

Angriffe wird es immer geben

Öffentliche Einrichtungen rücken zunehmend in den Fokus von Cyberkriminellen und staatlich gelenkten Hackern. Kommune21 sprach mit regio-iT-Geschäftsführer Stefan Wolf darüber, wie Städte und Gemeinden den Gefahren begegnen können.

Herr Dr. Wolf, welche IT-Sicherheitsbedrohungen sehen Sie derzeit als die größten Herausforderungen für öffentliche Einrichtungen?

Laut dem aktuellen Jahresbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) bleibt Ransomware die größte Herausforderung. Die Angriffsvektoren haben sich nicht wesentlich geändert: Phishing, das Ausnutzen von Schwachstellen und zunehmend die Nutzung von User-IDs aus Datenlecks. Diese Bedrohungen beschäftigen uns massiv. Hinzu kommt, dass Angreifer zunehmend KI-Tools einsetzen, um Angriffe mit einem hohen Automatisierungsgrad durchzuführen.

regio iT hat ein Computer Emergency Response Team, KomCERT, ins Leben gerufen. Welche Aufgaben und Ziele hat das KomCERT?

Das KomCERT wurde bereits 2017 gegründet, zunächst als Informationsdrehscheibe für unsere Kunden zu Bedrohungslagen und Sicherheitsvorfällen. In den vergangenen Jahren hat sich der Fokus verändert. Heute steht die Beratung im Vordergrund: Security Assessments, Beratung zu neuen Technologien und Unterstützung bei Sicherheitsvorfällen – von

Phishing-Mails bis hin zu Vor-Ort-Einsätzen bei erfolgreichen Angriffen. Daneben bieten wir klassische Dienstleistungen wie den Warn- und Informationsdienst und die Vernetzung mit dem BundesCERT und den LandesCERT an.

Stellen wir uns einen konkreten Fall vor. Ein IT-Verantwortlicher einer Kommune stellt fest, dass alle Daten verschlüsselt wurden. Was sind die ersten Schritte, die er unternehmen sollte?

Die ersten Schritte hängen vom Status des Angriffs ab. Ist der Angriff noch im Gange, sollten Internet-Verbindungen und externe Zugänge sofort unterbrochen und die Systeme in einen sicheren Modus gebracht oder heruntergefahren werden. Ist der Angriff bereits erfolgt, muss eine gründliche forensische Analyse durchgeführt werden, um das Ausmaß und den Status des Angriffs festzustellen. Parallel dazu müssen die weiteren Schritte eingeleitet werden, wie etwa das Einberufen eines Krisenstabs und die Kommunikation nach innen und außen.

Wie wichtig ist in solchen Fällen die Zusammenarbeit mit der Polizei?

Wir empfehlen, sofort die Ermittlungsbehörden einzuschalten, da es sich bei Cyberangriffen um



regio iT GmbH

Dr. Stefan Wolf

Straftaten handelt und die Polizei mit Rat und Tat zur Seite steht. Sie verfügt über Spezialeinheiten zur Cyberabwehr und für Verhandlungen mit Ransomware-Tätern. Die Ermittlungsbehörden, insbesondere in Nordrhein-Westfalen, sind gut vorbereitet und haben mittlerweile große Erfahrung und Kompetenz in diesem Bereich.

Welche technischen Maßnahmen werden getroffen, um Daten nach einem Angriff zu retten?

Zunächst muss eine forensische Analyse durchgeführt werden, um das Ausmaß des Schadens zu ermitteln. Es sollten mehrere forensische Werkzeuge mit einem Vier-Augen-Prinzip eingesetzt werden, um eine größtmögliche Sicherheit über den Schaden und die Wiederanlauf-

möglichkeiten zu erhalten. Diese Analysen sind oft sehr langwierig und umfangreich.

Was ist zu tun, um zum Normalbetrieb zurückzukehren?

