Stadt Luzern
Stadtrat
Hirschengraben 17
6002 Luzern
www.stadtrat.stadtluzern.ch

T 041 208 82 11
stadtrat@stadtluzern.ch

Antwort auf die Interpellation 284

Gewährleistung der Cybersicherheit

Benjamin Gross namens der SP-Fraktion vom 4. August 2023
StB 31 vom 17. Januar 2024

Wurde anlässlich der Ratssitzung vom 29. Februar 2024 beantwortet.

Ausgangslage
Die Stadt Luzern hat sowohl die zunehmende Bedrohung durch Cyberattacken als auch die Tragweite von Sicherheits- und Datenschutzvorfällen im Zusammenhang mit der digitalen Transformation erkannt. Mit B+A 29 vom 30. August 2021: «Digitalstrategie und Smart City Luzern» wurde der Grundstein für den Aufbau der erforderlichen Ressourcen und Fähigkeiten im Bereich der Informationssicherheit und des Datenschutzes gelegt.
Inzwischen ist die Fachstelle Digitale Sicherheit und Privatsphäre (Fachstelle DSP) operativ und seit April 2023 mit den vorgesehenen personellen Ressourcen bestückt:
- Leiter Fachstelle / CISO (50%-Pensum);
- Beauftragter digitale Sicherheit / Wirtschaftsinformatiker, Spezialist Informationssicherheit (80%-Pensum);
- Beauftragte digitale Privatsphäre / Juristin, Spezialistin Datenschutz (100%-Pensum).

Allgemeines
Cybersicherheit wird allgemein definiert als Schutz vor Angriffen auf die Vertraulichkeit, die Integrität und die Verfügbarkeit von Informations- und Kommunikationstechnologie sowie auf digitale Daten, welche durch die Ausnutzung von Schwachstellen oder Umgehung von Schutzmassnahmen durch externe oder interne Angreifende stattfinden. Cybersicherheit ist ein integraler Teil der Informationssicherheit und des Datenschutzes, adressiert jedoch lediglich den Bereich der vorsätzlichen Handlungen unter Zuhilfenahme von technischen Mitteln und Methoden.
Diesbezüglich sei darauf hingewiesen, dass sich die Beantwortung der Fragen aus der Interpellation auf das gesamte Spektrum der Informationssicherheit und des Datenschutzes bezieht. Damit sollen die vielen bereits getroffenen Massnahmen, aber auch der weiterhin bestehende Handlungsbedarf aufgezeigt werden. Aufgrund der sich stetig verändernden Technologien sowie der weiterhin stark zunehmenden Bedrohung durch Cyberattacken und -betrug stellen die digitale Sicherheit und die digitale Privatsphäre eine Daueraufgabe der Stadtverwaltung dar.
Die Beantwortung der gestellten Fragen bezieht sich auf den Zeitraum bis Mitte Dezember 2023.

Zu 1:
Wie werden diese Daten der Stadt Luzern vor unbefugtem Zugriff, Datenverlust oder Manipulation geschützt?

Massnahmen im Bereich der Datensicherheit adressieren technische und organisatorische Aspekte und entwickeln sowohl präventive als auch reaktive Wirkung.

Bereits getroffene oder im Aufbau befindliche Massnahmen sind insbesondere
- Technisch:
  - Aufbau eines zweiten, gespiegelten Datacenters zur Erhöhung der Verfügbarkeit;
  - Sichere Infrastruktur für mobil-flexibles Arbeiten (Homeoffice) mit geschützten Endgeräten, sicherer Geräteauthentifizierung und verschlüsselten Datenverbindungen;
  - Sichere Authentifizierungsmechanismen für Benutzerinnen und Benutzer wie Single-sign-on und Multifaktor-Verfahren;
  - Sicherheitsorientierte Architektur der Netzwerk- und Serverinfrastruktur;
  - Schutz des Zugangs zu städtischen Netzwerken durch sichere Geräteauthentifizierung;
  - Datensicherung (Back-up) mit Schutz vor Verschlüsselungstrojanern (Ransomware);
  - Erkennung und Schutz vor Schadsoftware an allen relevanten Eintrittspunkten;
  - Sperrung von risikobehafteten und unerwünschten Website-Kategorien;
  - Automatisierte Sperrung von schädigenden Internetadressen;
  - Filterung von schädlichen E-Mails und Dateianhängen;
  - Niederschwelliges Melde- und Analyseverfahren für verdächtige E-Mails (Anti-Phishing Service);
  - Durchgehendes abgestuftes und bedarfsgerechtes Prinzip für privilegierte Systemzugänge.

