DIVERSES

Schutz kritischer Infrastrukturen – Synthesebericht vergangener Prüfungen mit Schwerpunkt Cyberresilienz

Bundesamt für Bevölkerungsschutz, Bundesamt für Cybersicherheit, Staatssekretariat für Sicherheitspolitik

EFK-23160

INKL. STELLUNGNAHMEN

23.04.2024

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS
SWISS FEDERAL AUDIT OFFICE

DOKUMENTINFORMATION

BESTELLADRESSE
ADRESSE DE COMMANDE
INDIRIZZO DI ORDINAZIONE
ORDERING ADDRESS

Eidgenössische Finanzkontrolle (EFK)
Monbijoustrasse 45
3003 Berne
Suisse

BESTELLNUMMER
NUMÉRO DE COMMANDE
NUMERO DI ORDINAZIONE
ORDERING NUMBER

506.23160

ZUSÄTZLICHE INFORMATIONEN
COMPLÉMENT D'INFORMATIONS
INFORMAZIONI COMPLEMENTARI
ADDITIONAL INFORMATION

www.efk.admin.ch
info@efk.admin.ch
+ 41 58 463 11 11

PRIORITÄTEN DER EMPFEHLUNGEN

Die Eidgenössische Finanzkontrolle priorisiert ihre Empfehlungen auf der Grundlage definierter Risiken: 1 = hoch, 2 = mittel, 3 = gering.
Als Risiken gelten beispielsweise unrentable Projekte, Verstösse gegen die Legalität oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Damit werden die Auswirkungen und die Wahrscheinlichkeit des Eintretens beurteilt. Diese Beurteilung richtet sich nach dem konkreten Prüfungsgegenstand (relativ) und nicht nach der Relevanz für die Bundesverwaltung als Ganzes (absolut).

INHALTSVERZEICHNIS

PRÜFUNG

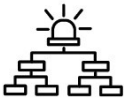
Schutz kritischer Infrastrukturen – Synthesebericht vergangener Prüfungen mit Schwerpunkt Cyberresilienz

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.

AUDIT

Protection des infrastructures critiques – Rapport de synthèse des audits précédents axés sur la cyberrésilience

Office fédéral de la protection de la population, Office fédéral de la cybersécurité, Secrétariat d'État à la politique de sécurité

L'ESSENTIEL EN BREF

Les infrastructures critiques telles que l'approvisionnement en électricité, les soins médicaux ou les télécommunications sont essentielles au fonctionnement de l'économie et à la subsistance de la population. La protection des infrastructures critiques (PIC) revêt une grande importance.

Aujourd'hui, il n'est plus possible d'exploiter des infrastructures critiques sans recourir aux technologies numériques connectées. Cela accroît aussi la probabilité de cyberattaques et la cybersécurité joue un rôle clé dans la PIC. Dans ce contexte, le Contrôle fédéral des finances (CDF) a analysé un échantillon de neuf audits antérieurs (voir annexes 4 et 5) portant sur la PIC et axés sur la cyberrésilience. Le CDF en a déduit sept facteurs de réussite pour une cybersécurité et une surveillance efficaces :

Facteurs de réussite en matière de cybersécurité	Facteurs de réussite en matière de surveillance
Définir clairement les rôles et les responsabilités	Élaborer des directives contraignantes avec la participation des secteurs et des échelons fédéraux
Ancrer et mettre en œuvre les mises à jour des systèmes et les cycles de vie dans les contrats de maintenance	Assurer la communication et la diffusion des informations en cas d'incidents
Protéger les composants critiques de manière appropriée contre les accès virtuels et physiques	Surveiller et contrôler de près les mesures de résilience
S'exercer à mettre en œuvre les plans et les organisations d'intervention d'urgence	

La cybersécurité peut déjà être améliorée avec des mesures « simples »

Souvent, des mesures simples peuvent déjà contribuer de manière significative à une meilleure cyberrésilience. Ainsi, une organisation bien structurée avec des rôles et des responsabilités clairement définis peut avoir un effet positif sur la mise en œuvre des processus liés à la sécurité. Une protection adéquate contre l'accès non autorisé aux systèmes et/ou aux composants critiques améliore considérablement la sécurité. En fin de compte, la préparation à une éventuelle attaque constitue une « bouée de sauvetage » qui peut aider à la reprise rapide de l'exploitation des infrastructures critiques. Les plans d'intervention et les exercices contribuent à la préparation de cette reprise.

Les projets et les durées d'exploitation qui se prolongent ainsi que les technologies obsolètes menacent la cybersécurité

Les projets et l'exploitation des installations d'infrastructures critiques qui se prolongent constituent des défis pour la cyberrésilience. En effet, les systèmes qui sont à la pointe de la technologie pendant la phase de planification sont déjà obsolètes au moment de leur mise en service. Tandis que les installations d'infrastructures critiques sont exploitées pendant plusieurs dizaines d'années, les composants informatiques devraient être remplacés tous les trois à quatre ans. Les composants logiciels devraient faire l'objet d'une maintenance continue et être actualisés au moyen de correctifs de sécurité. Cependant, un renouvellement permanent peut être très coûteux et complexe, raison pour laquelle il n'est souvent pas effectué. Par conséquent, il est fréquent de trouver des composants obsolètes dans les infrastructures critiques, le logiciel n'est pas à jour et présente des vulnérabilités connues. De tels systèmes constituent des cibles faciles pour les cyberattaques.

Les exploitants sont tenus de maintenir à jour les installations d'infrastructures critiques et leurs composants TIC grâce à des architectures faciles à entretenir, des planifications systématiques et une mise en œuvre conséquente des mesures.

La PIC constitue une tâche commune et permanente, les directives nécessaires ne sont pas assez contraignantes

Les infrastructures critiques sont classées par secteurs et sous-secteurs. Selon les secteurs, les responsabilités en matière de surveillance et de réglementation incombent soit à la Confédération, soit aux cantons. En outre, de nombreuses infrastructures critiques sont exploitées par des entreprises privées. Tous ces éléments compliquent la surveillance des exploitants par les autorités fédérales. La diffusion des informations, la communication et une réaction ciblée et rapide en cas d'incident sont ainsi entravées.

