Stadtrat

Marktgasse 58
9500 Wil

stadtkanzlei@stadtwil.ch
www.stadtwil.ch
Telefon 071 913 53 53

3. November 2026

Anfrage 286 / Olav Baumann, FDP
eingereicht am 11. August 2026 – Wortlaut siehe Beilage

Cyberangriffe machen vor Gemeindegrenzen nicht halt - wie ist Wil vorbereitet?

Olav Baumann, FDP, hat am 11. August 2026 eine Anfrage zum Thema "Cyberangriffe machen vor Gemeindegrenzen nicht Halt – wie ist Wil vorbereitet?" eingereicht und bittet den Stadtrat um die Beantwortung von fünf Fragen.

Beantwortung

Vorbemerkung:
Die Stadt Wil misst der Cybersicherheit einen hohen Stellenwert bei und verfolgt einen mehrschichtigen Sicherheitsansatz, welcher technische, organisatorische und personelle Massnahmen kombiniert. Die interne Informatik betreibt und betreut dabei eine umfangreiche und vielfältige IT-Landschaft für die Stadtverwaltung, die Schulen sowie weitere angeschlossene Organisationen. Dazu gehören zwei Verzeichnisdienste, drei Microsoft Tenants mit rund 3'500 Benutzerkonten, zwei zentrale Serverinfrastrukturen mit insgesamt 95 Servern, das gesamte Netzwerk mit 78 Standorten, rund 3'200 Arbeitsplätze und mobile Endgeräte sowie die dazugehörigen Druck-, Telefonie- und weiteren IT-Systeme.
Zu den bestehenden Sicherheitsmassnahmen gehören unter anderem Phishing-Simulationen, die kontinuierliche Überwachung der IT-Infrastruktur durch ein Security Operations Center (SOC) mit Managed Detection and Response (MDR), die Überwachung exponierter Internetzugänge und WAN-IP-Adressen auf mögliche Bedrohungen, die Überwachung sicherheitsrelevanter Ereignisse sowie regelmässige Audits. Die interne Informatik greift dabei in jenen Bereichen auf verschiedene spezialisierte Dienstleister zurück.
Ziel ist es, Cyberrisiken frühzeitig zu erkennen, Sicherheitsvorfälle wirksam zu behandeln und das Sicherheitsniveau der Stadt Wil kontinuierlich weiterzuentwickeln. Die zunehmende Digitalisierung der Verwaltungs-, Schul- und Fachanwendungen sowie die stetig wachsende Bedrohungslage erfordern dabei laufende Investitionen in organisatorische, personelle und technische Schutzmassnahmen.

Die nachfolgenden Ausführungen zur städtischen Informatik werden durch die Angaben der Technischen Betriebe Wil (TBW) ergänzt. Die TBW sind als Betreiberin kritischer Infrastrukturen und digitaler Dienstleistungen besonders gefordert. Aus Sicherheitsgründen beschränken sie ihre Angaben auf Informationen, die keine Rückschlüsse auf konkrete Systemarchitekturen, Konfigurationen, Schwachstellen oder das operative Sicherheitsdispositiv zulassen.

1. Über welche Cyber-Defence-Strategie verfügt die Stadt Wil, und wie stellt sie mit organisatorischen, personellen und technischen Massnahmen sicher, dass Cyberrisiken präventiv erkannt, angemessen begrenzt und Sicherheitsvorfälle wirksam bewältigt werden können?

Die Stadt Wil verfolgt einen mehrschichtigen Sicherheitsansatz ("Defense in Depth"), welcher organisatorische, personelle und technische Massnahmen kombiniert. Ziel ist es, Cyberrisiken möglichst früh zu erkennen, Angriffe zu verhindern sowie Sicherheitsvorfälle rasch und wirksam zu behandeln. Des Weiteren dienen die Vorgaben der KOM SG-Richtlinien als Orientierung.

Zu den wesentlichen Massnahmen gehören:
- Einsatz moderner Firewall- und Netzwerkschutzsysteme
- Mehrstufige Authentifizierung für kritische Systeme und Dienste
- Regelmässige Sicherheitsupdates und Schwachstellenbehebungen
- Sensibilisierung und Schulung der Mitarbeitenden
- Durchführung von Phishing-Simulationen zur Überprüfung und Verbesserung des Sicherheitsbewusstseins
- Überwachung der IT-Umgebung durch einen externen Security Operations Center (SOC) inklusive Managed Detection and Response (MDR) Dienst
- Schwachstellenmanagement für öffentlich zugängliche Dienste
- SIEM auf Firewall

