

Geheimdienste stehlen Stadt-Daten

Essen. Das Hans Sachs-Berufskolleg in Oberhausen hatte Glück im Unglück. Anfang Februar hackten sich Unbekannte in den Verwaltungsrechner der Schule. Der Plan der Hacker war kriminell: Sie wollten Geld vom Schulkonto ins Ausland abzweigen. Die Hacker scheiterten.

Der Oberhausener Schulleiter Marc Bücher glaubt, dass die sorgsame Pflege des Virenschutzes den Angriff vereitelt hat. Die Angreifer müssen über Passwörter und Zugangsdaten verfügt haben. Schlimm genug. Die Essener Kripo ermittelt. Für Frank Herrmann von der Landtagsfraktion der Piraten kommt ein Vorgang wie der in Oberhausen nicht überraschend: Kommunale Computernetze in NRW seien „löchrig wie ein Schweizer Käse“, sagt er.

Ein Passwort reicht

Tobias Morsches hat die Befürchtungen auf breiter Front bestätigt. Der Computer-Experte hat in fünfzehn Kommunen des Landes Netze getestet. Zwischen zwei und acht Stunden hat er im Schnitt gebraucht, um in sie einzudringen. „An vielen Stellen haben wir niedrige Sicherheitsschwellen“, sagt er.

Beruf des Mannes ist es, unbemerkt Datenbanken zu hacken, um deren Eignern anschließend darzulegen, wie sicher oder unsicher ihre Daten verwahrt sind. Mit einem bunten Mix an Methoden weist er Lecks und Nachlässigkeit nach. „Wir haben Phishing-Attacken gemacht, zu 80 Prozent erfolgreich.“ Man habe übers Internet – so über Bürgerportale – hineingefunden, sei zu Fuß ins Rathaus gegangen: „Dann gucken wir, ob irgendwo Netzwerkdozen auf dem Gang oder in anderen für Besucher erreichbaren Bereichen zugänglich sind. Wir schließen uns an und greifen zu.“

„Sie brauchen nur einen ständigen Mitarbeiter dieser Verwaltung“

Zu den frechsten Varianten der im Fachjargon „Penetrationstests“ genannten verdeckten Prüfungen gehört es, an die Büros der Stadtbediensteten zu klopfen. „Guten Tag, IT“, sagen Morsches und seine Mitarbeiter. „Wir wollen die Rechner inventarisieren.“ Oft dürfen sie – und sind, frei nach Boris Beckers Werbespot, wenig später „drin“.

„Sie brauchen nur einen ständigen Mitarbeiter dieser Verwaltung“, berichtet Morsches, „mit seinem Passwort kommen Sie auf Dateifreigaben und Gruppenlaufwerke.“ Wenn er einen Account ergaunert habe, dann sei er „in fünf bis zehn Minuten auch Administrator“ – der Herr der Daten der Stadt.

Kommunen wissen viel. Sie kennen das Gehalt des Antragstellers für einen Kita-Platz, den Umsatz eines gewerbesteuerpflichtigen Betriebs, wie ein Schüler die letzte Klausur schrieb oder, der Extremfall: wie ein vom Staat mit einer Tarnidentität versehener Zeuge wirklich heißt und wo er wohnt.

2000 bis 3000 Angriffe täglich auf Rechner von Ministerien und Kanzleramt

Rechner von Ministerien und Kanzleramt sind 2000 bis 3000 Angriffen ausgesetzt. Täglich. 100 davon sind ernst, glaubt das Bundesamt für die Sicherheit in der Informationstechnik. Wie oft greifen Hacker Städte-Daten an – und ab?

Tatsächlich wird das von den Betroffenen meist entweder nicht bemerkt oder „unter den Tisch gekehrt“, wie der Landtagsabgeordnete Frank Herrmann von den Piraten glaubt. Eine Ausnahme: Kölns Stadtverwaltung ist offensiv damit umgegangen, als Unbekannte Weihnachten 2012 gezielt die Melddatei knacken wollten. Nach den Feiertagen fanden die Beamten eine blockierte Einwohnerliste vor. Die Firewall hatte die Attacke abgewehrt, aber keinen Alarm geschlagen. In einem weiteren NRW-Fall hat eine Verwaltung Hinweise, dass sie über längere Zeit einen Geheimdienst zu Gast hatte. Was ein Geheimdienst mit städtischen Daten will? Einmal im Netz, kommt er an Informationen aus den verbundenen Netzen von Bund und Ländern.

Größtes Problem, so Morsches: „Die Kommunen wissen nicht mehr wirklich, wo die ganzen Daten liegen.“ Jeder Mitarbeiter lege Kopien „irgendwo ungeschützt ab“. Seine Empfehlung: Nicht zentralisieren. Aber mehr Zusammenarbeit sei nötig, mehr Sorgfalt der Mitarbeiter, die Frage: „Welche Sicherheitsstufen haben unsere Daten?“ Und im Ernstfall: Zurück zum Papier.

Was Städte sagen und was Kritiker glauben: **Der Geschäftsführer des Städtetages NRW, Stephan Articus**, versichert: „Datensicherheit wird in den Stadtverwaltungen groß geschrieben.“ Es sei eine permanente Aufgabe, sensible Daten der Bürger vor Missbrauch zu schützen. Städte würden regelmäßig den Schutz kontrollieren.

Dagegen glaubt **Frank Herrmann, Landtagsabgeordneter der Piraten**: „Es gibt eine riesige Dunkelziffer von Vorfällen, die nicht öffentlich gemacht werden.“