Die Rückkehr zum Regelbetrieb erfordert einen klaren Wiederanlaufplan. Es muss genau überlegt werden, in welcher Reihenfolge und mit welcher Priorität die Systeme wieder hochgefahren werden sollen. Dabei spielen technische Möglichkeiten wie abgeschottete Bereiche oder die Unterstützung

kaum vorstellbar. Im privatrechtlichen Bereich mag es Fälle geben, in denen die Abwägung zwischen Schaden und Lösegeld zu einer Zahlung führt. Wir empfehlen aber immer, die Ermittlungsbehörden einzubeziehen, da viele Lösegeldzahlungen nicht zu einer effektiven Entschlüsselung der Systeme führen.

Welche Maßnahmen sollten öffentliche Einrichtungen ergreifen, um sich besser gegen Cyberangriffe zu schützen?

Eine grundlegende Cyberhygiene ist notwendig: Passwort-Manage-

Sie helfen, Anomalien zu erkennen und automatisiert auf Angriffe zu reagieren. Auch Logfile-Analysen durch KI werden immer wichtiger, da Menschen diese komplexen Datenstrukturen nicht alleine bewältigen können.

Wie können Kommunen von der Zusammenarbeit mit regio iT und dem KomCERT profitieren?

Neben den Notfalldienstleistungen des KomCERT bieten wir eine Reihe von Präventions- und Detektionsprodukten an, die vor

„Für die Mehrzahl der Kommunen können wir das Sicherheitsniveau deutlich verbessern.“

durch Hard- und Software-Hersteller eine Rolle. Auch die Menge der wiederherzustellenden Daten hat einen großen Einfluss auf den Wiederanlaufprozess.

Welche Schulungs- und Sensibilisierungsmaßnahmen können Sie empfehlen, um Angriffen vorzubeugen?

Cybersecurity sollte in die Regelkommunikation jeder Organisation integriert werden, ähnlich wie Arbeitssicherheit und betriebliches Gesundheitsmanagement. Regelmäßige Awareness-Veranstaltungen für Mitarbeitende und technische Schulungen für IT-Mitarbeitende sind unerlässlich. Dazu gehört auch die regelmäßige Information über aktuelle Phishing-Kampagnen.

Was raten Sie betroffenen Institutionen im Umgang mit Lösegeldforderungen?

Im öffentlich-rechtlichen Bereich halte ich Lösegeldzahlungen für

ment, Sicherung externer Zugänge, regelmäßige Schwachstellen-Scans und aktuelles Patch-Management. Diese Maßnahmen können das Sicherheitsniveau deutlich erhöhen.

Wie sieht ein gutes Back-up-Management aus, um Daten im Falle eines Angriffs zu schützen?

Das Back-up-Management sollte dem 3-2-1-Prinzip folgen: drei Kopien auf zwei verschiedenen Medien, eine davon ausgelagert. Zusätzlich empfehle ich so genannte Cybervaults, das sind abgekoppelte Umgebungen, die Back-ups enthalten und nicht manipulierbar sind. Diese Back-up-Tresore sollten nur einem begrenzten Personenkreis zugänglich sein.

Welche Technologien können zur Erhöhung der Cybersicherheit beitragen?

KI-basierte Lösungen wie Extended Detection and Response (XDR) sind bereits heute unverzichtbar.

Ort eingesetzt werden können. KomCERT unterstützt auch bei individuellen Security Assessments und der Entwicklung von Notfallkonzepten. Unser großes Netzwerk bietet zusätzliche Unterstützung und Ressourcen.

Es gab krasse Fälle, wo Gemeinden wochenlang lahmgelegt waren. Wie optimistisch sind Sie, dass sich solche Fälle nicht wiederholen?

Angriffe wird es immer geben, denn die Intensität der Angriffe nimmt nicht ab. Aber ich bin optimistisch, dass wir mit den richtigen technischen Maßnahmen viele Angriffe erfolgreich abwehren oder schnell erkennen und reagieren können. Bei staatlich gelenkten Akteuren mit großen Ressourcen wird es schwieriger, aber für die Mehrzahl der Kommunen können wir das Sicherheitsniveau deutlich verbessern.

Interview Alexander Schaeff