GEMEINDERAT

ALLSCHWIL

Geschäft 4741A

Beantwortung der Interpellation von Christian Jucker, GLP, vom 24.06.2024, betreffend Status Cybersecurity@Allschwil

Bericht an den Einwohnerrat
vom 11. September 2024

Inhalt Seite

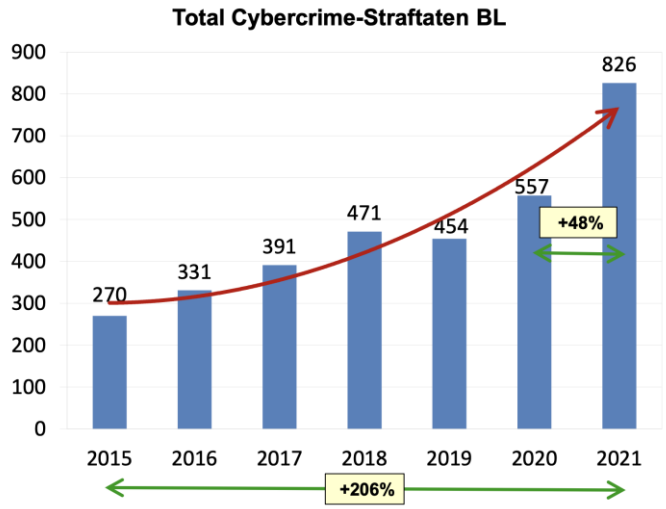
Beilage/n

- keine

1. Ausgangslage

Am 24. Juni 2024 reichte Christian Jucker, GLP eine Interpellation betreffend Status Cybersecurity@Allschwil mit folgendem Wortlaut ein:

«Die Cyberangriffe auf die Informatik von Gemeinden und Verwaltungen nehmen weiter zu, d.h. die Bedrohungslage hat sich weiter verschärft. Auch im Baselland wurden Gemeinden schon erfolgreich angegriffen (z.b. Bubendorf) und die Anzahl an Cybercrime Straftaten im Baselland nimmt schnell zu:



Im Rahmen der GPK hat der Einwohnerrat vor einiger Zeit einen Einblick in die laufenden Bestrebungen im Bereich IT-Sicherheit/Cybersecurity erhalten. Im Rahmen dieser Interpellation möchten wir einen aktuellen Stand dieser Aktivitäten einfordern.

Wir bitten daher um die schriftliche Beantwortung folgender Fragen:

1. *Welche weiteren Penetrationstests bzw. Security Audits wurden durchgeführt? Wird ein regelmässiger Security Review eingeführt?*
2. *Strebt die Gemeinde ein Cybersafe Label https://www.cyber-safe.ch/de/label-cyber-safe/#dienstleistungen oder ähnliches an (z.B. Teile des IKT-Mindeststandards)?*
3. *Sind die organisatorischen Abläufe im Falle eines Cyberangriffs getestet und dokumentiert? Insbesondere Aufbau eines Notfallstabes, Krisenkommunikation, Führungsstruktur und Aufbau von unabhängigen Notfallsystemen für die Kommunikation ?*
4. *Wird regelmässig ein technischer Totalausfall und die entsprechende Wiederherstellung getestet? Insbesondere auch unter Berücksichtigung der Wiederherstellung aller Client- und Serversysteme ?*
5. *Ist Cybersecurity "Chefsache", d.h. wo ist es im Betrieb und auf strategischer Ebene angesiedelt. Sind diese Personen entsprechend geschult, um im Falle eines Angriffs richtig zu reagieren?*
6. *Wurden Absichtserklärungen, Verträge oder SLAs mit Incident Response Dienstleistern abgeschlossen?*
7. *Ist die Auslagerung kritischer Cybersecurity Prozesse in ein SOC (Security Operations Center) geplant oder bereits erfolgt?*
8. *Wie wird die Zusammenarbeit mit externen Dienstleistern aus Sicht der Cybersecurity validiert (sind die Dienstleister zertifiziert, müssen sie Mindeststandards erfüllen, sind*

Cybersecurity Themen in den Verträgen abgedeckt, Regelung der Vertraulichkeit etc.) ?

