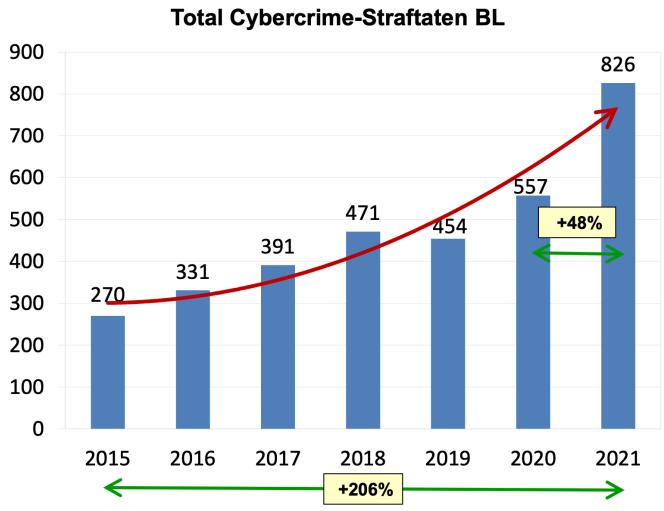
Interpellation
«Status Cybersecurity@Allschwil»

Ausgangslage

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.

Fragen

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)?

C. Jucker

Christian Jucker, GLP Allschwil-Schönenbuch