Les technologies numériques employées évoluent rapidement. La mise en place et la garantie d'une cybersécurité robuste sont une tâche permanente. Elle ne peut être accomplie que si toutes les parties impliquées dans la PIC travaillent main dans la main. Les directives existantes pour la réglementation de la PCI sont aujourd'hui incomplètes et, pour certaines, trop peu contraignantes. Les autorités sectorielles de surveillance et de réglementation sont donc chargées de préciser les directives afin que la mise en œuvre des mesures de cyberrésilience puisse être exigée des exploitants d'infrastructures critiques. Au moment de la rédaction du rapport de synthèse, la Confédération s'efforce en outre d'examiner les bases légales relatives à la PIC.

VERIFICA

Protezione delle infrastrutture critiche – rapporto di sintesi sulle precedenti verifiche incentrate sulla ciber-resilienza

Ufficio federale della protezione della popolazione, Ufficio federale della cibersicurezza, Segreteria di Stato della politica di sicurezza

L'ESSENZIALE IN BREVE

Le infrastrutture critiche sono essenziali per il buon funzionamento dell'economia e per preservare le basi vitali della popolazione. Tra di esse rientrano, ad esempio, l'approvvigionamento elettrico, l'assistenza medica o le telecomunicazioni. La protezione delle infrastrutture critiche (PIC) è di grande importanza.

Oggigiorno non è più possibile assicurare il funzionamento delle infrastrutture critiche senza l'impiego delle tecnologie digitali interconnesse. Questo aumenta tuttavia il rischio di subire ciberattacchi, ragion per cui la cibersicurezza gioca un ruolo chiave nella PIC. Alla luce di quanto precede, il Controllo federale delle finanze (CDF) ha analizzato una selezione di nove verifiche precedenti (vedi allegati 4 e 5) correlate alla PIC e incentrate sulla ciber-resilienza. In base a queste verifiche, il CDF ha desunto sette fattori di successo per una cibersicurezza efficace e per la relativa vigilanza:

Fattori di successo per la cibersicurezza	Fattori di successo per la vigilanza
Definire chiaramente ruoli e responsabilità	Elaborare direttive vincolanti con il coinvolgimento dei settori specialistici e di tutti i livelli federali
Consolidare ed eseguire gli aggiornamenti e il ciclo di vita dei sistemi nei contratti di manutenzione	Garantire la comunicazione e il flusso di informazioni in caso di eventi
Proteggere in modo adeguato le componenti critiche dagli accessi non autorizzati (fisici e digitali)	Sorvegliare e controllare le misure di resilienza in modo capillare
Svolgere esercitazioni per testare i piani di risposta e le organizzazioni per i casi di emergenza	

La cibersicurezza può essere migliorata da subito tramite misure semplici

Spesso semplici misure possono già contribuire sostanzialmente al miglioramento della ciber-resilienza. Ad esempio, un'organizzazione ben strutturata con ruoli e responsabilità chiaramente definiti può avere effetti positivi sull'attuazione dei processi rilevanti per la sicurezza. Una protezione adeguata contro gli accessi non autorizzati ai sistemi e/o alle componenti critiche consente di migliorare notevolmente la sicurezza. Infine, la preparazione a un eventuale attacco può rivelarsi un'ancora di salvezza, perché favorisce la ripresa rapida dell'esercizio delle infrastrutture critiche. I piani di risposta e le esercitazioni sono strumenti utili in tal senso.

I progetti e i periodi di utilizzo di lunga durata nonché le tecnologie obsolete mettono a rischio la cibersicurezza

I progetti di lunga durata e i periodi di utilizzo estesi degli impianti delle infrastrutture critiche rappresentano una sfida per la ciber-resilienza. I sistemi che durante la fase di pianificazione erano considerati all'avanguardia, risultano già obsoleti al momento dell'entrata in funzione. Mentre gli impianti delle infrastrutture critiche restano in uso per decenni, le componenti TIC vanno sostituite ogni tre o quattro anni. Le componenti software necessitano di una manutenzione costante e di aggiornamenti con patch di sicurezza. Un rinnovo costante può però rivelarsi particolarmente costoso e complesso, perciò spesso vi si rinuncia. Di conseguenza, è frequente trovare nelle infrastrutture critiche componenti obsolete e software non aggiornati che presentano note vulnerabilità. Tali sistemi sono bersagli facili per i ciberattacchi.

I gestori delle infrastrutture critiche sono incoraggiati a mantenere i loro impianti e le relative componenti TIC aggiornati tramite architetture di facile manutenzione, pianificazioni sistematiche e misure corrispondenti.

La protezione delle infrastrutture critiche è un compito congiunto e duraturo, ma le condizioni necessarie al suo svolgimento non sono abbastanza vincolanti

Le infrastrutture critiche sono suddivise in settori e settori parziali. Le responsabilità di vigilanza e di regolamentazione vengono assegnate alla Confederazione o ai Cantoni a seconda del settore. Inoltre, molte infrastrutture critiche sono gestite da imprese private. Di conseguenza, la sorveglianza dei gestori da parte delle autorità federali diventa più difficile. Nel caso di un evento concreto, il flusso di informazioni, la comunicazione e da ultima una risposta rapida ed efficace ne risultano ostacolati.

Le tecnologie digitali impiegate cambiano rapidamente. Lo sviluppo e la garanzia di una cibersicurezza solida rappresentano quindi un compito duraturo che però può essere svolto con successo solo se sussiste una collaborazione tra tutte le parti coinvolte. Attualmente, le direttive vigenti che disciplinano la PIC sono incomplete e talvolta non abbastanza vincolanti. Si raccomanda quindi alle autorità settoriali di vigilanza e di regolamentazione di precisare le direttive, affinché si possa richiedere ai gestori delle infrastrutture critiche di rispettare le misure di ciber-resilienza. Al momento della stesura del rapporto di sintesi, sono in atto sforzi da parte della Confederazione per esaminare le basi legali nel settore della PIC.

AUDIT

Critical infrastructure protection – summary report of past audits, focusing on cyber-resilience

Federal Office for Civil Protection, National Cyber Security Centre, State Secretariat for Security Policy

KEY FACTS

Critical infrastructures are essential for the proper functioning of the economy and for people's livelihoods. They include the power supply, medical care and telecommunications. Protecting these critical infrastructures (CIP) is extremely important.