9. *Wie werden Informationen und Systeme klassifiziert, damit sie entsprechend den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit (CIA) betrieben werden können?*
10. *Welche Massnahmen werden regelmässig zur Schulung und Sensibilisierung der Mitarbeiter (auch Teilzeitpersonal) durchgeführt?*
11. *Wie werden besonders exponierte Personen geschult (z.B. IT-Personal, Geschäftsleitung, Gemeinderat)?*
12. *Wie werden besonders exponierte Prozesse geschützt (z.B. Online-Banking)?*
13. *Wie werden schützenswerte Daten nach dem Stand der Technik gesichert, insbesondere auf den Arbeitsgeräten, beim Transport und in den jeweiligen Anwendungen?*
14. *Wer ist für den Umgang mit sensiblen Daten verantwortlich (wurde ein "Data Privacy Officer" definiert)?*
15. *Wie sind die Systeme der Blaulichtorganisationen (Gemeindepolizei und Feuerwehr) von der normalen Informatik getrennt und zusätzlich geschützt?*
16. *Für das Bundesamt für Cybersecurity (BACS, MELANI) ist es zentral, schnell die richtigen Ansprechpartner zu finden. Aktuell zeigt https://allschwil.ch/.well-known/security.txt auf die Talus AG und nicht auf die Gemeinde, ist hier vertraglich geregelt, wie im Falle eines Angriffs zu reagieren ist?*
17. *Ist der Zugriff auf wichtige Daten immer mit Multifaktor-Authentifizierung geschützt (z.B. auch E-Mail von Extern/privaten Geräten)?»*

2. Antworten des Gemeinderates

1. Welche weiteren Penetrationstests bzw. Security Audits wurden durchgeführt? Wird ein regelmässiger Security Review eingeführt?

Die Gemeinde Allschwil lässt in regelmässigen Abständen von zwei bis maximal drei Jahren Penetrationstests durchführen. Die letzte Prüfung fand im Januar 2024 statt. Weitere Tests bzw. Reviews werden nicht durchgeführt, da die regelmässigen Penetrationstest als zweckmässig und ausreichend erachtet werden.

2. Strebt die Gemeinde ein Cybersafe Label https://www.cyber-safe.ch/de/label-cyber-safe/#dienstleistungen oder ähnliches an (z.B. Teile des IKT-Mindeststandards)?

Nein. Der Schwerpunkt der Gemeinde Allschwil lag bisher und liegt auch in Zukunft bei der Erhöhung der IT-Sicherheit. Dies unter der Berücksichtigung der Grösse und Komplexität der Organisation sowie den verfügbaren personellen Ressourcen. Das Erlangen eines Cybersafe Label wurde dabei nicht priorisiert.

3. Sind die organisatorischen Abläufe im Falle eines Cyberangriffs getestet und dokumentiert? Insbesondere Aufbau eines Notfallstabes, Krisenkommunikation, Führungsstruktur und Aufbau von unabhängigen Notfallsystemen für die Kommunikation?

Die Gemeinde Allschwil verfügt im IT-Bereich über ein Desaster Recovery Konzept. Darin sind mögliche Ereignisse, Recovery-Prozesse, Restore-Szenarien, etc. beschrieben. Abläufe im Falle eines Cyberangriffs wurden mangels personeller und technischer Ressourcen bisher nicht getestet. Zudem verfügt die Gemeinde Allschwil über keine unabhängigen Notfallsysteme (z.B. Georedundanz). In Bezug auf den Aufbau eines Notfallstabes, Krisenkommunikation sowie Führungsstrukturen würde ähnlich wie bei den Ereignissen zur Corona-Pandemie, des Ukraine-Konfliktes sowie der Energiemangellage, die Geschäftsleitung der Gemeinde Allschwil die notwendigen Schritte koordinieren.

