Stadt Kriens Stadtrat

Stadtplatz 1
CH-6010 Kriens
kriens.ch

kriens

Beantwortung Interpellation

Interpellation Piras: Cyber-Kriminalität: Wie gut ist die Stadt Kriens geschützt? Nr. 175/2023

Eingang	Zuständiges Departement
05. April 2023	Finanzdepartement

Beantwortung

Die Interpellation wird wie folgt beantwortet:

1. **Wie schätzt der Stadtrat die Gefahr eines Cyber-Angriffs auf die Stadt Kriens ein?**
   Die Wahrscheinlichkeit eines Angriffs bzw. Versuch wird als gross eingeschätzt. Ungezielte Angriffsversuche passieren heute täglich. Zum Beispiel blocken die Firewalls dies laufend ab. Bezüglich Einschätzung der Wahrscheinlichkeit der Gefahr und Auswirkung kommt es auf die Professionalität des Vorgehens der Angreifenden an und wie schnell der Angriff bemerkt wird. Der Gemeindeverband ICT (GICT) ist technisch gut geschützt. Durch finanzielle Investitionen wäre ein zusätzlicher Schutz möglich, jedoch nehmen die Kosten für einen noch besseren Schutz exponentiell zu. Z. B. könnte man ein Security Operation Center (SOC) beauftragen die Infrastruktur 7x24 zu überwachen, verdächtige Aktivitäten zu analysieren und "First Response" durchzuführen. GICT ist aktuell in Abklärung für die Zusammenarbeit mit einem SOC und dem Vorstand von GICT werden hierzu Informationen geliefert für einen Entscheid in den kommenden Monaten.

2. **War die Stadt Kriens bereits Opfer eines Cyber-Angriffs? Falls ja, wie gross war das Ausmass des Angriffs?**
   Gemäss Rücksprache mit GICT sind seit Ende 2018 zwei Vorfälle zu verzeichnen:
   - Vor rund zwei Jahren wurde unbefugt auf Mailaccounts von einzelnen Schülern der Stadt Kriens auf den Servern von Microsoft (nicht GICT) zugegriffen (vermutlich durch Erraten der Passwörter). Dies wurde festgestellt und das Passwort geändert. Grundsätzlich ist es möglich, dass GICT die Anforderungen an das Passwort für die Schulen erhöht (Länge, Komplexität, etc.). Bisher wurden von den Schulen (Arbeitsgruppe Schule/GICT) explizit geringere Anforderungen gewünscht als diese bei der Verwaltung der Stadt Kriens der Fall ist. Dies müsste mit den schulverantwortlichen Personen besprochen werden.
   - Ende Juni 2023 fand ein Cyber Angriff auf die GICT Infrastruktur statt. Ermöglicht wurde dies dadurch, dass zwei Benutzer einer der Gemeinde auf einen Link in einem E-Mail geklickt haben. Der Vorfall wurde von der Überwachung der GICT erkannt, direkt Sofortmassnahmen eingeleitet, die Verbreitung eingedämmt und die Malware mit viel Aufwand und unter Beizug eines externen Spezialisten beseitigt. Gemäss heutigem Wissenstand ist es weder zu einem unerlaubten Zugriff durch Dritte, noch zu Datenverlust oder Datendiebstahl gekommen. In den kommenden Wochen

Stadtplatz 1
CH-6010 Kriens
kriens.ch

wird sämtlicher Datenverkehr noch durch zusätzliche technische Hilfsmittel überwacht, um einen weiteren Befall sofort feststellen zu können. Die technischen Massnahmen der GICT werden laufend verbessert und ergänzt. Das grösste Risiko bleibt jedoch das Verhalten der Benutzer. Darum wurden die Mitarbeitenden der Gemeinden (nebst der laufenden E-Learning Kampagne) über den Umgang und die Mail-Einstellungen hingewiesen.
Der Vorfall wurde dem Nationalen Zentrum für Cybersicherheit (National Cyber Security Centre – NCSC) der Bundesverwaltung gemeldet. Nach Absprache und Rücksprache zwischen GICT, NSCS und der betroffenen Gemeinde wurde Strafanzeige gegen die Täterschaft (unbekannt) bei der Kriminalpolizei eingereicht, da durch den Vorfall relativ hohe Kosten (rund Franken 30'000) entstanden sind. In Zusammenarbeit mit der Polizei werden Logs, Mails und falls nötig weitere Daten analysiert.

3. **Wie schützt sich die Stadt Kriens gegen Cyber-Angriffe?**
   a. **Besteht eine Strategie gegen Cyber-Angriffe?**
   Nach der Ausarbeitung und Einführung der ICT Strategie zum 1. Januar 2023 wurde anschliessend eine Cybersecurity Strategie der Stadt Kriens ausgearbeitet. Diese wird nach Durchsicht und Abstimmung mit GICT und externen Berater in den nächsten Wochen vom Stadtrat zur Einführung besprochen und beschlossen. Wichtig ist die konkrete Umsetzung der Konzepte und Massnahmen aufgrund der Cybersecurity Strategie. Von Seiten des GICT sind bereits diverse technische Schutzmassnahmen getroffen und geplant (z.B. Segmentierung) und weitere Folgen aufgrund der laufenden Besprechungen zwischen der Abteilung Finanzdienste und GICT aufgrund der erwähnten Strategie. Nebst den technischen Massnahmen kann die Daten- und Informationssicherheit adäquat gewährleistet werden durch die konsequente Umsetzung der organisatorischen Massnahmen durch die Verwaltung der Stadt Kriens (Zugangsbeschränkung zu den Büros, Schulung und Sensibilisierung der Mitarbeitenden, etc.).
   b. **Wie sieht die Vorgehensweise im Fall eines Cyber-Angriffs aus?**
   Dies kommt immer auf die Art des Angriffs an. Es besteht eine Organisation, Planung und Umsetzung von Massnahmen zur Bewältigung von Vorfällen. Die Incident-Response erfolgt hauptsächlich durch GICT unter Einbezug von externen Partner und der Gemeinden (Kommunikation, Rechtliches, etc.) bei Entscheiden zu Massnahmen. Bezüglich der technischen Vorgehensplanung hat der GICT z. B. mit einem externen Partner einen Vorgehensplan für einen Ransomware Angriff erarbeitet. Dieser ist streng vertraulich.