- Organisatorisch:
  - Identitäts- und Zugangskontrolle mit applikationsspezifischen Rollen- und Berechtigungskonzepten;
  - Prozess zum Melden und Behandeln von Sicherheitsvorfällen;
  - Software-Kategorisierung mit Schutzbedarf;
  - Security-Ausnahmeantragsprozess;
  - Cyberattacken-Notfallübungen mit der Notfallorganisation der Zentralen Informatikdienste (NOZ);
  - Vorsorgliche Vereinbarung und Abstimmung mit einem spezialisierten Unternehmen für die Reaktion auf Cyberattacken;
  - Zusammenarbeit mit dem nationalen Zentrum für Cybersicherheit (NCSC);
  - Integration von Sicherheit und Datenschutz als integraler Bestandteil der Projektmethodik.

Momentan wird an folgenden Punkten gearbeitet:
- Kontinuierliche Umsetzung der technischen und organisatorischen Sicherheitsstandards (siehe Antwort auf Frage 4);
- Konsolidierung des Rollen- und Berechtigungsmodells;
- Förderung der Kompetenz von Projektleitenden hinsichtlich digitaler Sicherheit und Privatsphäre;
- Aktualisierung des Verzeichnisses der Bearbeitungstätigkeiten von Personendaten;
- Formalisierung der Verfahren zur Gewährleistung der Betroffenenrechte.

Zu 2.:
Welche Massnahmen wurden bisher ergriffen, um potenzielle Schwachstellen in den IT-Systemen der Stadt zu identifizieren und zu beheben? Wie häufig werden Sicherheitsüberprüfungen durchgeführt, um sicherzustellen, dass die Sicherheitsmassnahmen den aktuellen Bedrohungen standhalten?

Bereits in der Vergangenheit wurden einzelne bezüglich Sicherheit und Datenschutz kritische Systeme und Fachapplikationen hinsichtlich deren Sicherheit auditiert. Seit 2019 erfolgen die Überprüfungen durch interne und externe Fachpersonen regelmässig und gezielt. Insbesondere bei Projektabnahmen, bei der Einführung neuer Software oder Cloud-Services werden Sicherheits- und Datenschutzüberprüfungen als Abnahmekriterium durchgeführt.

Audits, Penetrationstests, Sicherheits- und Datenschutzverifikationen wurden insbesondere in folgenden Bereichen durchgeführt:
- Zentrale Sicherheits- und Berechtigungssysteme;
- Penetrationstests auf Systemen, die via Internet exponiert sind;

- Technische Schwachstellenanalysen (Vulnerability-Scans) von kritischen Applikationen, Clients, Servern und Netzwerkkomponenten;
- Umfassende interne Situationsanalyse auf Basis der Norm ISO/IEC 27002:2022.

Weitere etablierte Massnahmen sind das monatliche automatisierte Patching («Flicken», Aktualisierung) von Betriebssystemen, systemnaher Software sowie Fachapplikationen und Bürokommunikationssystemen; ebenso die priorisierte Behandlung von kritischen Softwareschwachstellen.
Die Prozesse der ZID werden jährlich einer externen Prüfung gemäss Prüfnorm ISAE 3402 unterzogen.

Handlungsbedarf besteht noch in folgenden Bereichen:
- Aufbau eines umfassenden und kontinuierlichen Vulnerability-Managements;
- Regelmässiges Patching diverser Kleinapplikationen; eine Problematik hierbei ist, dass in der Verwaltung eine grosse Anzahl verschiedener Applikationen eingesetzt werden;
- Durchführung regelmässiger Audits, Penetrationstests und Simulationen von Cyberattacken.