Nowadays, it is no longer possible to operate critical infrastructures without using networked digital technologies. However, this also increases the likelihood of cyberattacks, which means that cybersecurity plays a key role in CIP. Against this backdrop, the Swiss Federal Audit Office (SFAO) selected nine past audits (see Appendix 4 and Appendix 5) and analysed them in relation to CIP, focusing on cyber-resilience. The SFAO identified seven success factors for effective cybersecurity and supervision:

Cybersecurity success factors	Supervision success factors
Clearly define roles and responsibilities	Establish binding requirements in consultation with the sectors and the different federal levels
Anchor and implement system updates and life cycles in maintenance contracts	Ensure communication and an efficient flow of information in the event of incidents
Protect critical components appropriately against access and physical intrusion	Closely monitor and control resilience measures
Conduct drills of response plans and emergency organisations	

Cybersecurity can be improved even with "simple" measures

Simple measures can often make a major contribution to improving cyber-resilience. For example, a well-structured organisation with clearly defined roles and responsibilities can have a positive impact on the implementation of security-related processes. Appropriate protection against unauthorised access to systems and/or unauthorised physical access to critical components significantly improves security. Ultimately, preparing for a possible attack is a type of lifeline to help rapidly resume the operation of critical infrastructures. Response plans and drills help with this recovery preparation.

Long projects and service lives, as well as outdated technologies jeopardise cybersecurity

Lengthy projects and the sometimes prolonged use of critical infrastructure facilities pose challenges in terms of cyber-resilience. Systems that are state of the art during planning are already outdated by the time they go into operation. While critical infrastructure systems can be used for several decades, the ICT components should be replaced every three to four years. Software components should be continuously maintained and updated with security patches. However, as ongoing renewal can be very costly and complex, it is often not

carried out. This means that critical infrastructures tend to have outdated components, and the software is not always up to date and has known vulnerabilities. Such systems are easy targets for cyberattacks.

Critical infrastructure operators are required to keep critical infrastructure facilities and their ICT components up to date by means of architecture that is easy to maintain, systematic planning and consistent implementation of measures.

Protecting critical infrastructures is a joint, long-term task, and the necessary requirements are not sufficiently binding

Critical infrastructures are divided into sectors and sub-sectors. Depending on the sector, supervisory and regulatory responsibilities lie with the federal government or the cantons. Moreover, many critical infrastructures are operated by private companies. All of this makes it more difficult for the federal authorities to monitor operators. The flow of information, communication and ultimately a targeted, rapid response in the event of an incident are hindered.

The digital technologies used change quickly. Consequently, establishing and ensuring robust cybersecurity is an ongoing task, but it can be successfully performed only if all parties involved in CIP work together. The existing CIP requirements are currently incomplete and, in some cases, not binding enough. The sectoral supervisory and regulatory authorities are thus called upon to make the requirements more precise, so that the implementation of cyber-resilience measures can be imposed on critical infrastructure operators. At the time of the summary report, federal efforts were also under way to review the legal basis in the CIP area.

GENERELLE STELLUNGNAHME DES BUNDESAMTES FÜR BEVÖLKERUNGSSCHUTZ

Das BABS bedankt sich bei der EFK für die konstruktive Zusammenarbeit und die Bestrebungen, die Cyber-Resilienz der kritischen Infrastrukturen weiter zu verbessern. Das BABS unterstützt insbesondere die Empfehlung, dass vor allem die sektoriellen Aufsichts- und Regulierungsbehörden aufgefordert sind, unter Einbezug der Branchen und der föderalen Ebenen die Vorgaben verbindlicher auszugestalten.

GENERELLE STELLUNGNAHME DES BUNDESAMTES FÜR CYBERSICHERHEIT

Das NCSC dankt der EFK für den Synthesebericht vergangener Prüfungen zum Schutz kritischer Infrastrukturen mit Schwerpunkt Cyberresilienz. Es zeigt sich mit dem Bericht und den Einschätzungen der EFK einverstanden und unterstützt die im Bericht aufgezeigten Erfolgsfaktoren für eine angemessene Cybersicherheit resp.-resilienz bei den kritischen Infrastrukturen.

1 AUFTRAG UND VORGEHEN

1.1 Ausgangslage

Kritische Infrastrukturen sind Prozesse, Systeme und Einrichtungen die für das Funktionieren der Wirtschaft und für die Lebensgrundlagen der Bevölkerung essenziell sind. Nebst vielem anderem zählen die Stromversorgung, die Blaulichtorganisationen oder die Telekommunikation dazu.

Um den Schutz der kritischen Infrastrukturen (SKI) möglichst optimal sicherzustellen, sind durch den Bund folgende Strategien in Kraft gesetzt worden:

- Nationale Strategie zum Schutz kritischer Infrastrukturen vom Juni 2023
- Nationale Cyberstrategie (NCS) vom April 2023.

Während die SKI-Strategie einen ganzheitlichen Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen verfolgt, fokussiert die NCS als Querschnittsthema auf die Cybersicherheit. Der SKI hat zum Ziel, die Verfügbarkeit von wichtigen Gütern und Dienstleistungen zu gewährleisten. Dabei handelt es sich um Massnahmen, mit denen die Resilienz der kritischen Infrastrukturen verbessert und Ausfälle verhindert oder im Ereignisfall die Auswirkungen reduziert werden sollen. Die Wiederherstellung des Normalbetriebes soll so beschleunigt werden.

Die kritischen Infrastrukturen sind in Sektoren und Teilsektoren aufgeteilt (z. B. Sektor Energie und Teilsektoren Erdgasversorgung, Erdölversorgung, Stromversorgung, Fern- und Prozesswärme – siehe Anhang 5). Es gibt Teilsektoren mit Querschnittsfunktionen, wie beispielweise Energie und Telekommunikation. Dementsprechend sind auch die Verantwortlichkeiten im Bereich des SKI vielschichtig. Die Kompetenzen für die Festlegung von Vorgaben in Bezug auf die Resilienz der kritischen Infrastrukturen liegen je nach Sektor beim Bund (z. B. Energieversorgung), bei den Kantonen (z. B. medizinische Versorgung) oder gar auf kommunaler Ebene (z. B. Wasserversorgung).