4. **Ist die Stadt Kriens gegen Cyber-Kriminalität versichert?**
   Aktuell verfügt die Stadt Kriens über keine Cyber-Versicherung. Diesbezüglich sind Abklärungen mit einer grossen Versicherungsgesellschaft betreffend Umfang und Kosten für eine Offerte am Laufen.

5. **Werden regelmässig IT-Sicherheitssysteme der Stadt Kriens gegenüber Cyber-Angriffe geprüft?**
   Der GICT lässt seine Systeme jährlich durch einen externen Anbieter prüfen (interne und externes «Penetration Testing»). Die Stadt Kriens arbeitet auch mit anderen mit anderen Providern z. B. bezüglich Applikationshosting zusammen. Die Abteilung Finanzdienste wird bis Ende 2023 bei diesen Partnern über die Prüfverfahren, Konzepte und Massnahmen nachfragen.

6. **Wie werden Mitabeiter:innen gegen Cyber-Sicherheit sensibilisiert? Finden regelmässige Schulungen diesbezüglich statt?**

Stadtplatz 1
CH-6010 Kriens
kriens.ch

Es findet eine vier Jahre dauernde Awareness Initiative zum Thema Informationssicherheit statt (aktuell im zweiten Jahr), bei der jährlich drei Themen in Kampagnen bearbeitet werden. Die Kampagne beinhaltet Merkblätter und E-Learning (Videos, Tests) mit Fortschrittskontrolle.

7. **Wie gut sind vertrauliche/sensible Daten wie z.B. Steuererklärungen, persönliche Daten von Bürger:innen, Sozialdiensten, aber auch interne Daten wie Lohn, Personalbeurteilungen etc. geschützt?**
   Von der technischen Seite kann der Schutz als gut beurteilt werden. Bei der Arbeit im Home-Office ist z. B. der gesamte Datenverkehr ins Rechenzentrum des GICT verschlüsselt. Der Zugriff von extern erfolgt über Zwei-Faktor-Authentifizierung. Die Möglichkeit auf Drei-Faktor-Authentifizierung zu erweitern wird zwischen der Verwaltung Stadt Kriens und GICT besprochen. Die aktuelle grössere Gefahr besteht für die ungewollte Veröffentlichung von Daten im Rahmen von Social Engineering Angriffen, bei denen Angreifer über die Mitarbeitenden der Stadt Kriens an Daten und Informationen gelangen. Social Engineering ist dieses Jahr auch Thema bei der Awareness Kampagne.

8. **Der Schweizerische Gemeindeverband, das Nationale Zentrum für Cybersicherheit (NCSC) sowie die Kantonspolizei Bern hat Informationen und Wegleitungen für Gemeinden erstellt. Kann sich der Stadtrat vorstellen aufgrund der vorhandenen Wegleitungen, sich dem Thema Cyber-Sicherheit anzunehmen?**
   Ja. Als Grundlage dient die erwähnte Cyber-Strategie der Stadt Kriens und die Verwendung von Informationen und Wegleitungen (insbesondere NSCS) in der Zusammenarbeit mit GICT zur Umsetzung der Konzepte. Ergänzend dazu arbeitet die GICT mit ausgewählten Spezialisten und Partner im Bereich Cyber-Sicherheit zusammen.

9. **Kann sich der Stadtrat vorstellen, das Label «Cyber-Safe» anzustreben, um ein angemessenes Sicherheitsniveau zu erlangen?**
   Ja. Das Label «Cyber-Safe» bietet Behörden die Möglichkeit, ihre IT-Infrastruktur zu testen und ein angemessenes Niveau an Cybersicherheit zu erlangen. Zu einem Preis des Gütesiegels von rund 15'000 Franken (250 IT Arbeitsplätze) wird eine Diagnose und ein Audit durchgeführt. Die organisatorischen Voraussetzungen (Kompetenz und Verantwortlichkeit) in der Stadt Kriens müssen gemäss «Cyber-Safe» zuvor erfüllt sein, nebst a) einer internen Ansprechperson für IT Fragen und b) eine im IT-Bereich geschulte Ansprechperson (beides erfüllt) muss c) in der Geschäftsleitung der antragsstellenden Organisation eine Person für die Cybersicherheit verantwortlich sein. Das Anstreben des Labels «Cyber-Safe» und die Verantwortlichkeiten kann mit der Cyber-Strategie festgelegt werden und die Umsetzung der Erlangung für das Label für 2024 geplant und budgetiert werden.

Kriens, 29. Juni 2023