VETTERMANN.DE · SICHERHEIT & KRITIS

Krisenvorsorge: Großflächiger Satellitenausfall

Schritt-für-Schritt-Checkliste (Abhängigkeits-Audit) & Tabletop-Übung „Szenario Spaceout“

Einsatzbereich: Unternehmen, Stadtwerke, Kommunen & KRITIS-Betreiber | **Quelle / Herausgeber:** vettermann.de (Fake Fun Facts – Gesamtverteidigung & KRITIS) | **Stand:** November 2026

Teil 1: Schritt-für-Schritt-Checkliste für das Abhängigkeits-Audit (IT & Strom)

Schritt 1: Bestandsaufnahme aller Zeit- und Positionsquellen (Discovery)

- ☐ **Physische Empfänger kartieren:** Alle GPS-/Galileo-Antennen an Serverräumen, Umspannwerken, Mobilfunkmasten und Fahrzeugflotten erfassen.
- ☐ **Zeitserver (NTP/PTP) prüfen:** Klären, ob der primäre Zeitserver (Stratum 1) ausschließlich an einer GNSS-Antenne hängt.
- ☐ **Versteckte GNSS-Module finden:** Industriesteuerungen (SPS/SCADA), Wechselrichter, Netzschutzgeräte, Bankterminals und Zutrittssysteme prüfen.
- ☐ **Satellitenkommunikation erfassen:** Alle Backup-Internetleitungen (z. B. Starlink) und Satellitentelefone auflisten.

Schritt 2: Kritikalität und Ausfallzeiten bewerten (Impact-Analyse)

- ☐ **Drift-Toleranz & Holdover bestimmen:** Ermitteln, wie lange interne Uhren ohne externes Zeitsignal stabil weiterlaufen (kritisch bei Stromnetzen & Funk).
- ☐ **Fail-Safe-Verhalten prüfen:** Klären, ob Anlagen bei Signalverlust sicherheitshalber abschalten (*Fail-Close*) oder weiterarbeiten (*Fail-Open*).
- ☐ **Kaskadeneffekte abbilden:** Auswirkungen auf Betriebsabläufe bewerten, wenn Mobilfunk, Kartenzahlung und Logistik nacheinander ausfallen.

Schritt 3: Digitale und Cloud-Abhängigkeiten isolieren

- ☐ **Offline-Fähigkeit testen:** Prüfen, ob Leitsysteme, ERP-Software, elektronische Schließanlagen und Kassensysteme ohne Cloud-/Lizenzserver laufen.
- ☐ **Zertifikate & Authentifizierung prüfen:** Sicherstellen, dass Active Directory / Kerberos bei leicht abweichenden Serveruhren stabil bleibt.
- ☐ **Analogen Notfallzugriff sichern:** Passwörter, Netzschaltpläne, Notfallhandbücher und Kontaktlisten lokal und ausgedruckt vorhalten.

Schritt 4: Physische und externe Lieferketten prüfen

- ☐ **Notstrom-Autarkie berechnen:** Laufzeit der Notstromaggregate (Serverräume, Wasserwerke, Leitwarten) ohne Nachschub exakt dokumentieren.
- ☐ **Treibstoff-Logistik unter Ausfallbedingungen:** Sicherstellen, dass Betriebstankstellen im Notstrombetrieb und ohne elektronische Tankkarten funktionieren.
- ☐ **Kritische Zulieferer auditieren:** Notfallpläne von Dienstleistern (Wasserchemie, IT-Wartung, Kraftstoff, Lebensmittel) abfragen.

Schritt 5: Gegenmaßnahmen umsetzen und „Black-Sky“-Test durchführen

- ☐ **Terrestrische Zeit-Redundanz schaffen:** Lokale Atomuhren (Rubidium/Cäsium) oder glasfaserbasierte Zeitdienste (z. B. PTB via PTP) einbinden.
- ☐ **Autarke Kommunikations-Backups:** BOS-Digitalfunk (Direktmodus), Betriebsfunk, Kurzwelle oder lokale Richtfunkstrecken etablieren.
- ☐ **Simulierten Ausfall testen:** In einem Wartungsfenster oder einer Stabsübung GNSS- und Internetverbindung kappen und Notfallprozesse prüfen.

