Resilienz bei der Kapo ZH

Technische Perspektive

Member-Apéro der asut / «Sicherheit und Resilienz in vernetzten Systemen»

Sicherheitsverbundsübung 2014 (SVU 14)

Das **Szenario** kombinierte eine schwere **Grippepandemie** mit einer **lang anhaltenden Strommangellage**: Ausgelöst durch eine Cyberattacke auf die Stromwirtschaft kam es zuerst zu einem rund 48-stündigen Blackout, danach zu einer mehrwöchigen Mangellage mit nur etwa 70 % der üblichen Strommenge. Parallel dazu infizierte eine Pandemie bis zu ein Viertel der Bevölkerung und belastete das Gesundheitswesen massiv.

SVU 14: Erkenntnisse und weiteres Vorgehen

Konzept «BREAK» der Kapo ZH

Das BREAK-Konzept definiert BCM-Massnahmen und Ziele, um ein Szenario analog SVU-14 wirksam zu bewältigen.

Handlungsfelder

WAS: Priorisierte Wirkungsfelder und einsatzkritische Systeme
WIE: Führungsstruktur und Entscheidungswege
WO: Operative Standorte
WER: Personal- und Einsatzplanung

Konzept «BREAK» der Kapo ZH

Im Bereich Logistik und IT umfasst das Konzept «BREAK» alle Massnahmen, die sicherstellen, dass kritische Infrastruktur, Versorgung und digitale Dienste auch bei eingeschränkten Ressourcen, Schadenslagen oder Systemausfällen funktionsfähig, verfügbar und steuerbar bleiben.

Versorgung & Infrastruktur	Technische Kernsysteme	Prozesse & Betrieb
• Wasserversorgung • Lebensmittelversorgung • Notstromversorgung • Wärme • Transport & Mobilität • Energieversorgung (Tankstellen)	• Rechenzentren • Netzwerke • Kommunikation • Einsatzkritische- und geschäftskritische Systeme • Datenmanagement & Sicherheit	• Instandhaltung & Ersatzteile • Personal • Dokumentation & Runbooks • Notbetrieb & Wiederanlauf

Heutige ICT-Systemlandschaft

Die ICT-Systemlandschaft der Kantonspolizei Zürich ist heute technisch so aufgebaut, dass der Betrieb auch bei kritischen Ereignissen, Systemausfällen oder Infrastrukturbeeinträchtigungen fortgeführt, kontrolliert und wiederhergestellt werden kann.

- Zwei eigene, redundante Rechenzentren
- Vollständig georedundante Architektur
- Redundante Netzwerkinfrastruktur
- Hochverfügbare Funk- und Kommunikations-architektur
- Standortversorgung mit Notstrom
- Systematische Härtung und Sicherheitsarchitektur
- Security Operations Center (SOC)
- Betriebs-, Service- und Sicherheitsprozesse
- Regelmässige technische Failover-Tests
- Backup- und Datenresilienzkonzept

Externe Abhängigkeiten

Verfügbarkeit der Mobilfunknetze

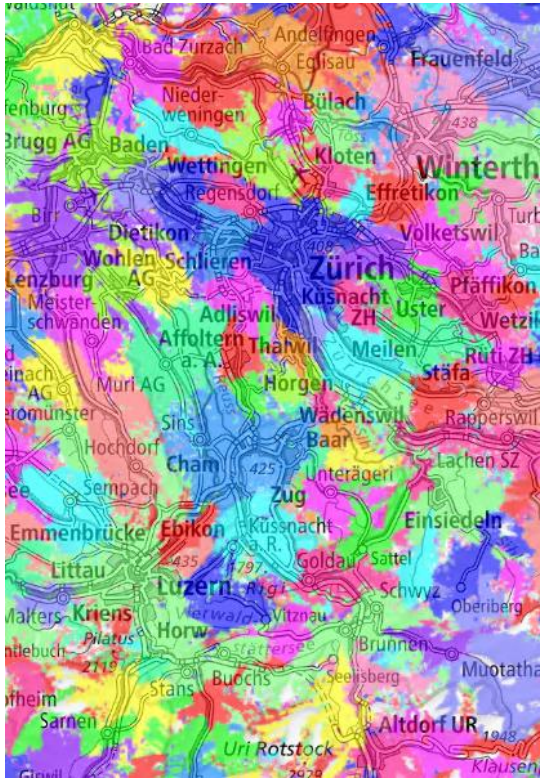
Im Zuge der FDV-Revision ist im Entwurf eine Autonomie von bis zu 72 Stunden für die Mobilfunkinfrastruktur vorgesehen. Netzbetreiber und Branche haben jedoch umfangreiche Kosten- und Machbarkeitsbedenken angemeldet; aktuell wird eine Variante mit nur noch 4 Stunden Autonomie als pragmatischer Ansatz diskutiert.