Zu 3:
Welche Schulungen und Sensibilisierungsmassnahmen werden den Mitarbeiter:innen der Stadtverwaltung in Bezug auf Cybersicherheit angeboten? Wie wird sichergestellt, dass alle Mitarbeiter:innen über die neuesten Sicherheitsrisiken und -verfahren informiert sind?

Früher wurde die IKT(Informations- und Kommunikationstechnologie)-Anwenderweisung anlässlich des Einführungsprogramms für neue Mitarbeitende geschult und durch die Anwendenden unterzeichnet. 2021 wurde diese komplett überarbeitet. Basierend darauf wurden 2022 Basisschulungen (Videos, E-Learning, Quiz) für alle bestehenden und seither für alle neu eintretenden Mitarbeitenden durchgeführt. Die Basisschulung ist Pflicht für alle Mitarbeitenden; ein entsprechendes Controlling ist etabliert. Die Fachstelle Digitale Sicherheit und Privatsphäre informiert zudem regelmässig in verschiedenen Gremien (Geschäftsleitungssitzungen aller Direktionen, Abteilungssitzungen, Fachgremien) über aktuelle Bedrohungen und Schutzmassnahmen. Interne Kommunikationskanäle (Intranet, Mitarbeitendenzeitschrift) werden ebenfalls für aktuelle Themen der Cybersicherheit und des Datenschutzes genutzt.
Bis 2019 wurden einzelne, punktuelle Sensibilisierungsmassnahmen mit simulierten Phishing-E-Mails durchgeführt und ausgewertet. Seit Mitte 2022 werden allen Mitarbeitenden regelmässig unterschiedliche simulierte Phishing-E-Mails zugestellt. Die Reaktion der Mitarbeitenden darauf wird statistisch ausgewertet und regelmässig intern publiziert. Diesbezüglich konnte eine erfreuliche Steigerung der Awareness (Bewusstsein, «Gewahrsein» von Gefährdungen) beobachtet werden.

Schulungsbedarf besteht hinsichtlich der Vertiefung der Thematik für spezifische Zielgruppen wie Projektleitende, Informatikfachpersonen, Daten- und Anwendungsverantwortliche. Einen besonderen Schwerpunkt wird die Sensibilisierung bei der Nutzung von Microsoft 365 (M365) und anderen Cloud-Services bilden. Weiter geplant ist die Durchführung von «Cyber-Attack-Games» sowie die laufende Aktualisierung und Ergänzung der Basisschulung und der Videos im Zusammenhang mit der anstehenden Aktualisierung der IKT-Anwenderweisung. Die Schulung und Sensibilisierung der Mitarbeitenden bleibt eine Daueraufgabe.

Zu 4.:
Welche klaren Sicherheitsrichtlinien und -standards wurden festgelegt, die von allen städtischen Institutionen, Partnerfirmen und -behörden befolgt werden müssen? Wie wird die Einhaltung dieser Richtlinien überwacht und sichergestellt?

Handlungsgrundlage für Sicherheitsrichtlinien und -standards bildet die Digital-/Informatikverordnung der Stadt Luzern. Der Stadtrat hat im Herbst 2023 die Informationssicherheitspolitik in Form der Weisung «Digitale Sicherheit und Privatsphäre» erlassen. Bereits 2021 wurde vom Stadtrat die revidierte IKT-Anwenderweisung in Kraft gesetzt, welche die sichere Nutzung der IKT-Sachmittel für alle Mitarbeitenden

regelt. Die Einhaltung der IKT-Anwenderweisung wird stichprobenartig und anhand statistischer Auswertungen kontrolliert. Eine Überwachung des Verhaltens von Mitarbeitenden ist dabei ausdrücklich ausgeschlossen.
Aktuell werden die Sicherheits- und Datenschutzstandards fertiggestellt, welche die technischen und organisatorischen Grundanforderungen der Stadt Luzern auf Basis der Normen ISO/IEC 27002 und 27701 definieren. In der operativen Umsetzung werden weitere Sicherheitsstandards wie beispielsweise NIST Cyber Security Framework, OWASP oder BSI Kriterienkatalog C5 angewandt.