Die sektoriellen Aufsichts- und Regulierungsbehörden sind gemäss SKI-Strategie beauftragt zu prüfen, ob die Vorgaben angemessen sind oder angepasst werden müssen. Die Betreibenden der kritischen Infrastrukturen sind für die Einhaltung der Vorgaben und die Gewährleistung einer minimalen Sicherheit verantwortlich. Diese Verantwortung kann auch nicht an die Aufsichtsbehörden der Sektoren/Teilsektoren delegiert werden. Die föderalen Aufsichtsbehörden haben die Aufgabe, die Umsetzung der Vorgaben zu prüfen und damit die Betreibenden der kritischen Infrastrukturen bestmöglich beim SKI zu unterstützen.

Der Betrieb und das Funktionieren der kritischen Infrastrukturen hängt zunehmend von der Verfügbarkeit und der korrekten Funktion von Informatik- und Kommunikationsmitteln (IKT) ab. Der Cybersicherheit resp.-resilienz kommt daher eine Schlüsselrolle beim SKI zu.

1.2 Kritische Infrastrukturen – Prüfungskompetenzen, Aufsicht und Verantwortlichkeiten

Der SKI erstreckt sich über alle föderalen Ebenen und darüber hinaus auf die privatwirtschaftlichen Betreibenden von kritischen Infrastrukturen. Wie aus Anhang 5 ersichtlich, sind je Teilsektor oftmals mehrere Bundesstellen als zuständige Aufsicht- und Regulierungsbehörde bezeichnet. Das Bundesamt für Bevölkerungsschutz (BABS) ist für die übergeordnete Koordination zuständig, hat jedoch keine Vorgabe- oder Regulierungskompetenz. Zudem sind je nach Teilsektor die Zuständigkeiten zwischen Bund und Kantonen getrennt oder es bestehen sogar gemeinsame Kompetenzen von Bund und Kantonen im selben Teilsektor. Das BABS ist zum Zeitpunkt dieser Synthese daran, die Kompetenzverteilung zwischen Bund und Kantonen zu klären. In den Sektoren, in denen die föderalen Verantwortlichkeiten klar definiert sind, lassen sich auch die Zuständigkeiten der verschiedenen Aufsichtsbehörden und Prüfinstanzen (z. B. Eidgenössische Finanzkontrolle (EFK), kantonale Finanzkontrollen) ableiten. So kann die EFK bspw. im Teilsektor Stromversorgung die Aufsichtsbehörden (z. B. BFE, ELCOM) prüfen, hat dann jedoch keine Kompetenzen, die Stromproduzenten zu auditieren. Analog dazu kann die EFK im Teilsektor medizinische Versorgung zwar beim Bundesamt für Gesundheit prüfen, hat jedoch keine Kompetenzen auf Ebene der Spitäler.

Das Finanzkontrollgesetz legt in Art. 8 die Aufsichtsbereiche der EFK fest, namentlich bei den Verwaltungseinheiten der zentralen und dezentralen Bundesverwaltung, den Parlamentsdiensten, den Empfängerinnen und Empfängern von Abgeltungen und Finanzhilfen, Organisationen denen der Bund die Erfüllung öffentlicher Aufgaben übertragen hat und Unternehmen an denen der Bund mit mehr als 50 % beteiligt ist. Damit hat die EFK zwar weitgehende, aber dennoch begrenzte Prüfungskompetenzen. Eine abschliessende Festlegung dieser Kompetenzen über alle Teilsektoren bis auf Stufe der Betreibenden von kritischen Infrastrukturen ist kompliziert und muss jeweils fallweise geklärt werden.

Aufgrund der erwähnten föderalen Strukturen, im Bereich der kritischen Infrastrukturen haben daher auch die kantonalen Finanzkontrollen die Kompetenz, Prüfungen bei kritischen Infrastrukturen durchzuführen. Unberührt von allen Prüfungen und Aufsichtstätigkeiten verbleibt die Verantwortung für eine angemessen geschützte kritische Infrastruktur bei den jeweiligen Betreibenden.

1.3 Zielsetzung Synthese

Die EFK will mit dem vorliegenden Synthesebericht mögliche Erfolgsfaktoren für eine angemessene Cybersicherheit resp.-resilienz bei den kritischen Infrastrukturen aufzeigen. Der Bericht soll gleichermassen die Aufsicht und die Betreibenden unterstützen. Die Erfolgsfaktoren leiten sich aus den Ergebnissen von neun ausgewählten EFK-Prüfungen aus den Jahren 2020 bis 2023 ab. Die einzelnen Prüfungen sind in Anhang 4 aufgelistet. Die sieben herausgearbeiteten Faktoren sind nicht abschliessend. Sie sollen jedoch alle im Zusammenhang mit dem SKI beteiligten Parteien dazu motivieren, ihren Wirkungsbeitrag selbstkritisch zu hinterfragen und ggf. Verbesserungsmassnahmen um-zusetzen und so zu einem besseren Schutz der kritischen Infrastrukturen beitragen. Details zu den angeführten Beispielen finden sich in den publizierten Einzelberichten.

1.4 Umfang und Grundsätze des Synthesesberichts

Die vorliegende Synthese wurde zwischen Dezember 2023 und Februar 2024 von Frank Ihle (Revisionsleitung) zusammen mit Roland Gafner erarbeitet. Sie erfolgte unter der Federführung von Bernhard Hamberger. Da die Synthese sich auf neun durchgeführte EFK-Prüfungen stützt, deckt sie nur einen kleinen Teil der Sektoren sowie Teilsektoren der kritischen Infrastrukturen ab und ist somit nicht repräsentativ (siehe Anhang 5). Der Fokus der ausgewählten Prüfungen lag hauptsächlich auf der Anwendung des «Minimalstandards zur Verbesserung der IKT-Resilienz» des Bundesamts für wirtschaftliche Landesversorgung (BWL – siehe auch Kapitel 3). Die jeweiligen Weiterentwicklungen nach den einzelnen Prüfungen wurden nicht berücksichtigt.

Allfällige Prüfungsberichte zu kritischen Infrastrukturen von kantonalen Finanzkontrollen und interne Revisionen wurden nicht berücksichtigt.

