Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

focus 5/23
November

STANDPUNKT

Cybersicherheit: Kräfte und Kompetenzen bündeln

Natacha Litzistorf
Mitglied der Stadtregierung von Lausanne, Leiterin Wohnungswesen, Umwelt und Architektur

In den letzten Jahren stellten sich Cyberangriffe als immer häufiger und komplexer heraus und betrafen zunehmend private und öffentliche Akteure. Über mehrere Attacken auf Gemeinden wurde in den Medien intensiv berichtet – häufiger übrigens als über private Betroffene. In der Politik löste dies einen echten, aber positiven Schock aus. Denn damit wurde uns stärker bewusst, dass «IT eine strategische öffentliche Politik ist» und dass Sicherheit und Datenschutz den Eckpfeiler dieser Politik darstellen. Diese brutalen Ereignisse haben uns dazu bewogen, eine angemessenere Haltung einzunehmen und mehr öffentliche Gelder in diesen Bereich zu investieren, Bescheidenheit zu zeigen, da niemand vor solchen Angriffen sicher ist, diskret vorzugehen und unsere taktischen Vorgehensweisen nicht offenzulegen, gleichzeitig aber die Bevölkerung zu informieren, und vor allem zusammenzuarbeiten und uns unter öffentlichen und privaten betroffenen Akteuren auszutauschen.

Am 14. Juni stellte die Lausanner Gemeindeverwaltung einen Cyberangriff auf im Internet exponierte Dienste fest. Eine sofort erfolgte Diagnose ergab, dass es sich um eine sog. Distributed-Denial of Service-Attacke (DDoS) handelte. Die Folge davon war hauptsächlich die Nicht-Verfügbarkeit der städtischen Webseiten. Das Notfallprotokoll wurde aktiviert, u.a. um die Beteiligten zu informieren und in Zusammenarbeit mit Kanton und Bund angemessene Massnahmen zu ergreifen. Dank dieser koordinierten Aktionen konnte die Intensität der Angriffe zum Schutz von Server und Daten gemildert werden.

Diese Attacke erlaubte uns, neue Erkenntnisse zu gewinnen sowie Aspekte zu bestätigen, die uns zumindest theoretisch bereits bekannt waren. Der Austausch von Informationen zwischen den betroffenen Städten ist entscheidend. In Krisensituationen sind wir alle voll und ganz mit der Suche nach Lösungen beschäftigt. Daher wäre es hilfreich, zur Erleichterung der Verbindungen mit Politik und Verwaltung über ein «Koordinationstool» zu verfügen. Kommunikation bleibt das Kernelement: Innerhalb des politisch-administrativen Systems ist sie von grundlegender Bedeutung, denn jeder muss seine Rolle und Verantwortlichkeiten kennen. Die Kommunikation mit dem Parlament muss geplant sein und unmittelbar nach der internen erfolgen. Gegenüber der Öffentlichkeit muss sie transparent sein, ohne dabei böswilligen Absichten Vorschub zu leisten. In den sozialen Netzwerken gilt es, Gerüchte zu dementieren. Die Erkenntnis, dass Krisenvorbereitung der Schlüssel zur Krisenbewältigung ist, liegt auf der Hand.

In unserer Sicherheits- und Datenschutzpolitik muss besonders auf den menschlichen Faktor gepocht werden. Durch obligatorische Weiterbildungskurse sowie regelmässige interne Information können wir Sensibilisierungsarbeit leisten und das Bewusstsein für die Herausforderungen schärfen. Und auch hier könnte auf Ebene der Städte auf Gegenseitigkeit gesetzt werden. Dies ist die Voraussetzung für einen Kulturwandel und für eine bessere Vorbereitung unsererseits auf die Cyberwelt, stets mit Kompetenz, Entschlossenheit und Bescheidenheit.

Liebe Leserin, lieber Leser

In einer zunehmend vernetzten Welt, in der digitale Technologien unseren Alltag dominieren, spielt Cyber Security eine entscheidende Rolle für die Sicherheit und Stabilität der Städte.

Soziale Netzwerke, Online-Kommunikation und E-Government sind allgegenwärtig für die Bevölkerung und die Mitarbeitenden – und somit anfällig für Cyberangriffe. Dasselbe gilt für stark digitalisierte und kritische Infrastrukturen wie Wasser- und Stromversorgung, Verkehrssysteme und Gesundheitseinrichtungen.