Ein MDR-Dienst ergänzt klassische Schutzmechanismen durch die kontinuierliche Überwachung von sicherheitsrelevanten Ereignissen. Verdächtige Aktivitäten werden rund um die Uhr analysiert und bewertet. Im Ereignisfall können so Angriffe früh erkannt und Gegenmassnahmen rasch eingeleitet werden.
Die Stadt Wil greift zusätzlich auf spezialisierte Dienstleister zurück. Diese unterstützen die ICT bei der Überwachung, Beurteilung und Weiterentwicklung der Sicherheitsmassnahmen und arbeiten dabei eng mit den internen Fachstellen zusammen. Ergänzend werden öffentlich erreichbare Systeme und Internetanbindungen kontinuierlich überwacht. Dazu gehört auch die Überwachung der öffentlichen WAN-IP-Adressen auf sicherheitsrelevante Auffälligkeiten, bekannte Bedrohungen, Schwachstellen oder Hinweise auf missbräuchliche Aktivitäten. Dadurch können potenzielle Risiken frühzeitig erkannt und geeignete Massnahmen eingeleitet werden.

Auch die TBW verfolgen einen mehrschichtigen Sicherheitsansatz aus technischen, organisatorischen und personellen Massnahmen. Stadtverwaltung und TBW stimmen damit im grundlegenden Vorgehen überein. Während sich die städtische Informatik an den KOM SG-Richtlinien orientiert, dient den TBW der IKT-Minimalstandard des Bundes als wesentlicher Referenzrahmen. Dessen Anforderungen erfüllen die TBW gemäss dem für sie massgebenden Schutzniveau. Zu ihren Massnahmen gehören insbesondere geregelte Zugriffs- und Berechtigungskonzepte, Mehrfaktor-Authentisierung, Security Monitoring, Patchmanagement, Datensicherungs- und Wiederherstellungsverfahren mit regelmässiger Überprüfung der Wiederherstellbarkeit sowie externe Sicherheitsüberprüfungen, Penetrationstests und Mitarbeitendenschulungen.

2. Welche Vorkehrungen und Zuständigkeiten sind für den Eintritt eines Not- oder Krisenfalls vorgesehen, und wie wird die Funktionsfähigkeit dieser Incident-Response- und Wiederherstellungsprozesse regelmässig überprüft?

Die Stadt Wil verfügt über definierte Prozesse für den Umgang mit Sicherheitsvorfällen und IT-Störungen. Die Zuständigkeiten zwischen der internen Informatik, externen Fachpartnern sowie spezialisierten Sicherheitsdienstleistern sind geregelt.

Zu den wichtigsten Vorkehrungen gehören:
– Regelmässige Datensicherungen
– Unterstützung durch externe Spezialisten bei Sicherheitsereignissen
– Permanente Überwachung durch den MDR-Dienst

Die Wirksamkeit der definierten Prozesse wird regelmässig überprüft und im Rahmen von Audits sowie technischen Tests bewertet. Aufgrund der hohen Relevanz dieser Verfahren besteht ein kontinuierlicher Bedarf an der Weiterentwicklung und regelmässigen Erprobung der entsprechenden Konzepte. Dabei sollte aber weiter in die Erprobung von Vorfällen investiert werden, sodass die Abläufe spätestens innerhalb von zwei Stunden nach einem Vorfall definiert, getestet und validiert werden können.

Die TBW verfügen bereits über ein etabliertes IT-Notfall- und Krisenmanagement mit definierten Zuständigkeiten sowie Melde- und Eskalationswegen. Im Ereignisfall stehen die Erkennung und Eindämmung des Vorfalls, der Schutz von Systemen und Daten sowie die Aufrechterhaltung beziehungsweise möglichst rasche Wiederherstellung der notwendigen Betriebsfähigkeit im Vordergrund. Wie die städtische Informatik setzen die TBW auf Datensicherungen, regelmässige Überprüfungen und bei Bedarf externe Spezialisten. Die TBW überprüfen die Wiederherstellbarkeit regelmässig und berücksichtigen Erkenntnisse aus Tests und Ereignissen bei der Weiterentwicklung ihrer Prozesse.

3. Anhand welcher Kennzahlen oder anderer Kriterien beurteilt die Stadt die Wirksamkeit ihrer Cybersicherheitsmassnahmen, wie häufig erfolgt diese Beurteilung und in welcher Form wird darüber intern oder extern berichtet?

Die Wirksamkeit der Cybersicherheit wird anhand verschiedener Kriterien beurteilt. Dazu gehören unter anderem:
– Ergebnisse aus Phishing-Simulationen
– Anzahl und Schwere identifizierter Sicherheitsvorfälle
– Reaktionszeit bei Sicherheitsmeldungen
– Ergebnisse externer Sicherheitsaudits
– Erkenntnisse aus Schwachstellen- und Sicherheitsanalysen

Die Ergebnisse aus externen Audits, Schwachstellenscans und Phishing-Simulationen werden systematisch ausgewertet und zur kontinuierlichen Verbesserung der Sicherheitsmassnahmen genutzt. Zur unabhängigen Bewertung des Sicherheitsniveaus erfolgt mindestens alle drei Jahre ein professionelles Audit, dessen Empfehlungen in die Weiterentwicklung der Sicherheitskontrollen einfliessen.