1.5 Schlussbesprechung

Der Synthesebericht wurde zwischen der EFK, dem BABS, dem Bundesamt für Cybersicherheit und dem Staatssekretariat für Sicherheitspolitik auf dem Korrespondenzweg bereinigt. Auf die formale Schlussbesprechung konnte im gegenseitigen Einvernehmen verzichtet werden.

Die EFK dankt für die gewährte Unterstützung.

EIDGENÖSSISCHE FINANZKONTROLLE

2 BESONDERHEITEN KRITISCHER INFRASTRUKTUREN

In einer zunehmend vernetzten Welt, in der kritische Infrastrukturen wie Energieversorgung, Verkehrssysteme und/oder Kommunikationsnetze immer stärker von Informationstechnologie und vernetzten Systemen abhängig sind, gewinnt das Thema Cybersicherheit resp.-resilienz eine immer grössere Bedeutung. Die Bedrohungen durch Cyberangriffe auf diese lebenswichtigen Systeme sind real und können verheerende Auswirkungen haben.

Der Einsatz der Informationstechnologie ermöglicht zwar Effizienzsteigerungen, birgt jedoch auch entsprechende Risiken. Cyberangriffe können die Verfügbarkeit, Integrität und Vertraulichkeit dieser Systeme gefährden und somit die Funktionsfähigkeit der Infrastruktur beeinträchtigen.

Die Bedeutung der Cyberresilienz liegt darin, dass sie dazu beiträgt, die Auswirkungen von Cyberangriffen zu minimieren und die Widerstandsfähigkeit der Infrastruktur zu stärken. Dies kann durch die Implementierung von Sicherheitsmassnahmen wie Firewalls, Intrusion Detection Systemen und regelmässige Sicherheitsaudits geschehen, aber auch durch den Aufbau von Systemarchitekturen, die eine Abschaltung der Systeme oder ihrer Teile aushalten können, ohne komplett den Dienst zu versagen. Darüber hinaus ist es wichtig, dass Organisationen, die kritische Infrastrukturen betreiben, über Notfallpläne verfügen, um schnell und wirksam auf Cyberangriffe reagieren und die Funktionsfähigkeit rasch wiederherstellen zu können.

Die Massnahmen zur Gewährleistung einer angemessenen Cyberresilienz können und müssen keine absolute Sicherheit anstreben. Sie sollten aber in der Lage sein, erwartete Angriffe abzuwehren oder genügend Zeit zu gewinnen, um einen vorbereiteten Notbetrieb aufzunehmen und Schäden oder Einschränkungen für die Wirtschaft und die Bevölkerung zu vermeiden resp. zu minimieren. Da Cyberangriffe nie ganz ausgeschlossen werden können, leisten diese Vorkehrungen einen wichtigen Beitrag zur Verbesserung der Resilienz. Cyberangriffe werden immer raffinierter und fortschrittlicher, weshalb eine kontinuierliche Überwachung und Anpassung der Sicherheitsmassnahmen erforderlich ist. Die Komplexität liegt darin, dass die Zusammenarbeit zahlreicher Stakeholder im öffentlichen und im privaten Bereich notwendig ist, um die Cyberresilienz der kritischen Infrastrukturen zu verbessern.

2.1 Die Herausforderungen beim sicheren Betrieb von kritischen Infrastrukturen sind systematisch anzugehen

Die Cybersicherheit resp.-resilienz von kritischen Infrastrukturen birgt eine Vielzahl von Herausforderungen. Die Systeme sind oft hochkomplex, vernetzt und von verschiedenen Akteurinnen und Akteuren über lange Zeiträume und unter massiven Investitionen aufgebaut worden. Zu den wichtigsten Herausforderungen zählen:

- Eine fehlende Redundanz sowie veraltete Systeme und Technologien: Viele kritische Infrastrukturen werden aus Kostengründen oder Gründen der Komplexität nicht regelmässig erneuert und sind auch nicht redundant aufgebaut. Das führt einerseits zu veralteten Technologien und Systemen, die über kurz oder lang nicht mehr von Herstellern unterstützt werden. Andererseits führt die fehlende Redundanz gepaart mit hohen Anforderungen an die Verfügbarkeit der Systeme dazu, dass zu wenig Zeit für die Wartung und Updates der eingesetzten Firmware und Software besteht. Dies erschwert die Implementierung von Sicherheitspatches und Updates, was diese Systeme anfälliger für bereits bekannte Cyberangriffsverfahren macht (siehe auch Kapitel 2.2).
- Interkonnektivität: Kritische Infrastrukturen sind zunehmend miteinander vernetzt oder sogar über das Internet erreichbar, um Effizienz und Leistung zu verbessern und die Wartung zu vereinfachen. Diese Interkonnektivität erhöht jedoch auch die Angriffsfläche für Cyberangriffe.
- Mangelnde Ressourcen: Einigen Betreibenden von kritischen Infrastrukturen, insbesondere bei kleinen Organisationen, stehen begrenzte Ressourcen für die Cybersicherheit zur Verfügung. Dies kann die Implementierung und Wartung von Sicherheitsmassnahmen sowie rasche und zielführende Reaktionen auf Cyberereignisse verhindern. Fehlende Ressourcen führen auch dazu, dass

Angriffe in Echtzeit schlechter erkannt werden, insbesondere wenn Angreifende fortschrittliche Taktiken zur Verschleierung ihrer Aktivitäten einsetzen.

- Fehlende Standardisierung: Es gibt keine internationalen, einheitliche Cybersicherheitsstandards für kritische Infrastrukturen, da die verschiedenen Sektoren unterschiedliche Anforderungen und Bedrohungen haben. Dies erschwert die Entwicklung branchenübergreifender Sicherheitslösungen. Die Schweiz versucht diesem Umstand mit dem IKT-Minimalstandard des BWL entgegenzuwirken.

Um diesen Herausforderungen zu begegnen, ist eine umfassende Herangehensweise an die Cybersicherheit erforderlich, die Architektur, Technologie, Richtlinien, Zusammenarbeit, Schulung und kontinuierliche Anpassungen umfasst.