Die Städte müssen somit in die Sicherheit ihrer digitalen Infrastruktur investieren und ihre Mitarbeitenden sensibilisieren. Wir erfahren im «focus»: Wie geht Lausanne damit um? Was sagt der politisch Verantwortliche aus Biel? Und: Was empfiehlt das Nationale Zentrum für Cybersicherheit? Sie erfahren es in der vorliegenden Ausgabe des «focus».

Wir wünschen Ihnen gute Lektüre!

Inhalt

INTERVIEW

«Sensibilisierung allein reicht nicht aus»

Beat Feurer,
Gemeinderat der Stadt Biel

Beat Feurer (SVP) ist Gemeinderat (Exekutive) der Stadt Biel. Er wurde 2012 in die Stadtregierung gewählt und leitete bis März 2023 die Dirketion Soziales und Sicherheit.

Seit April 2023 ist der 63-Jährige Finanzdirektor. In dieser Funktion ist er auch für die Abteilung Informatik und Logistik und somit für die Cyber Security zuständig.

Als politisch zuständige Person für die Informatik: Welche Bedeutung nimmt die Cyber Security für Biel ein?

In den letzten Jahren hat sich diese Thematik entwickelt und die Stadt Biel hat viel in diesen Bereich investiert. Was das Management der Informationssicherheit betrifft, so beachten wir die Empfehlungen der Norm ISO 27001.

Wurden Sie bereits Opfer eines Angriffs?

Wie jede andere Organisation erleiden wir täglich Angriffe. Bis heute hatte keine davon ernsthafte Konsequenzen für die Sicherheit unserer Systeme und die darin enthaltenen Daten.

Stand heute: Sind Sie für einen allfälligen Angriff gut gerüstet?

In den letzten drei Jahren haben wir viel in diesen Bereich investiert. Dass wir nie vollständig vor solchen Angriffen sicher sind, ist selbstredend. Doch wir haben auf jeden Fall die notwendigen Massnahmen ergriffen, um Cyberattacken zu verhindern und im Problemfall rasch reagieren zu können.

Was sind die grossen Herausforderungen, um die Stadt und ihre Bevölkerung so gut als möglich vor einem weiteren Angriff zu schützen?

Heute bleibt der menschliche Faktor das Hauptrisiko. Deshalb legen wir besonderen Nachdruck auf die Sensibilisierung. Doch Sensibilisierung allein reicht nicht aus. Ein entscheidender Punkt liegt ebenfalls darin, dass die Mitarbeitenden der Verwaltung über abgesicherte Tools verfügen. Die rasche Bereitstellung dieser Tools ist für die Abwehr der Angriffe unabdingbar. Leider gehen unsere aktuellen Verwaltungsprozesse nicht immer mit den technologischen Entwicklungen einher, was uns mitunter in unserer Reaktionsfähigkeit beeinträchtigen kann.

Welche konkreten Massnahmen wurden ergriffen, um Daten der Bevölkerung und die städtische Infrastruktur vor Cyberangriffen zu schützen?

Wir arbeiten auf folgenden Ebenen:
- Erstellung von klar definierten regulatorischen Rahmenbedingungen für die Sicherheit, welche Richtlinien über den Schutz von Informationen und über die sachgerechte Verarbeitung der Daten einschliessen.
- Unterstützung der Mitarbeitenden der Verwaltung durch Schulungen mit Schwerpunkt auf die Risiken im Bereich Informationssicherheit, Sensibilisierung durch Simulation realer Cyberangriffe und Bereitstellung leistungsstarker Tools
  - Einsatz von fortschrittlichen Tools zur Überwachung unserer Systeme, zur Erkennung von Eindringungsversuchen und zur Reaktion bei Angriffen.
- Zusammenarbeit mit den anderen Verwaltungen.

Wie verläuft die Zusammenarbeit mit anderen Gemeinden, dem Kanton und dem Bund bezüglich Cybersecurity?

Wir arbeiten eng mit allen Verwaltungsebenen zusammen, dies reicht von interkommunalen Austauschgruppen bis hin zur Unterstützung, die wir vom Nationalen Zentrum für Cybersicherheit des Bundes erhalten. Wir messen diesen partnerschaftlichen Kooperationen grösste Wichtigkeit zu, denn wir sind uns bewusst, dass in diesem Bereich das Arbeiten im Alleingang keine gangbare Lösung ist.