Handlungsbedarf besteht in folgenden Bereichen:
- Weitere Konkretisierung und Umsetzung der Standards in Projekten im M365-Umfeld (Programm «Azzurro 2.0»);
- Formalisierung der Sicherheitsvorgaben in der Projektmethodik, damit die Standards durchgängig und nachvollziehbar eingehalten werden;
- Befähigung von Projektleitenden, IT-Fachpersonen und weiteren Betroffenen hinsichtlich Anwendung der Sicherheitsstandards;
- Umstellung der ISAE 3402 Prüfung auf Kontrollen, welche inhaltlich auf die Sicherheitsnormen ISO/IEC 27002 und 27701 abgestimmt sind.

Zu 5:
Werden personenbezogene oder andere vertrauliche Daten an Externe (bspw. zu Testzwecken) weitergegeben?

Im Rahmen von Digitalisierungs- und Informatikprojekten ist es teilweise unvermeidlich, dass Externen Zugang zu möglicherweise als «vertraulich» klassifizierten Daten gewährt werden muss. Eine eigentliche Weitergabe wird, wenn immer möglich, vermieden. Ist dies unumgänglich, so erfolgt das durch die Dienstabteilung Zentrale Informatikdienste (ZID) in einem geregelten Verfahren und über eine sichere, verschlüsselte Datenaustausch-Plattform. Es lässt sich technisch nicht verhindern, dass sensible Daten auch durch Mitarbeitende bewusst oder unbewusst an Externe bekannt gegeben werden, sei dies mittels E-Mail, MS Teams oder durch Cloud-Services, Social Media usw. Hierzu ist jedoch festzuhalten, dass dies per IKT-Anwenderweisung ausdrücklich untersagt ist.

Zu 6.:
Wie erfolgt die Zusammenarbeit mit externen Partnern und Behörden im Hinblick auf den Austausch von Daten? Welche Sicherheitsvorkehrungen werden getroffen, um sicherzustellen, dass auch diese Partner angemessene Sicherheitsstandards einhalten?

Die Beschaffung von IKT-Sachmitteln, Software und Cloud-Services erfolgt für die ganze Verwaltung durch die ZID (gemäss Informatik- und Digitalverordnung vom 11. März 2020; sRSL 0.6.1.1.2). Dadurch ist sichergestellt, dass Informationssicherheits- und Datenschutzaspekte in den standardisierten Verträgen angemessen berücksichtigt sind. Mit sämtlichen externen Partnern bestehen explizite Datenschutzvereinbarungen (Erklärung Datenschutz und -sicherheit), die einen integrierenden Vertragsbestandteil darstellen. Darin sind die durch die externen Partner einzuhaltenden technischen und organisatorischen Massnahmen definiert. Dazu gehört insbesondere auch die Pflicht zum Löschen von Daten der Stadt Luzern.
In technischer Hinsicht wurden Datenaustauschverfahren etabliert, welche eine gesicherte und verschlüsselte Übertragung von Daten ermöglichen. Fernzugänge für Supportzwecke unterliegen einem Bewilligungsverfahren durch die Fachstelle DSP und werden streng kontrolliert.

Kontrollen im Sinne von direkten Lieferantenüberprüfungen sind zwar Teil der allgemeinen Vertragsbedingungen, wurden aber aufgrund des hohen Aufwands bisher nicht durchgeführt. Lieferanten mit Zugang zu vertraulichen Daten oder solche, die für Projekt- oder Supporttätigkeiten über Kopien von vertraulichen Daten verfügen, sind identifiziert. Diese werden per Anfang 2024 schriftlich auf ihre vertraglichen Pflichten aufmerksam gemacht, und es wird eine ausdrückliche Bestätigung eingefordert, dass allfällig noch vorhandene und nicht zwingend benötigte Datenbestände der Stadt tatsächlich gelöscht sind.

