Empfehlungen zum Schutz vor Cyberrisiken in Gemeinden

Von der Stadtverwaltung bis zum Stromversorger: Cyberattacken können alle treffen. Die Kantonspolizei Bern und der Sicherheitsverbund Schweiz illustrieren am Beispiel einer Gemeinde, was passieren kann und wie man sich schützt.

Die Digitalisierung eröffnet der Verwaltung neue Möglichkeiten, mit der Bevölkerung in Kontakt zu treten und die Effizienz von Dienstleistungen zu steigern. Zugleich erfordert sie eine Neuorganisation der Prozesse und führt zu einer grösseren Abhängigkeit von einer funktionierenden Informationstechnologie-Infrastruktur. Diese Vernetzungen und Abhängigkeit nutzen Kriminelle aus. Von der Stadtverwaltung bis hin zu Stromversorgern – es kann alle treffen.

Der vorliegende Artikel ist im Rahmen der Implementierung des Umsetzungsplans der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 (NCS) entstanden. Anhand eines konkreten Beispiels einer Gemeinde wird illustriert, wie die Verwaltungstätigkeit aufgrund eines Cyberangriffs eingeschränkt oder allenfalls sogar lahmgelegt werden kann und welche Schäden daraus resultieren können. Für den Schutz vor Cyberangriffen sind nachfolgend konkrete Empfehlungen aufgelistet sowie die Vorgehensweisen, wenn es dennoch zu einem Vorfall kommt.

Der Angriff auf eine Gemeinde

Mithilfe einer E-Mail haben Cyberkriminelle bei einem Mitarbeiter einer Schweizer Gemeinde eine Malware platziert, mit der sie in der Lage waren, die Bildschirminhalte eines Rechners zu sichten und die Eingaben aufzuzeichnen. Zudem hatten sich die Kriminellen Zugang zu anderen Rechnern im lokalen Netzwerk der Gemeinde verschafft.

Um Zahlungen an Dritte zu tätigen, nutzte die Gemeinde eine Zahlungssoftware. Die kommunale Verwaltung hatte richtigerweise erkannt, dass Zahlungen nur an einem separaten Computer vorgenommen werden sollten. Da dieser sich jedoch im gleichen Netz wie der Rechner des befallenen Mitarbeiters befand, konnten die Kriminellen auf den Zahlungscomputer zugreifen. Ausserdem erfüllte die Zahlungssoftware zum

«Verwenden Sie sichere Passwörter, mindestens 12 Zeichen, Zahlen wie auch Sonderzeichen, in Kombination mit einer Zwei-Faktoren-Authentifizierung und pro Dienst ein anderes Passwort»: So lautet eine der Empfehlungen zum Schutz vor Cyberattacken. *Bild: Kantonspolizei Zürich*

damaligen Zeitpunkt nur ungenügend die zwingenden Sicherheitsanforderungen, zum Beispiel keine Zwei-Faktor-Authentifizierung. Als der Buchhalter sich in das Zahlungsprogramm einloggte, zeichneten die Hacker die Log-in-Daten auf.

Eines Tages legten die Hacker das gesamte System der Gemeinde mit einem Distributed Denial of Services (DDoS)-Angriff – einer Überlastattacke – lahm. Bei einem solchen Angriff werden die Dienste wie zum Beispiel der Internetauftritt, der Mailservice oder die digitale Telefonanlage überlastet und fallen aus. Die Störungen bzw. der Ausfall dieser Dienste lenkte die Mitarbeitenden der Gemeinde ab, was den Hackern die nötige Zeit verschaffte, im Hintergrund eigene Zahlungsaufträge zu erfassen. So wurde die Gemeinde um mehrere Tausend Franken bestohlen.

Die Polizei wurde umgehend kontaktiert. Spezialisierte Mitarbeitende berieten und unterstützten die Gemeinde im weiteren Vorgehen, sicherten Spuren und ermittelten.