Welche langfristigen Strategien oder Pläne verfolgt die Stadtverwaltung, um die Sicherheit der Stadt vor Cyberangriffen zu gewährleisten und stets auf dem neuesten Stand zu sein?

Seine eigenen IT-Systeme zu schützen bedeutet, über deren Architektur und Inhalt genauso gründlich Bescheid zu wissen wie etwa ein Ingenieur, der jedes Detail eines Gebäudes verstehen und seine Nutzung kennen muss, um die Sicherheit zu gewährleisten. Vor diesem Hintergrund haben wir eine Initiative mit dem Ziel gestartet, unsere Daten, deren Schutzniveau, Schnittstellen und Qualität besser zu dokumentieren und zu kennen. Angesichts der aktuellen technologischen Entwicklungen werden die Gemeindeverwaltungen bald kein einziges proprietäres System mehr haben.

Alle Anwendungen werden ausschliesslich in sogenannten «Cloud»-Lösungen verfügbar sein, wie dies schon für private Nutzer gängig ist. Diese Entwicklung setzt voraus, dass wir den Informationsfluss zwischen den Rechnern der Verwaltung und den externen Anbietern beherrschen müssen. Dies ist eine unabdingbare Voraussetzung, um uns in die Lage zu versetzen, eine angemessene Sicherheitsstrategie anzuwenden und im Falle einer Attacke auf unsere Systeme oder bei Datenverlust rasch zu reagieren.

THEMA

Cyberangriff – was gilt es zu beachten?

Cyberangriffe und damit einhergehende Datenverluste können das Vertrauen der Bevölkerung in die Verwaltung nachhaltig stören. Um sich optimal zu schützen, sollten alle Behörden und Unternehmen und somit auch die Stadtverwaltungen die Cybersicherheit ganzheitlich angehen und zur Chefsache erklären. Es reicht nicht aus, die Verantwortung allein dem IT-Verantwortlichen zu übertragen.

Sandra Lüthi
Expertin für Sensibilisierung und Prävention, Nationales Zentrum für Cybersicherheit NCSC

Die Mitarbeitenden von Stadtverwaltungen befinden sich aufgrund ihrer öffentlichen Tätigkeit in einer Schlüsselrolle innerhalb der IT-Sicherheitskette. Sie arbeiten mit Informatik-Infrastrukturen und Geräten, die ihnen den Zugang, die Erfassung und die Bearbeitung von schützenswerten Informationen ermöglichen. Zur Erfüllung des gesetzlichen Auftrags ist es unumgänglich, dass die Verwaltungsmitarbeitenden verschiedene Personendaten der Einwohnerinnen und Einwohner, des Personals sowie von Firmen speichern, bearbeiten und in bestimmten Fällen weitergeben.

«Die Mitarteitarbeiterinnen und Mitarbeiter von Stadtverwaltungen befinden sich in einer Schlüsselrolle.»

Zudem stehen sie täglich mit internen und externen Partnern via diverse Kommunikationskanäle in engem Kontakt. Bei ihrer Tätigkeit unterstehen die Mitarbeitenden dem Amtsgeheimnis und sind zur vertraulichen Behandlung von dienstlichen Angelegenheiten verpflichtet. Aufgrund der grossen Abhängigkeiten von der Informatik-Infrastruktur kann bei einem Cybereregnis die Handlungsfreiheit einer Stadtverwaltung rasch, nachhaltig und den Auftrag gefährdend beeinträchtigt werden.

Einige Stadtverwaltungen sind sich diesen Umständen bewusst und haben deshalb das Thema Cybersicherheit bereits gut integriert. Allerdings gibt es auch Verwaltungen, die Aufholbedarf haben. Lücken können vor allem bei fehlenden Sensibilisierungsmassnahmen und Schulungen, fehlenden Absprachen mit IT-Dienstleistern und fehlenden praxisnahen Erfahrungen im Umgang mit einem Cyberangriff festgestellt werden.