2.2 Die Anforderungen an die Verfügbarkeit stehen im Vordergrund

Sicherheitsziele spiegeln die grundlegenden Prinzipien der Informationssicherheit wider und sind entscheidend, um die Funktionsfähigkeit und Zuverlässigkeit von kritischen Infrastrukturen zu schützen. Die Sicherheitsziele können wie folgt zusammengefasst werden:

- Verfügbarkeit: Gewährleistung der kontinuierlichen Verfügbarkeit von Diensten und Ressourcen. Dies schliesst Massnahmen wie Redundanz, Notfallwiederherstellung und gehärtete Systeme ein, um Ausfälle durch Naturkatastrophen, Unfälle oder gezielte Angriffe zu minimieren.
- Integrität: Sicherstellung der Unversehrtheit von Daten und Systemen. Durch die Implementierung von Integritätskontrollen wird sichergestellt, dass Daten oder Systeme nicht unbemerkt verändert werden – sei es durch absichtliche Angriffe oder unbeabsichtigte Vorfälle.
- Vertraulichkeit: Schutz vor unberechtigtem Zugriff auf sensible Informationen. Dies umfasst Massnahmen wie Verschlüsselungen, Zugriffskontrollen und Datenschutz, um sicherzustellen, dass nur autorisierte Personen oder Systeme auf bestimmte Informationen zugreifen können.

Anders als in der klassischen Informatik sind die Sicherheitsziele bei kritischen Infrastrukturen darauf ausgerichtet, in erster Linie die Verfügbarkeit zu gewährleisten. Die Integrität und Vertraulichkeit der Systeme sind dabei in der Regel sekundäre Ziele.

Unterschiede Informationstechnologie und Operative Technologie

IT steht für Informationstechnologie und bezieht sich auf die Verarbeitung, Speicherung und Übertragung von Informationen mithilfe von Computern und Netzwerken.

OT hingegen steht für Operative Technologie und bezieht sich auf die Technologie, die in industriellen Prozessen und Anlagen zur Automatisierung von Abläufen eingesetzt wird. OT umfasst beispielsweise die Steuerung von Maschinen und die Überwachung von Produktionsprozessen.

Der Hauptunterschied zwischen IT und OT liegt in ihrem Anwendungsbereich. Während IT sich auf die Verarbeitung von Informationen konzentriert, liegt der Fokus von OT auf der Steuerung und Überwachung von physischen Prozessen. Allerdings verschmelzen diese beiden Bereiche zunehmend, da Unternehmen verstärkt auf vernetzte Systeme setzen, um ihre Produktionsprozesse effizienter zu gestalten.

---

3 OPERATIVE SCHWACHSTELLEN AUS DEN AUSGEWÄHLTEN PRÜFUNGEN

Die EFK hat in den vergangenen Jahren verschiedene Betreibende von kritischen Infrastrukturen auf deren Cyberresilienz geprüft. Dabei ist in den meisten Fällen auf der technischen Ebene der «Minimalstandard zur Verbesserung der IKT-Resilienz» des BWL zum Einsatz gekommen.

IKT-Minimalstandard als Ausdruck der Schutzverantwortung des Staates

Der IKT-Minimalstandard des BWL dient als Empfehlung und mögliche Leitplanke zur Erhöhung der IKT-Resilienz. Er kann als Nachschlagewerk dienen und vermittelt Hintergrundinformationen zur IKT-Sicherheit. Das Framework und das dazu gehörende Self-Assessment-Tool bieten den Anwenderinnen und Anwendern ein Bündel konkreter Massnahmen zur Umsetzung an. Die Massnahmen sind nach fünf Themenbereichen gegliedert: «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen».

Der IKT-Minimalstandard setzt dort an, wo sich die Gesellschaft Ausfälle am wenigsten leisten kann: bei den IKT-Systemen, die für das Funktionieren der kritischen Infrastrukturen von Bedeutung sind. Betreibenden von kritischen Infrastrukturen wird empfohlen, den vorliegenden IKT-Minimalstandard oder vergleichbare Vorgaben umzusetzen. Obschon er sich vornehmlich an die Betreibenden von kritischen Infrastrukturen richtet, ist er grundsätzlich für jedes Unternehmen anwendbar.

Der Standard kennt vier Stufen für die Bewertung der Maturität. Diese beschreiben das Schutzniveau, das ein Unternehmen umgesetzt hat.

0 Nicht umgesetzt

1 Partiell umgesetzt, nicht vollständig definiert und abgenommen

2 Partiell umgesetzt, vollständig definiert und abgenommen

3 Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch

4 Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert

Zur Festlegung des eigenen Schutzniveaus (Soll-Wert) soll eine Organisation ihre Risikomanagementpraktiken, die Bedrohungslage sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorische Vorgaben genau kennen und berücksichtigen.

3.1 Mangelnde Sicherheitsgovernance und unzureichende Ressourcen stellen ein erhebliches Risiko dar

Fehlt eine angemessene Governance bei der Cybersicherheit, kann dies dazu führen, dass einer Vielzahl von Risiken ungenügend begegnet wird und die Cybersicherheit von Informationen und Systemen gefährdet ist. Ohne eine effektive Kontroll- und Steuerungsstruktur mit klaren Rollen und Verantwortlichkeiten besteht die Gefahr, dass Sicherheitsmassnahmen lückenhaft sind oder nicht den aktuellen Bedrohungen entsprechen. Erfolgreiche Cyberangriffe, bei denen Daten gestohlen und Systeme beschädigt oder beeinträchtigt werden, können die Folge sein.

In verschiedenen Prüfungen hat die EFK festgestellt, dass nicht genügend Ressourcen für die Implementierung und Aufrechterhaltung angemessener Cybersicherheitsmassnahmen eingesetzt wurden. Dies beeinträchtigt die Effektivität der Sicherheitsbemühungen erheblich.

Um diesen Risiken angemessen zu begegnen, ist eine umfassende Governance bei der Cybersicherheit erforderlich. Sie muss klare Richtlinien, Prozesse und Verantwortlichkeiten in einer Organisation festlegen. Insbesondere müssen alle relevanten Stakeholder beteiligt sein, regelmässige Schulungen und Risikobewertungen erfolgen sowie Sicherheitsrichtlinien und ein ganzheitlicher Ansatz zur Cybersicherheit vorliegen.

