PRÜFUNG

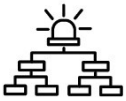
Schutz kritischer Infrastrukturen – Synthesebericht vergangener Prüfungen mit Schwerpunkt Cyberresilienz

Bundesamt für Bevölkerungsschutz, Bundesamt für Cybersicherheit, Staatssekretariat für Sicherheitspolitik

DAS WESENTLICHE IN KÜRZE

Kritische Infrastrukturen sind essenziell für das Funktionieren der Wirtschaft und für die Lebensgrundlagen der Bevölkerung. Dazu gehören etwa die Stromversorgung, die medizinische Versorgung oder die Telekommunikation. Dem Schutz dieser kritischen Infrastrukturen (SKI) kommt eine wichtige Bedeutung zu.

Der Betrieb der kritischen Infrastrukturen kommt heute ohne den Einsatz vernetzter digitaler Technologien nicht mehr aus. Damit erhöht sich aber auch die Wahrscheinlichkeit von Cyberangriffen, und der Cybersicherheit kommt eine Schlüsselrolle beim SKI zu. Vor diesem Hintergrund analysierte die Eidgenössische Finanzkontrolle (EFK) neun ausgewählte frühere Prüfungen (siehe Anhang 4 und 5) mit Bezug zum SKI und mit Schwerpunkt Cyberresilienz. Die EFK leitet sieben Erfolgsfaktoren für eine wirksame Cybersicherheit und Aufsicht darüber ab:

Erfolgsfaktoren Cybersicherheit	Erfolgsfaktoren Aufsicht
 Klare Definition der Rollen und Verantwortlichkeiten	 Verbindliche Vorgaben unter Einbezug der Branchen und föderalen Ebenen erarbeiten
 Updates und Life-Cycle der Systeme in den Wartungsverträgen verankern und durchführen	 Kommunikation und Informationsfluss bei Ereignissen sicherstellen
 Kritische Komponenten angemessen gegen Zugriffe und physische Zutritte schützen	 Resilienzmassnahmen engmaschig beaufsichtigen und kontrollieren
 Reaktionspläne und Notfallorganisationen üben	

Die Cybersicherheit kann bereits mit «einfachen» Massnahmen verbessert werden

Oft können einfache Massnahmen bereits einen wesentlichen Beitrag zu einer besseren Cyberresilienz leisten. So kann etwa eine gut strukturierte Organisation mit klar definierten Rollen und Verantwortlichkeiten positiv auf die Umsetzung der sicherheitsrelevanten Prozesse wirken. Durch einen angemessenen Schutz gegen unbefugtes Zugreifen auf Systeme und/oder den unbefugten Zutritt zu kritischen Komponenten wird die Sicherheit deutlich verbessert. Letztlich ist die Vorbereitung auf einen möglichen Angriff ein «Rettungsanker», der die rasche Wiederaufnahme des Betriebs der kritischen Infrastrukturen unterstützen kann. Reaktionspläne und Übungen helfen bei dieser Vorbereitung zur Wiederaufnahme.

Lange Projekte und Nutzungsdauern sowie veraltete Technologien gefährden die Cybersicherheit

Herausforderungen für die Cyberresilienz stellen die lang dauernden Projekte und die teilweise lange Nutzung der kritischen Infrastrukturanlagen dar. Systeme, die während der Planung dem neusten Stand der Technik entsprechen, sind bei der Inbetriebnahme bereits veraltet. Während die kritischen Infrastrukturanlagen mehrere Jahrzehnte im Einsatz sind, sollten die IKT-Komponenten alle drei bis vier Jahre erneuert werden. Software-Komponenten sollten laufend gewartet und mit Sicherheitspatches aktualisiert werden. Eine stete Erneuerung kann jedoch sehr kostspielig und komplex sein, daher bleibt sie oft aus. In der Folge finden sich in kritischen Infrastrukturen häufig veraltete Komponenten, die Software ist nicht aktuell und weist bekannte Schwachstellen auf. Solche Systeme sind einfache Ziele für Cyberattacken.

Die Betreibenden der kritischen Infrastrukturen sind gefordert, die kritischen Infrastrukturanlagen und deren IKT-Komponenten durch wartungsfreundliche Architekturen, systematische Planungen und konsequente Massnahmenumsetzungen aktuell zu halten.

Der Schutz kritischer Infrastrukturen ist eine Verbund- und Daueraufgabe, die dazu erforderlichen Vorgaben sind zu wenig verbindlich

Die kritischen Infrastrukturen sind in Sektoren und Teilsektoren gegliedert. Je nach Sektor liegen die Aufsichts- und Regulierungsverantwortlichkeiten beim Bund oder bei den Kantonen. Zudem werden viele kritische Infrastrukturen durch private Unternehmen betrieben. All das führt dazu, dass die Überwachung der Betreiber durch die föderalen Behörden erschwert wird. Der Informationsfluss, die Kommunikation und letztlich eine zielgerichtete, rasche Reaktion im Ereignisfall werden behindert.

Die eingesetzten digitalen Technologien ändern sich rasch. Der Aufbau und die Gewährleistung einer robusten Cybersicherheit sind folglich eine Daueraufgabe. Diese kann jedoch nur dann erfolgreich umgesetzt werden, wenn alle am SKI beteiligten Parteien zusammenarbeiten. Die zur Regelung des SKI bestehenden Vorgaben sind heute unvollständig und teilweise zu wenig verbindlich. Die sektoriellen Aufsichts- und Regulierungsbehörden sind deshalb aufgefordert, die Vorgaben zu präzisieren, damit die Umsetzung der Cyberresilienzmassnahmen bei den Betreibenden der kritischen Infrastrukturen eingefordert werden können. Zum Zeitpunkt des Syntheseberichts sind beim Bund zudem Bestrebungen im Gange, die rechtlichen Grundlagen im SKI-Bereich zu prüfen.