Krisenvorbereitung

Damit Sie auf allfälligen Cybersicherheitsvorfall möglichst gut vorbereitet sind, sollten Sie sich bereits heute überlegen, wie Sie im Ernstfall reagieren würden. Nur so erkennen Sie, ob Sie im Ernstfall vorbereitet sind. Setzen Sie zusammen mit Ihrem I**KT-Verantwortlichen** die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Klären Sie mit ihm die Prozesse und Verantwortlichkeiten im Normalbetrieb sowie im Falle eines Cybersicherheitsvorfalles. Halten Sie diese in einem Business Continuity Management-Plan fest, damit die Geschäftskontinuität gewährleistet ist.

Darin enthalten sollte auch ein **Kommunikations- und Krisenkonzept** sein. Definieren Sie zudem den **Notfallkontakt** bei einem Cybersicherheitsvorfall. Weitere Empfehlungen für die Zusammenarbeit mit IT-Dienstleistern finden Sie auf der Webseite des Nationalen Zentrums für Cybersicherheit (NCSC) unter dem Behörde-Button bei aktuellen Themen. Ebenfalls von hoher Wichtigkeit sind das **Sensibilisieren und Schulen** der Mitarbeitenden. Aktuelle Sensibilisierungsinhalte finden Sie auf der Webseite der jährlichen Sensibilisierungskampagne S-U-P-E-R.ch.

Zudem haben Sie die Möglichkeit, Zugriff auf das neue eLearning des Sicherheitsverbundes Schweiz (SVS) zu beantragen. Bitte wenden Sie sich hierfür bei info@elearningcyber.ch. Für kleine und mittlere Verwaltungen könnte ebenfalls der EBAS-Kurs für KMU interessant sein: www.ebas.ch/kmucourse.

Schadensbegrenzung im Falle eines Angriffs

Im Falle eines Cyberangriffs ist es wichtig, schnell zu handeln:

- Trennen Sie die mit Schadsoftware infizierten Systeme umgehend vom Netzwerk. Trennen Sie hierfür das Netzwerkkabel vom Computer und schalten allenfalls vorhandene WLAN-Adapter ab.
- Um eine Weiterverbreitung zu verhindern, unterbrechen Sie die Internetverbindungen (Web, E-Mail sowie Fernzugriff und VPN von Standort zu Standort).
- Überprüfen Sie die Backups und schützen Sie diese sofort.
- Backups sollten so schnell wie möglich physisch vom infizierten Netzwerk getrennt werden («offline genommen werden»).
- Ändern Sie im Falle eines Cyberangriffs sofort alle Passwörter. Überprüfen Sie E-Mail-Konten auf allfällige Weiterleitungsregeln.

Kontaktieren / Melden / Informieren

- Wenden Sie sich an Ihren IT-Notfallkontakt.
- Prüfen Sie die Kontaktaufnahme zur Polizei und die **Erstattung einer Anzeige.** Warten Sie mit dem Wiederaufsetzen der Systeme, bis die Polizei die Spuren gesichert hat.
- Mitarbeitende der Polizei beraten und unterstützen Sie im Vorgehen, sichern Spuren und ermitteln. Informieren Sie die Polizei via Polizeinotruf 117.
- Melden Sie den Vorfall dem **NCSC** über das Online-Formular: www.report.ncsc.admin.ch.
- Wenn **Daten gestohlen** wurden (z. B. im Fall einer Ransomware), empfehlen wir, die Betroffenen proaktiv zu informieren. Klären Sie ab, ob es gesetzliche Meldepflichten gibt. Mit dem neuen **Datenschutzgesetz** müssen Verletzungen der Datensicherheit dem EDÖB gemeldet werden (Art.24 nDSG und Art.15 SDSG). Benutzen Sie hier für das Online-Formular: https://databreach.edoeb.admin.ch/report.

Weiteführende Informationen:

- Schützen Sie Ihre Behörde (admin.ch)
- Weitere Informationen/Links

Impressum
Herausgeber: Schweizerischer Städteverband SSV, Monbijoustrasse 8, Postfach, 3001 Bern. Telefon: 031 356 32 32, www.staedteverband.ch. «focus» abonnieren: info@staedteverband.ch
Redaktion SSV: Nathanël Bruchez, Marc Moser. **Bilder:** S 1: Rolf Siegenthaler; Porträt Seiten 2 und 3: zvg.