Auch die TBW beurteilen die Wirksamkeit anhand mehrerer technischer und organisatorischer Kriterien und nutzen die Erkenntnisse zur laufenden Verbesserung. Sie berücksichtigen insbesondere den Erfüllungsgrad des IKT-Minimalstandards, das Security Monitoring, externe Sicherheitsüberprüfungen und Penetrationstests, Sicherheitsereignisse, den Aktualisierungsstand der Systeme, die Funktionsfähigkeit der Datensicherungs- und Wiederherstellungsverfahren sowie Schulungsmassnahmen. Die Beurteilung erfolgt laufend im operativen Sicherheitsmanagement und periodisch in den Führungs-, Kontroll- und Risikomanagementprozessen. Wesentliche Erkenntnisse und Risiken werden den zuständigen Stellen stufengerecht berichtet.

4. Wie sind die Zuständigkeiten und Verantwortlichkeiten für die Cybersicherheit zwischen der Stadt Wil, ihren Betrieben sowie externen, kantonalen und eidgenössischen Leistungserbringern geregelt, und wie werden die daraus entstehenden Abhängigkeiten und Risiken gesteuert?

Die Verantwortung für die Informationssicherheit liegt grundsätzlich bei der Stadt Wil. Die operative Umsetzung erfolgt durch die zuständigen Informatik- und Fachstellen in Zusammenarbeit mit externen Partnern. Spezialisierte Dienstleister übernehmen definierte Aufgaben in Bereichen wie:

- Sicherheitsüberwachung (SOC/MDR)
- Sicherheitsberatung
- Audits und Risikoanalysen
- Unterstützung bei Sicherheitsvorfällen

Durch klare Rollen, definierte Verantwortlichkeiten und regelmässige Abstimmungen werden Abhängigkeiten und Risiken aktiv gesteuert.

Für ihre Daten, Prozesse und die von ihnen verantworteten Systeme nehmen die TBW die entsprechenden Steuerungs- und Kontrollaufgaben selbst wahr. Sie halten ausdrücklich fest, dass ihre Verantwortung für die Informations- und Cybersicherheit nicht vollständig an externe Leistungserbringer delegiert werden kann. Stadtverwaltung und TBW stimmen darin überein, spezialisierte externe Partner für definierte Aufgaben beizuziehen und die Verantwortlichkeiten klar zu regeln. Die TBW berücksichtigen Abhängigkeiten und daraus entstehende Risiken im Informationssicherheits- und Risikomanagement und stellen entsprechende Sicherheitsanforderungen an externe Leistungserbringer. Bei Cybervorfällen ziehen sie bei Bedarf auch kantonale und eidgenössische Fachstellen bei.

5. Welche organisatorischen, personellen und finanziellen Mittel wären notwendig, um die Cyber-Defence der Stadt Wil und ihrer Betriebe weiter zu stärken?

Die Stadt Wil verfügt bereits über ein solides Grundniveau im Bereich der Informationssicherheit und hat verschiedene organisatorische sowie technische Schutzmassnahmen etabliert. Gleichzeitig entwickeln sich Cyberbedrohungen kontinuierlich weiter und werden durch die zunehmende Nutzung von Automatisierung und Künstlicher Intelligenz professioneller, skalierbarer und gezielter. Um den Schutz von Systemen, Daten und Dienstleistungen langfristig sicherzustellen, müssen die bestehenden Sicherheitsmassnahmen regelmässig überprüft, weiterentwickelt und an die aktuellen Bedrohungslagen angepasst werden, welches folgendes umfasst:

- Ausbau der Endpoint Detection & Response (EDR)-Fähigkeiten zum Schutz von Endgeräten
- Stärkung der personellen Ressourcen im Bereich Informations- und Cybersicherheit
- Sicherstellung ausreichender Kapazitäten für operative und strategische Security-Aktivitäten
- Weiterentwicklung des Schwachstellenmanagements (Vulnerability Management)
- Einführung bzw. Ausbau eines zentralen Security Information and Event Management (SIEM)
- Erweiterung der Möglichkeiten zur Sicherheitsanalyse sowie zur automatisierten Erkennung und Reaktion auf Endgeräten und Servern
- Verstärkung von Schulungs-, Sensibilisierungs- und Awareness-Massnahmen für Mitarbeitende
- Kontinuierliche Weiterentwicklung der organisatorischen Sicherheitsprozesse und Governance-Strukturen
- Erarbeitung und regelmässige Aktualisierung eines ICT-Krisenkonzepts inklusive Krisenstab
- Definition klarer Eskalations-, Kommunikations- und Meldewege für Sicherheitsvorfälle
- Etablierung und regelmässige Erprobung von Wiederherstellungsprozessen für kritische Systeme

