an eine Gesetzgebung nicht herantrauen. Denn dann müssten sie dafür bezahlen. Aber wenn einmal die Einwohnermeldedaten geraubt wurden, müssen Kommunen sich fragen, wie sie vor ihren Bürgern dastehen. Das ist ein schmerzhafter Lernprozess. Besser wäre es, wenn die Regierung zu der Einsicht gelänge, dass man Kommunen hinsichtlich der IT-Sicherheit mehr in die Pflicht nehmen muss. Angesichts der dort vorgehaltenen kritischen Daten stellt sich ohnehin die Frage, ob sie nicht eine Einstufung als kritische Infrastruktur verdienen und damit auch dem Zwang ausgesetzt wären, gewisse Sicherheitsmaßnahmen umzusetzen.

()

Dieser Beitrag ist in der Ausgabe März 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Cyber-Sicherheit