Zu. 7.:
Gibt es Pläne, die Cybersicherheit weiter zu verbessern und zu stärken? Wenn ja, welche spezifischen Massnahmen sind geplant, um die digitale Sicherheit der Stadt Luzern und ihrer Bürger:innen langfristig zu gewährleisten?

Durch die integrale Betrachtung der digitalen Sicherheit und Privatsphäre in allen Projekten und wesentlichen Änderungen kann gewährleistet werden, dass die in Zukunft eingesetzten Systeme, Applikationen und Cloud-Services den Sicherheits- und Datenschutzstandards der Stadt Luzern entsprechen und so ein den Risiken angemessenes Sicherheitsniveau etabliert wird. Teil davon ist die Durchführung von Datenschutzfolgenabschätzungen sowie die Umsetzung entsprechender Massnahmen.

Bis 2023 bestand eine «Cyber-Versicherung», welche die finanziellen Folgen von Cyberattacken abdeckte. Aufgrund der massiv gestiegenen Prämien und des begrenzten Nutzens für die Stadt wurde beschlossen, die Versicherung durch einen Bereitschaftsvertrag (Incident Response Retainer) mit einem spezialisierten Unternehmen im Bereich Cybersecurity abzulösen. Dies ermöglicht bei einem Vorfall eine schnelle und unkomplizierte Intervention durch Expertinnen und Experten.

Innerhalb der ZID besteht eine durch die Fachstelle DSP koordinierte Fachgruppe (Security-Operations-Team). Diese Fachgruppe besteht aus Spezialisten der ZID und kümmert sich – soweit das neben deren übrigen betrieblichen Aufgaben möglich ist – um sicherheitsrelevante technische Aspekte und Ereignisse. Ein Team, das sich schwerpunktmässig oder ausschliesslich mit operativer Cybersecurity auseinandersetzt, konnte aufgrund fehlender personeller Ressourcen nicht geschaffen werden; ein solches wäre aber dringend notwendig.

Um die digitale Sicherheit der Stadt Luzern langfristig zu gewährleisten, sind neben dem bereits dargestellten Handlungsbedarf insbesondere folgende Massnahmen dringend notwendig und geplant:
- Aufbau der technischen und organisatorischen Fähigkeiten zur systematischen und umfassenden Identifikation von Schwachstellen und Bedrohungen (Vulnerability and Threat Management) mit dem Ziel, ein umfassendes und stets aktuelles Bild über die Verletzbarkeit gegenüber Cyberattacken zu erhalten und Angriffsflächen zu minimieren.
- Ausbau der technischen und organisatorischen Fähigkeiten zur systematischen Erkennung und Behandlung von sicherheitsrelevanten Ereignissen und Vorfällen (Security-Information and Event-Management) mit dem Ziel, Anzeichen von Cyberattacken möglichst schnell und zuverlässig zu erkennen und angemessen und effektiv darauf zu reagieren.

Teile dieser Fähigkeiten könnten zukünftig zwar als externe Dienstleistungen bezogen werden. In einem Umfeld mit der Grösse und Heterogenität der Stadtverwaltung, der Volksschule sowie Viva Luzern als Kundin der ZID ist es dennoch unerlässlich, dass innerhalb der ZID diese Fähigkeiten im Sinne eines Security-Operations-Teams zeitnah aufgebaut werden.
Aus diesem Grund wird aktuell ein Bericht und Antrag an den Grossen Stadtrat erarbeitet, um die zum Aufbau der genannten Fähigkeiten erforderlichen Ressourcen und Sachmittel zu beschaffen.

Zu 8.:
Ist die Stadt Luzern im Austausch mit dem Kanton bezüglich eines Gesetzes zur digitalen Unversehrtheit? Wie steht der Stadtrat zu einer rechtlichen Grundlage, wie sie in Genf ein Volksmehr von 94 % gutgeheissen hat?

Die Stadt Luzern steht zurzeit nicht im Austausch mit dem Kanton bezüglich eines Gesetzes zur digitalen Unversehrtheit. Einer Stärkung der digitalen Rechte an der geeigneten Stelle und in der geeigneten Form steht der Stadtrat positiv gegenüber.