– Festlegung und Überprüfung von Wiederanlaufzeiten (RTO) und Datenwiederherstellungszielen (RPO)
– Regelmässige Durchführung von Penetrationstests zur Überprüfung der Wirksamkeit der Sicherheitsmassnahmen

Aus Sicht der Informationssicherheit besteht insbesondere im Bereich der Endgerätesicherheit weiteres Ausbaupotenzial. Moderne Endpoint Detection and Response (EDR)-Lösungen ermöglichen eine deutlich frühzeitigere Erkennung von Angriffen auf Arbeitsplatzsysteme und Server und unterstützen eine schnelle Reaktion im Ereignisfall. Solche Funktionen gewinnen insbesondere bei Ransomware-Angriffen und gezielten Angriffen auf öffentliche Verwaltungen zunehmend an Bedeutung.

Die Stadt Wil setzt bereits auf regelmässige Sensibilisierungsmassnahmen, unabhängige Sicherheitsüberprüfungen sowie eine kontinuierliche Sicherheitsüberwachung durch ein Security Operations Center (SOC) mit Managed Detection and Response (MDR).

Die in den vergangenen Jahren umgesetzten Investitionen haben zu einem guten Sicherheitsniveau beigetragen. Gleichzeitig zeigt die aktuelle Bedrohungslage, dass insbesondere moderne Angriffe zunehmend auf Endgeräte wie Arbeitsplätze und Server von Gemeinden abzielen. Während die Stadt Wil bereits von einer professionellen Sicherheitsüberwachung durch MDR/SOC-Dienste, externen Audits und Security Services profitiert, bestehen im Bereich der erweiterten Endgerätesicherheit zusätzliche Entwicklungsmöglichkeiten. Moderne Endpoint Detection and Response (EDR)-Lösungen ergänzen bestehende Schutzmassnahmen und ermöglichen eine deutlich frühere Erkennung von Angriffen direkt auf Endgeräten.

Aus Sicht der Informationssicherheit würden zusätzliche Investitionen in diesem Bereich einen wichtigen Beitrag leisten, um die Widerstandsfähigkeit der Stadt Wil gegenüber zukünftigen Cyberbedrohungen weiter zu erhöhen. Der konkrete Mitteleinsatz ist jeweils im Rahmen der regulären Budget- und Investitionsplanung zu beurteilen und gegen andere Prioritäten abzuwägen.

Stadtverwaltung und TBW stimmen darin überein, die Sicherheitsmassnahmen laufend an die Bedrohungslage anzupassen und zusätzlichen Mittelbedarf im ordentlichen Planungs- und Budgetprozess zu beurteilen. Bei den TBW sind ein IT-Notfall- und Krisenmanagement, geregelte Melde- und Eskalationswege, regelmässige Überprüfungen der Wiederherstellbarkeit sowie externe Sicherheitsüberprüfungen und Penetrationstests bereits etabliert. Die vorstehend für die städtische Informatik genannten Ausbauschritte sind deshalb nicht unverändert auf die TBW übertragbar. Die TBW betonen zudem, dass eine weitere Stärkung nicht zwingend den Aufbau einer eigenen umfassenden Cyber-Defence-Einheit erfordert. Sie prüfen laufend, welche Kompetenzen intern erforderlich sind und für welche spezialisierten Aufgaben externe Fachstellen zweckmässiger und wirtschaftlicher sind. Den Ressourcenbedarf beurteilen sie anhand der Risiko- und Bedrohungslage, der Entwicklung der IT-Landschaft, der Digitalisierungsvorhaben und der Ergebnisse der Sicherheitsüberprüfungen.

Abschliessend ist anzumerken, dass ein hundertprozentiger Schutz weder wirtschaftlich sinnvoll noch technologisch machbar ist. Sicherheitsmassnahmen werden bei der Stadt Wil als kontinuierlicher Prozess und nicht als Zustand verstanden. Die Stadt verfolgt deshalb eine laufende Weiterentwicklung ihrer Sicherheitsorganisation unter Berücksichtigung der Empfehlungen der KOM SG sowie aktueller Erkenntnisse aus dem Cyber Security Hub des Bundes.

Diese grundsätzliche Beurteilung teilen auch die TBW: Absolute Sicherheit kann nicht gewährleistet werden. Sowohl die Stadtverwaltung als auch die TBW verstehen Cybersicherheit als kontinuierliche Aufgabe und überprüfen und entwickeln ihre Massnahmen laufend weiter.

Stadt Wil

Andreas Breitenmoser
Stadtpräsident

Janine Rutz
Stadtschreiberin