Wie Sie Ihre Verwaltung schützen können

Vor Cyberangriffen kann man sich schützen, indem sowohl technische als auch organisatorische Massnahmen ergriffen werden.

- Regeln Sie die Verantwortlichkeiten und Schnittstellen.
- Regeln Sie den Umgang mit Informationen und schützenswerten Daten.
- Schulen Sie Ihre Mitarbeitenden und Gemeinderatsmitglieder, speziell auch im Umgang mit E-Mails.
- Verwenden Sie sichere Passwörter (mind. 12 Zeichen, Zahlen wie auch Sonderzeichen) in Kombination mit einer Zwei-Faktoren-Authentifizierung und pro Dienst ein anderes Passwort.
- Verwenden Sie für Zahlungen einen separaten Computer, auf welchem Sie nicht im Internet surfen und keine E-Mails empfangen. Sprechen Sie mit Ihrem IT-Dienstleister über die Möglichkeit, Ihre Onlinezahlungen in einem von den restlichen Anwendungen abgegrenzten Bereich (Sandboxing) oder in einem dezidierten, besonders geschützten, virtualisierten System zu tätigen. Sämtliche Prozesse, welche den Zahlungsverkehr betreffen, sollten verwaltungsintern klar geregelt sein, zum Beispiel mit dem Vier-Augen-Prinzip und der Kollektivunterschrift.
- Erstellen Sie ein Krisen- sowie ein Kommunikationskonzept.
- Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt. Lagern Sie eine zusätzliche Kopie Ihres Back-ups getrennt (offline) und ausser Haus (offsite) aus.
- Implementieren Sie Antivirensoftware zur Erkennung und Vermeidung einer Infektion durch Schadsoftware, und halten Sie Ihre Systeme auf dem aktuellsten Stand.
- Sensible Daten sollten nie unverschlüsselt in der Cloud abgelegt werden. Verwenden Sie möglichst einen Schweizer Cloud-Anbieter.
- Aktivieren Sie spezielle Regeln für Firewalls und geografische Zugriffseinschränkungen (zum Beispiel Zugriffe nur aus der Schweiz).
- Schützen Sie Fernzugriffe auf Ihr Netzwerk keinesfalls mit einer einfachen Authentisierung (Benutzername und Passwort). Nutzen Sie mindestens eine Zwei-Faktor-Authentisierung oder setzen Sie eine sicherere Verbindung über ein virtuelles privates Netzwerk (VPN) ein. Dies gilt auch für den Zugriff von externen IT-Dienstleistern und Administratoren.

Tragen Sie zur Täterermittlung bei

Falls es trotz Schutzmassnahmen zu einem Cyberangriff kommt, wird empfohlen, umgehend die zuständigen Behörden und Dienstleister zu kontaktieren. Je länger Sie damit zuwarten, umso grösser ist die Wahrscheinlichkeit, dass wertvolle Spuren verwischt werden. Die Polizei ist nicht an Ihren Verwaltungsgeheimnissen interessiert und wirkt nicht auf Ihre Infrastruktur ein. Sie sucht bei einem Angriff nur nach Informationen und Spuren, die für die Aufklärung der Straftat relevant sind. Die Polizei nimmt Sie sehr ernst und spricht in der Regel Strafverfolgungsmassnahmen zuerst mit Ihnen ab. In den meisten Fällen kann eine Vorgehensweise gefunden werden, welche für beide Seiten stimmt.

Kantonspolizei Bern und Sicherheitsverbund Schweiz

Infos:

[1] Sicherheitsverbund Schweiz (2019). Umsetzungsplan der Kantone. URL: https://www.svs.admin.ch/de/themen-/Cybersicherheit/Cybersicherheit-Kantone.html (Stand: 30.03.2020).

[2] Informatiksteuerungsorgan des Bundes (2018). Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 (NCS). URL: https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie.html (Stand: 30.03.2020).