VETTERMANN.DE · STABSRAHMENÜBUNG

Teil 2: Krisen-Drehbuch „Szenario Spaceout“

Tabletop-Übung (90–120 Min.) für Krisenstab, IT-Leitung, Technik, Logistik & Kommunikation

Datum: _____

Leitung: _____

Phase 1: Ausgangslage und Ersteinschätzung (Minute 0–20)

> ***Einspielung (Inject 1):*** *Dienstag, 08:15 Uhr. Mehrere Navigations- und Kommunikationssatelliten im niedrigen und mittleren Erdorbit fallen aufgrund massiver Störungen aus. GPS- und Galileo-Empfänger liefern keine oder stark fehlerhafte Positions- und Zeitdaten.*

1. Wer bemerkt das Problem bei uns zuerst (IT, Fuhrpark, Leitwarte)?
2. Welche Systeme nutzen bei uns aktiv oder im Hintergrund GPS/Galileo-Zeitsignale?
3. Wie informieren wir jetzt unsere Mitarbeitenden, wenn erste Mobilfunkzellen bereits Störungen melden?

Phase 2: Eskalation – IT- und Infrastruktur-Störungen (Minute 20–50)

> ***Einspielung (Inject 2):*** *09:30 Uhr. Durch den Verlust der atomgenauen Zeitsynchronisation brechen das öffentliche Mobilfunknetz und Teile des Internets regional zusammen. Cloud-Dienste sind nicht mehr erreichbar. Erste lokale Server melden Zertifikatsfehler.*

1. Welche geschäftskritischen Anwendungen laufen ohne Internet- und Cloud-Anbindung lokal (*On-Premises*) weiter?
2. Wie kommunizieren unsere Standorte, Außenmitarbeitenden oder Einsatzkräfte jetzt miteinander?
3. Funktionieren elektronische Zutrittskontrollen, Schranken und Kassen-/Abrechnungssysteme noch?

Phase 3: Flächenlage – Strom und Logistik (Minute 50–80)

> ***Einspielung (Inject 3):*** *11:00 Uhr. Wegen Synchronisationsproblemen im europäischen Verbundnetz kommt es zu einem großflächigen Stromausfall (Blackout). Unsere Notstromaggregate springen an, der Treibstoffvorrat reicht für 36 Stunden. Zulieferer stehen ohne Navigation still.*

1. Welche Anlagen werden priorisiert mit Notstrom versorgt – und was schalten wir sofort ab?
2. Wie sichern wir den Nachschub an Diesel für die Notstromaggregate, wenn Tankstellen keinen Strom haben und Kartenzahlungen ausfallen?
3. Welche physischen Akten, Netzpläne oder Kontaktlisten fehlen uns jetzt, weil sie nur digital gespeichert sind?

Phase 4: Auswertung & Top-3-Sofortmaßnahmen (Minute 80–110)

Identifizierte Schwachstelle / Sofortmaßnahme	Verantwortlich	Frist
1.		
2.		
3.		

Fazit: Vom Science-Fiction-Szenario zur realen Vorsorgeaufgabe

Ein Konflikt im Weltraum ist längst kein abstraktes Zukunftsszenario mehr, sondern eine reale sicherheitspolitische Herausforderung. Die größte Verwundbarkeit moderner Gesellschaften wie Deutschland liegt dabei nicht allein im Orbit, sondern in der unsichtbaren Abhängigkeit unserer bodengestützten Infrastruktur von Satellitendaten. Während die Bundeswehr mit Milliardeninvestitionen eigene Weltraumfähigkeiten aufbaut, entscheidet sich die Widerstandsfähigkeit des Landes vor allem am Boden: **Resilienz entsteht durch Entkopplung** – durch lokale Zeitgeber, inselbetriebsfähige Stromnetze und trainierte analoge Rückfallebenen.