4. Wird regelmässig ein technischer Totalausfall und die entsprechende Wiederherstellung getestet? Insbesondere auch unter Berücksichtigung der Wiederherstellung aller Client- und Serversysteme?

Nein. Wie bereits vorstehend erläutert (vgl. Antwort auf Frage 3), fehlen dazu die personellen und technischen Ressourcen.

5. Ist Cybersecurity "Chefsache", d.h. wo ist es im Betrieb und auf strategischer Ebene angesiedelt. Sind diese Personen entsprechend geschult, um im Falle eines Angriffs richtig zu reagieren?

Das Thema Cybersecurity wird durch die Abteilung Informatik im Bereich Finanzen – Informatik – Personal bearbeitet. Auf strategischer Ebene wurde das Thema als wichtige Komponente der eGovernment Strategie festgehalten. Zudem wurden die Risiken IT-Verfügbarkeit und Informationssicherheit & Datenschutz im Rahmen der Leitbildmassnahme Risikomanagement auf die Risikolandkarte aufgenommen. Spezifischen Schulungen in diesem Bereich wurden nicht durchgeführt. Die Mitarbeitenden sind jedoch im Umgang mit solchen Situationen sensibilisiert.

6. Wurden Absichtserklärungen, Verträge oder SLAs mit Incident Response Dienstleistern abgeschlossen?

Ja. Die Gemeinde Allschwil verfügt seit Anfangs 2024 über ein externes Cyber Security Intelligence Center (SOC o.ä.). Es handelt sich dabei um Dienstleistungen, welche die Gemeinde in Anspruch nimmt zur Überwachung des gemeindeinternen Netzwerkes in Bezug auf mögliche Hackerangriffe und/oder sicherheitsrelevanten Anomalien.

7. Ist die Auslagerung kritischer Cybersecurity Prozesse in ein SOC (Security Operations Center) geplant oder bereits erfolgt?

Ja. Siehe dazu Antwort auf Frage 6.

8. Wie wird die Zusammenarbeit mit externen Dienstleistern aus Sicht der Cybersecurity validiert (sind die Dienstleister zertifiziert, müssen sie Mindeststandards erfüllen, sind Cybersecurity Themen in den Verträgen abgedeckt, Regelung der Vertraulichkeit etc.) ?

Es erfolgt keine spezifische Validierung in Bezug auf Cybersecurity bei der Zusammenarbeit mit externen Dienstleistern. Im Falle eines Datenaustausches werden jedoch i.d.R. die Aufgaben und Verantwortlichkeiten in Bezug auf den Datenschutz geregelt.

9. Wie werden Informationen und Systeme klassifiziert, damit sie entsprechend den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit (CIA) betrieben werden können?

Die Gemeinde Allschwil hat ihre Systeme bzw. Daten nicht konsequent klassifiziert. Im Rahmen des Desaster Recovery Konzeptes wurden die wichtigsten Applikationen in Bezug auf ihre Verfügbarkeit, die Wiederherstellungszeit sowie des maximalen Datenverlustes klassifiziert. Mit der Bearbeitung der Themengebiete Datenmanagement aus der eGovernment Strategie werden solche Fragestellungen adressiert werden. Über Zugriffsberechtigungen werden die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt.

10. Welche Massnahmen werden regelmässig zur Schulung und Sensibilisierung der Mitarbeiter (auch Teilzeitpersonal) durchgeführt?

Sämtliche Mitarbeitende führen eine IT-Security Schulung sowie regelmässige Update-Schulungen durch. Zusätzlich werden weitere Massnahmen zur Sensibilisierung z.B. in Bezug auf Phishing werden aktuell evaluiert.

11. Wie werden besonders exponierte Personen geschult (z.B. IT-Personal, Geschäftsleitung, Gemeinderat)?

Bei der Schulung (vgl. Antwort auf Frage 10.) wird nicht zwischen Personengruppen unterschieden. Im Grundsatz müssen sämtliche Mitarbeitende das gleiche Schulungsprogramm absolvieren.