3.2 Geräte und Software sind oftmals veraltet

Die Herausforderungen bei der Aktualisierung der IKT-Komponenten von kritischen Infrastrukturen sind auf verschiedene Faktoren zurückzuführen. Kritische Infrastrukturen umfassen oft komplexe Systeme, die aus verschiedenen Technologien, Plattformen und Anwendungen bestehen. Die konstante Aktualisierung solcher Systeme ist aufwändig, teuer und erfordert sorgfältige Planung, um sicherzustellen, dass alle Komponenten miteinander kompatibel bleiben und dass es zu keinen unerwarteten Problemen kommt. Darüber hinaus können die allgemein hohen Verfügbarkeitsanforderungen die für die Wartung zur Verfügung stehende Zeit stark beschränken.

Einige kritische Infrastrukturen nutzen veraltete Technologien, für die teilweise keine Updates oder Sicherheitspatches mehr verfügbar sind. Der Mangel an Unterstützung durch die Herstellerinnen und Hersteller kann die Aktualisierung verunmöglichen und lässt die Systeme anfälliger für bekannte Sicherheitslücken werden.

Erschwerend hinzu kommt die oft sehr lange Projektdauer beim Aufbau von kritischen Infrastrukturen. So sind Geräte und Systeme bei der Planung in der Regel auf dem neusten Stand, während dies Jahre später bei der Auslieferung resp. Inbetriebnahme kaum mehr der Fall ist. Dieselbe Problematik stellt sich bei den oft langen Nutzungszeiten. Während allgemeine IKT-Komponenten eine Lebensdauer von drei bis vier Jahren haben, sind es bei Systemen der OT oft mehr als 30 Jahre.

Um diesen Herausforderungen begegnen zu können, ist es entscheidend, dass die Betreibenden von kritischen Infrastrukturen systematisch Massnahmen ergreifen, um ihre Systeme auf einem aktuellen Stand zu halten und die Cybersicherheit zu gewährleisten. Dies kann nur durch eine sorgfältige Planung, durch Schulungen für das Personal und enge Zusammenarbeit mit den entsprechenden Aufsichts- und Regulierungsbehörden sowie Lieferanten erreicht werden.

3.3 Ein mangelnder Zugriffsschutz kann kritische Infrastrukturen erheblich gefährden

Zugriffsmanagement

Fehlt ein effektives Zugriffsmanagement, birgt dies erhebliche Gefahren und Risiken für die Sicherheit von Informationssystemen, Daten und Infrastrukturen. Ohne eine angemessene Benutzer- und Schlüsselverwaltung besteht die Gefahr, dass Benutzende unberechtigten Zugriff auf sensible Informationen und Systeme oder unberechtigten Zugang zu Infrastrukturen erhalten. Dies könnte zu Datenlecks, Datenschutzverletzungen und unbefugter Nutzung bzw. Störung von Ressourcen führen. Eine Manipulation von Systemen oder Daten kann erhebliche Auswirkungen auf die Integrität haben und den Betrieb einer kritischen Infrastruktur gefährden.

Um diese Gefahren zu minimieren, ist ein umfassendes Zugriffsmanagement unerlässlich. Dies beinhaltet die Implementierung starker Zugriffskontrollen, die regelmässige Überprüfung von Benutzerberechtigungen, das Prinzip der minimalen Rechte *(Least Privilege)*, die Verwendung sicherer Passwortrichtlinien, Schulungen und Sensibilisierungen für Mitarbeitende und die Implementierung von Mechanismen zur Überwachung und Rückverfolgbarkeit von Benutzeraktivitäten.

Physische Sicherheit und Zugangsschutz

Auch ein mangelnder physischer Schutz von Infrastrukturen kann schwerwiegende Konsequenzen haben und verschiedene Gefahren mit sich bringen. Er kann dazu führen, dass Angreiferinnen und Angreifer unbefugten Zugang und Zugriff erhalten, Systeme manipulieren, Daten stehlen oder den normalen Betrieb stören. Angriffe auf die Infrastruktur können zu Ausfallzeiten und Betriebsstörungen führen. Die Auswirkungen können von der Beeinflussung von industriellen Steuerungssystemen bis hin zur Manipulation von Verkehrsleitsystemen oder Wasserversorgungen reichen. Solche Angriffe können erhebliche wirtschaftliche Auswirkungen haben. Sie können sogar die Sicherheit der Öffentlichkeit gefährden, insbesondere in kritischen Sektoren wie Energie, Verkehr oder Gesundheit.

Um diese Gefahren zu minimieren, ist ein umfassender Ansatz zur Sicherheit von Infrastrukturen erforderlich. Dazu gehören regelmässige Sicherheitsbewertungen, die Implementierung von Sicherheitsstandards, Schulungen für Mitarbeitende und eine permanente Überwachung sensibler Bereiche. Eine Zusammenarbeit zwischen Aufsichts- und Regulierungsbehörden, Unternehmen derselben Branche und anderen relevanten Akteurinnen und Akteuren (z. B. Lieferanten) ist auch hier entscheidend, um einen wirksamen Schutz zu gewährleisten.

3.4 Die Wiederaufnahme des Betriebs nach Störungen will geplant und geübt sein

Business Continuity Management (BCM) bezieht sich auf die Strategien und Massnahmen, die Organisationen implementieren, um sicherzustellen, dass sie ihre geschäftskritischen Funktionen auch in Zeiten von Störungen oder Katastrophen aufrechterhalten können. Die analysierten Prüfungen haben auch in diesem Bereich Schwachstellen aufgezeigt.

Eine unzureichende Dokumentation von BCM-Plänen und-Verfahren sowie eine mangelhafte Kommunikation darüber, wie im Notfall vorzugehen ist, können zu Verwirrung und Unsicherheit im Krisenfall führen. Notfallpläne müssen geschult und die Mitarbeitende für ihre Rollen und Verantwortlichkeiten vorbereitet werden. Die Geschäftsumgebungen, Technologien und Risiken ändern sich ständig. Wenn BCM-Pläne nicht regelmässig überprüft und aktualisiert werden, könnten sie veraltet sein und im Ernstfall nicht effektiv funktionieren. Die Wirksamkeit von BCM-Plänen hängt von regelmässigen Tests und Schulungen ab. Wenn Pläne nicht realitätsnah getestet werden, können Schwachstellen übersehen werden, und im Ernstfall könnten Probleme auftreten, die in einem Testumfeld nicht berücksichtigt wurden.

