Security Incident Management beim Informatikzentrum Köniz-Muri

Studiengang: MAS Cyber Security

Wie jüngst Fälle der Gemeinden Rolle und Montreux zeigten, nehmen gezielte und systematische Angriffe auf Gemeinden stetig zu. Die Systeme werden komplexer und die Herausforderungen an die Benutzenden steigt. Das Informatikzentrum Köniz-Muri will sich an zukünftigen Anforderungen orientieren. Als Konsequenz müssen Prozesse überprüft und weiterentwickelt werden.

Ausgangslage

Das IZ stellt für die Gemeinden Köniz und Muri wie auch für weitere Kunden Informatikmittel zur Verfügung. Es betreibt aktuell ein eigenes Rechenzentrum. Dieses wird in naher Zukunft zu einem RZ-Dienstleister umgezogen. Mit dieser Massnahme macht das IZ einen ersten Schritt zur Verbesserung der Verfügbarkeit und Informationssicherheit.
Mit dem Legislaturziel 4.1.1 „Digitalisierung weiter vorantreiben (Mensch, Technik, Organisation)“ schreibt der Gemeinderat seine Absicht, in die Digitalisierung und als Konsequenz, in die Weiterentwicklung der Informationssicherheit zu investieren, nieder.
Wie das Legislaturziel bereits im Titel suggeriert, spielt die Organisation mit dem Menschen und der Technik eine zentrale Rolle. Mit dem Entscheid, das Rechenzentrum auszulagern, hat der Gemeinderat die Unterstützung zur Verbesserung der Technik vermittelt. Eine grosse Herausforderung steht jedoch noch vor uns: die Maturität der Organisation im Bezug zur Informationssicherheit zu erhöhen. Dies bedingt:

- Unterstützung der Führungsebene
- Sensibilisierung
- Aus- und Weiterbildung
- Freigabe von personellen und finanziellen Ressourcen

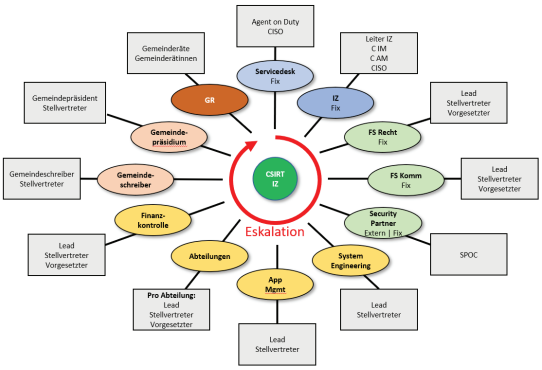
Zielsetzung

Als Ziel soll diese Arbeit aufzeigen, wie ein Security Incident Management für die Organisation in der Grösse eines KMU aufgebaut werden kann. Die Arbeit soll die Herausforderungen betreffend personellen sowie finanziellen Ressourcen, aber auch die Sensibilisierung aufzeigen und entsprechende Handlungsempfehlungen bieten.
Teile der Arbeit sind als „Onepager“ ausgeführt. Das heisst die Informationen finden kompakt auf einer Seite Platz. So können diese als Hilfsmittel, Checkliste oder Präsentationsvorlage dienen.

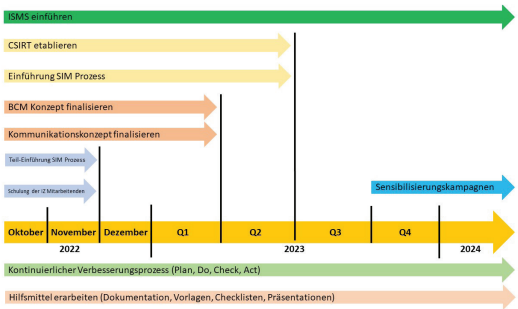
Ausblick

In dieser Master Thesis erarbeitete Themen wie der Security Incident Management Prozess und das CSIRT kann in Teilen rasch umgesetzt werden. Die Herausforderung wird sein, die Führungsebene und die Mitarbeitenden abzuholen, zu sensibilisieren und eine hohe Maturität der Organisation herbeizuführen. Dies gelingt aus meiner Sicht damit, dass sich das Informatikzentrum Köniz-Muri „sichtbar“ macht und die Führungsebene wie auch die Mitarbeitenden sensibilisiert, informiert und integriert.

Enrique Joaquin



Organisation CSIRT



Ausblick