12. Wie werden besonders exponierte Prozesse geschützt (z.B. Online-Banking)?

Die Gemeinde Allschwil hat ihre Prozesse in Bezug auf IT-Security nicht klassifiziert. Entsprechend sind besonders exponierte Prozesse auch nicht bestimmt. Über eingeschränkte Zugriffs- und Unterschriftsberechtigungen werden z.B. Prozesse wie Online-Banking geschützt.

13. Wie werden schützenswerte Daten nach dem Stand der Technik gesichert, insbesondere auf den Arbeitsgeräten, beim Transport und in den jeweiligen Anwendungen?

Sämtliche Mitarbeitende der Gemeinde Allschwil arbeiten primär mittels eines virtuellen Clients auf der Serverumgebung der Gemeinde Allschwil. Dies sowohl an ihrem Arbeitsplatz als auch ausserhalb und unabhängig davon, ob es sich um Arbeitsgeräte der Verwaltung oder um private Geräte handelt. Sämtliche Daten in der Server-Umgebung werden täglich im Backupserver, der virtuellen Tape library und der physische Tabe library gesichert. Bezüglich lokal gespeicherten Daten, werden die Mitarbeitenden mittels Weisung angehalten, für die zweckmässige Sicherung zu sorgen. Diese Weisung muss von sämtlichen Mitarbeitenden im Rahmen des Eintrittes unterzeichnet werden.

14. Wer ist für den Umgang mit sensiblen Daten verantwortlich (wurde ein "Data Privacy Officer" definiert)?

Die Gemeinde Allschwil verfügt über keinen «Data Privacy Officer» bzw. eine Rolle welche für den Umgang mit sensiblen Daten verantwortlich ist. Bei Projekten welche den Datenschutz betreffen, wird bei Bedarf die kantonale Aufsichtsstelle Datenschutz konsultiert.

15. Wie sind die Systeme der Blaulichtorganisationen (Gemeindepolizei und Feuerwehr) von der normalen Informatik getrennt und zusätzlich geschützt?

Die einsatzrelevanten Systeme und Daten der Feuerwehr werden über kantonale Applikationen betrieben und sind somit von der lokalen Informatik der Gemeinde Allschwil getrennt. Die übrigen Daten der Feuerwehr sowie die Systeme und Daten der Gemeindepolizei sind Teil der lokalen Informatik der Gemeinde Allschwil und somit nicht zusätzlich geschützt.

16. Für das Bundesamt für Cybersecurity (BACS, MELANI) ist es zentral, schnell die richtigen Ansprechpartner zu finden. Aktuell zeigt https://allschwil.ch/.well-known/security.txt auf die Talus AG und nicht auf die Gemeinde, ist hier vertraglich geregelt, wie im Falle eines Angriffs zu reagieren ist?

Ja. Aufgrund der neu in Anspruch genommenen externen Dienstleistungen (siehe Antwort auf Frage 6.) wurde der Text auf der Seite https://allschwil.ch/.well-known/security.txt angepasst.

17. Ist der Zugriff auf wichtige Daten immer mit Multifaktor-Authentifizierung geschützt (z.B. auch E-Mail von Extern/privaten Geräten)?»

Der Zugriff auf den virtuellen Client (vgl. Antwort zu Frage 13.) sowie Webmail und der Webapplikation für die Zeiterfassung erfolgt mittels Zweifaktoren-Authentifizierung. E-Mail Synchronisationen auf privaten Endgeräten werden nicht spezifisch mittels Multifaktor-Authentifizierung geschützt.

Gestützt auf diese Ausführungen wird die Interpellation als erledigt abgeschrieben.

GEMEINDERAT ALLSCHWIL

Präsident:	Leiter Gemeindeverwaltung:
Franz Vogt	Patrick Dill