POLYCOM

Sicheres Behördenfunknetz der Schweiz

POLYCOM stellt sicher, dass Einsatzkräfte auch dann kommunizieren können, wenn öffentliche Netze ausfallen oder überlastet sind – und bleibt damit ein zentraler Baustein der Einsatz- und Sicherheitsinfrastruktur der Schweiz.

- Flächendeckende Versorgung
- Resiliente Architektur
- Unabhängig von öffentlichen Mobilfunk- und Datendiensten
- Hohe Verfügbarkeit
- Reines Sprachfunknetz



Mobiles Sicherheitskommunikationssystem (MSK)

Heute fehlt in der Schweiz ein einheitliches, mobiles Breitbandsystem für sicherheitsrelevante Kommunikation. Da POLYCOM voraussichtlich 2035 das Nutzungsende erreicht, soll MSK als moderne, mobile Breitbandlösung die Kommunikation der BORS und BKI zukünftig sicherstellen.

Erarbeitung der Botschaft:	BABS
Leitung Vorprojekt MSK:	Polizeitechnik und –informatik (PTI)

Investitionen (gesamthaft)	1,1 Mrd. Franken (Zeitraum 2029-2036)
Betriebskosten (gesamthaft)	1,9 Mrd. Franken(Zeitraum 2029-2046)

MSK Faktenblatt vom 31. August 2025

MSK

Vom MSK-Vorprojekt zum funktionalen Netz

Vorprojekt: 2026 - 2028	Hauptprojekt: 2029 - 2034	Nutzung: 2035 ff
◆ Initialisierung	◆ Implementierung MSK Core	◆ Permanente Weiterentwicklung
◆ Aufbau Organisation BORS	◆ Implementierung MCx Services	◆ Monitoring QoS im Betrieb
◆ Verifikation Nutzeranforderungen	◆ Vorbereitung SDVN+ für MSK	
◆ Architektur-Varianten vergleichen	◆ Härtung Backhauling	
◆ Synergien identifizieren & nutzen	◆ Härtung Basisstationen	
◆ Technische Machbarkeiten klären	◆ Netzverdichtung / AGA	
◆ Kosten verifizieren	◆ Schulung Nutzer	
◆ Rechtsgrundlagen prüfen	◆ Migration Nutzer (gestaffelt)	
◆ Technologie-Radar führen		
◆ Ersteller festlegen		
◆ Standort-Strategie erarbeiten		

Sicheres Datenverbundnetz Plus (SDVN+)

SDVN+ ist die zukünftige, sichere Dateninfrastruktur für den schweizweiten Austausch sicherheitsrelevanter Informationen. Es ist resilient, interoperabel und unabhängig von öffentlichen Netzen konzipiert. Das System befindet sich derzeit im Aufbau, erste Pilotanwendungen sind ab Q1 2026 geplant.

Projektverantwortung:	BABS
Erstellung & Betrieb:	Kommando Cyber
Standorte/Anschlüsse:	120 (Bund, Kantone und BKI)

SDVN+ Faktenblatt vom 31. August 2025

Resilienz bei der Kapo ZH

Technische Perspektive

Member-Apéro der asut / «Sicherheit und Resilienz in vernetzten Systemen»