Protokollauszug
27. Sitzung vom 7. Oktober 2024

209 0.5.4 2022.1753 **Postulat der Fraktionen GLP/BFPW, Grüne, Die Mitte, FDP, SP/EVP und SVP Notfall- und Kommunikationskonzept bei Cyber-Angriffen vom 3. November 2022 Bericht und Antrag auf Abschreibung**

1. Wortlaut des Postulats

Das folgende Postulat ist am 8. November 2022 eingegangen und am 28. November 2022 überwiesen worden:

Der Stadtrat wird aufgefordert, ein Notfall- und Kommunikationskonzept bei Cyber-Angriffen auszuarbeiten.

Begründung:

Mit der Interpellation betreffend Cyber-Sicherheit der Gemeinde Wädenswil vom 14. Januar 2022, welche von sämtlichen Fraktionen unterzeichnet und an der Gemeinderatssitzung vom 21. März 2022 traktandiert und erläutert wurde, wurden dem Stadtrat diverse Fragen gestellt.

Der Stadtrat hat die Fragen am 30. Juni 2022 schriftlich beantwortet und an der Gemeinderatsitzung vom 5. September 2022 auch mündlich ausgeführt.

Bei der Beantwortung der folgenden zwei Fragen ist der Gemeinderat der Ansicht, dass man seitens Stadtrat ungenügend auf einen allfälligen Cyber-Angriff vorbereitet ist und dass die Gefahr eines solchen Angriffs unterschätzt bzw. die eigenen Fähigkeiten, wie in einem solchen Fall vorzugehen ist, überschätzt werden. Diese Einschätzung beruht auch darauf, dass der Stadtrat bei seinen übrigen Ausführungen stark auf Abwehr und Schutz fokussiert ist, dabei aber vernachlässigt, dass kein Schutz 100% Sicherheit bietet. Sollte ein Cyber-Angriff aber trotz allen getroffenen Massnahmen erfolgreich sein, ist ein rasches und konsequentes Handeln wichtig. Nur so kann der Reputationsschaden für Wädenswil eingedämmt und das Vertrauen in die Stadtverwaltung bewahrt werden.

Frage 4: Wie sind die Verantwortlichkeiten zum Thema Cyber-Sicherheit in der Gemeinde und bei den beauftragten Subunternehmen geregelt?

Antwort: Die Rollen und Verantwortlichkeiten sind durch den Stadtrat in der «Leitlinie zur Informationssicherheitspolitik» vom 11. Februar 2013 geregelt worden. Des Weiteren werden bei Verträgen mit externen Dienstleistern in der Regel die «AGB Auslagerung Informatikleistungen» sowie die «AGB Datenbearbeitung durch Dritte» des Kantons Zürich vom 24. Juni 2015 als integrale Vertragsbestandteile definiert, sofern zutreffend.

Frage 5: Existiert ein Krisen-sowie ein Kommunikationskonzept im Falle von Cyber-Angriffen?

Antwort: Nein, ein spezifisches Krisen- und Kommunikationskonzept für Cyber-Angriffe existiert nicht. Der Stadtrat bestimmt die Organisation für Not- und Katastrophenfälle und beruft ggf. das Gemeindeführungsorgan (GFO) ein.

Weil ein Notfall- und Kommunikationskonzept auch Verantwortlichkeiten (Frage 4) beinhaltet und weil die Frage 5 mit NEIN beantwortet wurde, weil eben KEIN explizites Notfall- und Kommunikationskonzept für Cyber-Angriffe existiert, wird der Stadtrat dringend ersucht, ein entsprechendes Notfall- und Kommunikationskonzept bei Cyber-Angriffen auszuarbeiten.

Konkret sollen Zuständigkeiten und Verantwortlichkeiten bei einem Angriff geregelt sein (sprich: Klarheit, wer was macht, wer zu involvieren ist, wer entscheidet, wer ausführt etc.). Auch muss klar sein, welche unmittelbaren technischen Schritte in Betracht gezogen werden müssen (Netzwerkabschaltungen, Trennen von Backup-Servern, Datenbanken etc.). Die Beurteilung des Schadenausmasses und das Aufgleisen weiterer Schritte (Involvieren von Polizei und anderen Behörden), die interne Kommunikation, eine rasche und vollständige und transparente Kommunikation an die Öffentlichkeit oder der Umgang mit allfälligen Lösegeldforderungen sind ebenfalls Themen, mit denen man sich auseinandersetzen muss, bevor ein Ereignis eintritt. Die Aufzählung erhebt nicht den Anspruch auf Vollständigkeit, aber sie soll zum Ausdruck bringen, wie wichtig ein solches Konzept eben ist. Letztlich ist es unverzichtbar, ein entsprechendes Konzept in Zusammenarbeit mit professionellen IT-Dienstleistern aufzusetzen. Dazu gehört ebenfalls, dass ein solches Konzepts regelmässig – mittels möglichst realitätsnaher Tests – auf seine Praxistauglichkeit geprüft und allenfalls angepasst wird.

