Motion von Patrick Käppeli, SVP, vom 23. August 2022, betreffend

«Cybersicherheit der Stadt Solothurn»

Um die Cybersicherheit der Stadt Solothurn zu erhöhen, sollen folgende Massnahmen durchgeführt werden:

- Durchführung einer Phishing Simulation in den nächsten 3 Monaten, anschliessend zyklisch wiederholend.

- Stand der Cybersicherheit überprüfen mittels einem Penetration Test.

Begründung:

Die Cyberbedrohung weltweit steigt, durch die Vernetzung aller Lebensbereiche steigt auch die Gefahr für die Schweiz bzw. die Stadt Solothurn.

Einige Beispiele:

- Mai 2021 Stadtverwaltung Rolle VD (Daten der Einwohner landen im Darknet)
- 11.10.2021 Stadtverwaltung Montreux VD (Ransomware)
- 13.01.2022 Stadtverwaltung Yverdon-les-Bains (Ransomeware)
- 22.07.2022 Stadtverwaltung Bülach ZH (Ransomeware)

Die Regio Energie Solothurn (RES) als IT Dienstleister ist zuständig für die Infrastruktur der Stadt Solothurn und deren Sicherheit. Die Sicherheit wurde in den letzten Jahren kontinuierlich verbessert.

Eine solche Phishing Simulation wurde jedoch in all den Jahren noch kein einziges Mal durchgeführt.

Jedoch liegt es an der Stadt Solothurn den Auftrag zu erteilen für eine Phishing Simulation.

Bei einer solchen Phishing Simulation werden simulierte betrügerische E-Mails an die eigenen Mitarbeiter gesendet, um die Reaktion der Mitarbeiter auf solche betrügerischen Mails zu überprüfen und im Nachgang das Bewusstsein für die Gefahren zu schärfen.

Es geht bei solchen Simulationen nicht darum die Mitarbeiter blosszustellen, sondern das Bewusstsein für solche und andere Cyberbedrohungen zu schärfen. Daher ist es essentiell, dass niemand aus der EGS den genauen Zeitpunkt und Inhalt der Simulation erfährt (nicht mal die VL oder Stadtpräsidentin) ausser der ITK, welche mit dem Dienstleister die Simulation durchführt.

Zusätzlich zur Simulation, soll ein Penetration Test durchgeführt werden. Bei einem solchen Test wird die Sicherheit aller Systembestandteile (Anwendungen, Computersysteme, Netzwerk etc.) auf mögliche Schwachstellen geprüft um unautorisierten Zugriff auf das System zu erhalten. Anschliessend werden Handlungsempfehlungen gegeben, wie diese Sicherheitslücken zu minimieren oder zu schliessen sind.

Erstunterzeichnender:

Patrick Käppeli

Marianne Wyss

Solothurn, 21. August 2022