Wir erachten es als unerlässlich, dass der Stadtrat ein solches Konzept erstellt, um im Fall eines erfolgreichen Cyber-Angriffs bestmöglich vorbereitet zu sein und wenigstens in der Reaktion darauf einen kleinen Vorsprung zu haben. Sicher kann man bei der Erstellung eines solchen Konzepts auch von Gemeinden lernen, welche bereits Opfer eines Cyber-Angriffsgeworden sind.

2. Bericht des Stadtrats

2.1 Notfall- und Kommunikationskonzept bei Cyber Angriffen

Der Stadtrat ist sich bewusst, dass zu einer Krisenbewältigung nicht nur das Krisenmanagement, sondern auch die Krisenkommunikation von grosser Bedeutung ist. Das Postulat gab Anlass, die Erarbeitung eines "Notfall- und Kommunikationskonzept bei Cyber Angriffen" anzugehen. Im Konzept werden fünf Schweregrade unterschieden und es wird festgelegt, wie beim Auftreten von Informations-Sicherheitsproblemen vorzugehen ist. Die fünf Stufen sind

- Informations-Sicherheits-Warnung
- Auffälligkeit / Störung
- Notfall
- Krise
- Katastrophe

2.2 Ziel

Mit dem Notfall- und Kommunikationskonzept werden die Voraussetzungen geschaffen, um IT-Systeme so zu betreiben, dass die grundlegenden Schutzziele

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität

während und nach einem Cyber Angriff erfüllt werden. Das Notfall- und Kommunikationskonzept beschreibt alle notwendigen Massnahmen, um auf Krisen vorbereitet zu sein sowie die Abläufe zur Bewältigung von Krisen. Das Notfallmanagement regelt folgende Bereiche:

- Schwellenwerte / Eskalation:
  Wann tritt die Notfallorganisation in Kraft? Wann findet eine Eskalation statt?
- Notfallorganisation:
  Beschreibung der Notfallorganisation, inkl. Stellvertretungen; Erreichbarkeit (Telefon, Natel, usw.) der Mitglieder der Notfallorganisation
- Alarmierung:
  Alarmierungsprozess; Definition, wer die Alarmierung auslöst; Regelungen bez. Stellvertretungen
- Kommunikation, intern und extern:
  Kommunikationsfluss während und nach dem Notfall; Definition wer wie und an wen kommuniziert wird; Kommunikation intern, an Einwohnerinnen und Einwohner, andere Behörden, Medien, usw.
- Ausbildung:
  Ausbildung / Schulung der Mitglieder der Notfallorganisation; Information der Mitarbeitenden bez. Notfallplanung, Vorgehen in einem Notfall
- Aktualisierung:
  Aktualisierung Kontinuitätspläne und Wiederanlaufpläne; Berücksichtigung von Ausweichmassnahmen
- Integration Change Management:
  Wenn Änderungen an Systemen durchgeführt werden, müssen die betroffenen Kontinuitätspläne und Wiederanlaufpläne angepasst werden
- Tests:
  Testen von Kontinuitäts- und Wiederanlaufplänen
- Hilfsmittel:
  Definition der Hilfsmittel, welche für die Notfallplanung und die Behandlung von Notfällen zur Verfügung stehen
- Nachbearbeitung:
  Nachbearbeitung mit Dokumentation und Reflektion des Notfalls
- Verhaltensregeln:
  Verhaltensregeln für die Mitglieder der Notfallorganisation, sowie für alle Mitarbeitenden.

Die im Rahmen der Notfallplanung getroffenen Vorkehrungen sind periodisch zu testen und allfällige Korrekturmassnahmen vorzunehmen.

2.3 Geltungsbereich

Das Notfall- und Kommunikationskonzept gilt für IKT-Systeme der Stadt Wädenswil, unabhängig von deren Einsatzgebiet und organisatorischer Verantwortlichkeit.

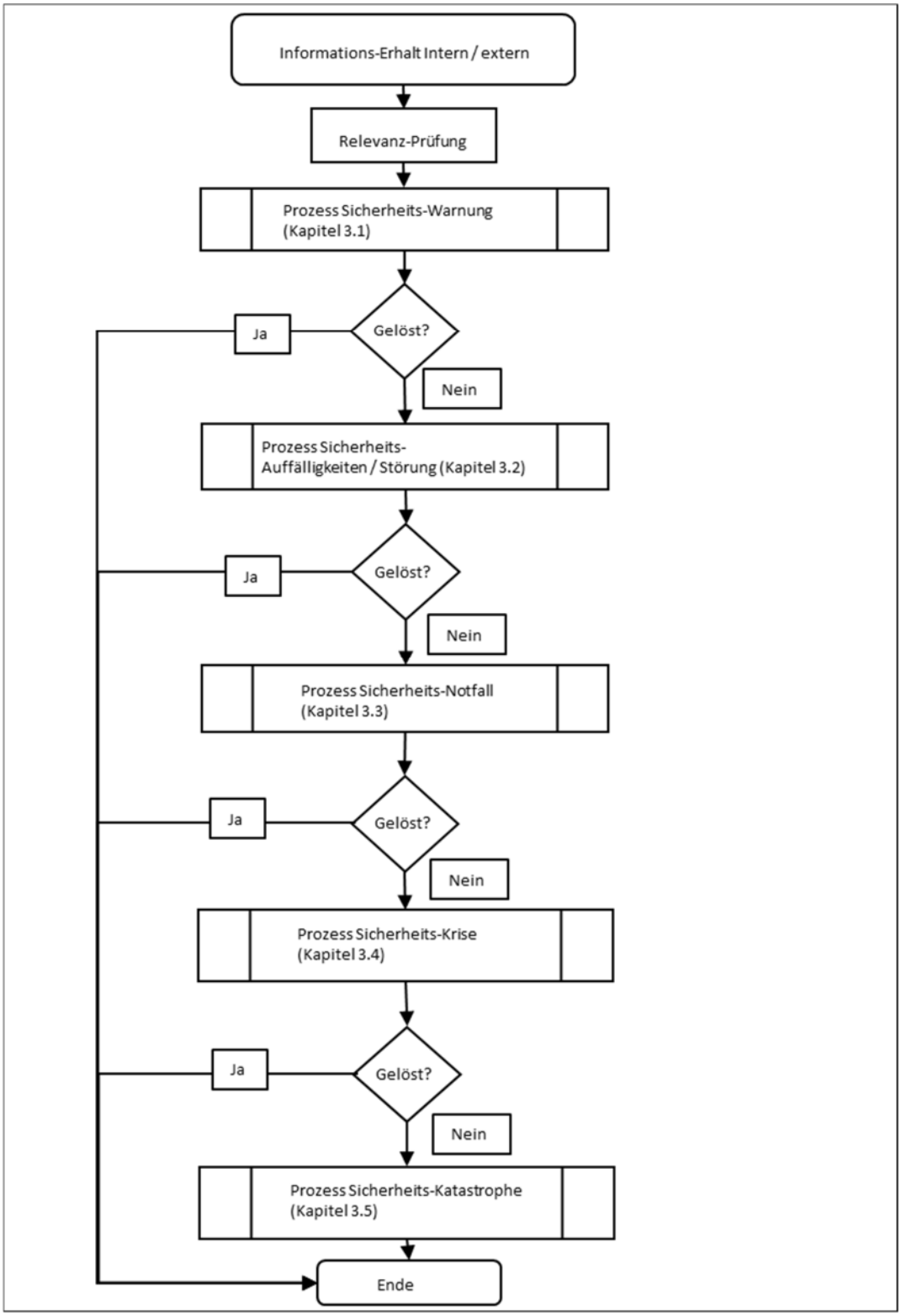
Die festgelegten Zuständigkeiten, Eskalationswege und Abläufe sollen eine zügige Abarbeitung, eine effektive Analyse und eine schadensmindernde Behandlung eines Informations-Sicherheitsvorfalls bzw. Informations-Sicherheitsnotfalls sicherstellen sowie durch eine fundierte Nachbearbeitung eine Wiederholung möglichst ausschliessen.

2.4 Mitgeltende Vorschriften / Unterlagen

Die für das Notfall- und Kommunikationskonzept geltenden gesetzlichen Grundlagen sind:

Name	Beschreibung
Gesetz über die Information und den Datenschutz (IDG)	IDG 170.4
Verordnung über die Information und den Datenschutz (IDV)	IDV 170.41
Verordnung über die Informationsverwaltung und -sicherheit	LS 170.8

2.5 Prozessbeschrieb der fünf definierten Stufen von Informations- Sicherheitsvorfällen



Weiter beinhaltet das Notfall- und Kommunikationskonzept die Prozessbeschreibungen aller fünf Stufen, die Beschreibung der Eskalationsstufen sowie der Notfallorganisation mit Aufgaben, Verantwortlichkeiten und Pflichten. Zudem sind der Umgang mit Drohungen- und Erpressungen sowie die Nachbearbeitung eines Informations-Sicherheitsvorfalls beschrieben.

Aufgrund der Vertraulichkeit weiterer Konzeptdetails muss auf die nähere Umschreibung und ausführlichere Informationen verzichtet werden.

Der Stadtrat, auf Antrag der Abteilung Präsidiales, beschliesst:

1. Der Bericht zum Postulat der Fraktionen GLP/BFPW, Grüne, Die Mitte, FDP, SP/EVP und SVP, vom 3. November 2022, überwiesen am 28. November 2022, betreffend Notfall- und Kommunikationskonzept bei Cyber-Angriffen, wird genehmigt.

2. Gestützt auf diesen Bericht wird dem Gemeinderat beantragt, das Postulat als erledigt abzuschreiben.

3. Mitteilung an:
   - Mitglieder des Gemeinderats
   - Mitglieder des Stadtrats
   - Abteilung Präsidiales

Status: öffentlich

Für richtigen Auszug:

Stadtrat Wädenswil

Esther Ramirez
Stadtschreiberin

Versand: 15. Oktober 2024