Die Vermeidung dieser Mängel erfordert eine umfassende und systematische Herangehensweise an das BCM. Sie muss eine Risikobewertung, eine klare Kommunikation, regelmässige Schulungen, eine sorgfältige Planung und Tests einschliessen.

4 HERAUSFORDERUNGEN DER AUFSICHT

Cybersicherheit ist eine permanente Herausforderung

Cybersicherheit ist keine «Einmalaufgabe», sondern eine permanente Herausforderung, der sich alle Betreibenden von kritischen Infrastrukturen und auch die zuständigen Aufsichts- und Regulierungsbehörden stellen müssen.

Verbundaufgabe Aufsicht und Betreibende von kritischen Infrastrukturen

Der SKI ist eine Verbundaufgabe zwischen den sektoriellen Aufsichts- und Regulierungsbehörden und den Betreibenden der kritischen Infrastrukturen. Dabei zeigen sich die föderalen Strukturen als zusätzliche Herausforderung in der Zusammenarbeit. Die sektorspezifischen Aufsichts- und Regulierungsbehörden sind einerseits für die Festlegung der Anforderungen an die Cyberresilienz der kritischen Infrastrukturen und andererseits für die Überwachung ihrer Umsetzung verantwortlich. Unberührt von der Aufsicht verbleibt die Verantwortung für die Sicherstellung des Schutzes der kritischen Infrastrukturen bei den Betreibenden.

Wie sich im Teilsektor Schienenverkehr zeigte, treffen kleinere Unternehmen aufgrund der knappen Ressourcen (Kapazitäten und Fähigkeiten) auf grössere Herausforderungen bei der Umsetzung der Cybersicherheitsvorgaben. Aus Sicht der EFK ist es nicht auszuschliessen, dass ähnliche Situationen auch bei Betreibenden von kritischen Infrastrukturen in anderen Teilsektoren auftreten können. Die sektorspezifischen Aufsichts- und Regulierungsbehörden sind hier gefordert, die einzuhaltenden Vorgaben mit «Augenmass» festzulegen. Dabei ist unter Berücksichtigung der jeweiligen Kritikalität die Frage hinsichtlich des zu erreichenden Maturitätsniveaus des jeweiligen Betreibenden der kritischen Infrastruktur zu beantworten. Ein weiterer möglicher Lösungsansatz seitens der Betreibenden von kritischen Infrastrukturen könnte, im Sinne der Stärkung von «kleineren» Unternehmen, auch die Förderung der Zusammenarbeit in den Branchen beim Thema Cybersicherheit sein.

Erfolgsfaktoren Aufsicht

In einer Querschnittsbetrachtung lassen sich aus den ausgewählten Prüfberichten verschiedene Aufgabenbereiche der Aufsicht mit Verbesserungspotenzial erkennen. Dabei handelt es sich Beispielsweise um Themen wie, etwa verbindliche Vorgaben, Transparenz in der Kommunikation und Informationsfluss im Ereignisfall sowie die angemessene Überprüfung der Einhaltung der Vorgaben. Im Umkehrschluss ergeben sich daraus die Erfolgsfaktoren für eine wirkungsvollere Aufsicht.

4.1 Vorgaben sollten verbindlicher werden

Insbesondere die «Prüfung des Schutzes kritischer Infrastrukturen – Governance und integrales Risikomanagement» (PA 22116) zeigt auf, dass den SKI-Grundlagen teilweise die Verbindlichkeit fehlt.[1] Dementsprechend sind die sektoriellen Aufsichts- und Regulierungsbehörden gefordert, die Vorgaben in den verschiedenen Bereichen verbindlicher auszugestalten, die Governance im Bereich des SKI zu verbessern und damit, die Umsetzung von Massnahmen einzufordern. Die Vorgaben sollten dabei nach einer einheitlichen Methodik und unter Berücksichtigung der föderalen Strukturen erarbeitet werden. Die sektorspezifischen Eigenheiten müssen dabei in den jeweiligen Vorgaben aufgenommen werden.

Wie aus der Motion 23.3001 «Zeitgemässe Rechtsgrundlagen für den Schutz kritischer Infrastrukturen» hervorgeht[2], sind die Rechtsgrundlagen je nach Teilsektor sehr unterschiedlich. Dies ist insbesondere darauf zurückzuführen, dass der Bund aus verfassungsrechtlichen Gründen keine umfassende Regulierungskompetenz hat. Er verfügt jedoch über die Möglichkeit, in Bereichen, in denen er über entsprechende Kompetenzen verfügt und besonderer Handlungsbedarf besteht, die sektoriellen Bundesgesetze

[1] Verfügbar auf der Website der EFK.

[2] Eingereicht von der sicherheitspolitischen Kommission, Ständerat, 12.1.2023.

anzupassen. Das BABS arbeitet zum Zeitpunkt der Erstellung dieses Syntheseberichtes daran, die Ausgangslage und Voraussetzungen für sektorübergreifende Vorgaben zu evaluieren.

Heute sind die Vorgaben zum SKI oft in Form von Empfehlungen formuliert, wie beispielsweise der Minimalstandard zur Verbesserung der IKT-Resilienz des BWL. Das Instrument des Minimalstandards ist sehr nützlich, aufgrund des Empfehlungscharakters gegenüber den Betreibenden von kritischen Infrastrukturen fehlt es aber an Verbindlichkeit und teilweise auch an Durchsetzungskraft. Die Umsetzung von Verbesserungsmassnahmen kommt, wenn überhaupt, nur zögerlich voran. Die Aufsicht kann in einem solchen Fall den Betreibenden der kritischen Infrastrukturen «nur» motivieren, die Schutzmassnahmen zu verbessern. Sie kann jedoch nicht die Umsetzung einfordern.

Im Teilsektor Schienenverkehr zeigt sich bezüglich verbindlicherer Vorgaben eine positive Entwicklung. Zudem wird durch das Einbinden der Branche zusätzlich die Akzeptanz erhöht (siehe Exkurs).

Positive Entwicklung im Teilsektor Schienenverkehr

Mit der Integration der IKT-Sicherheit in den Ausführungsbestimmungen der Eisenbahnverordnung (AB-EBV) wird über die Gesetzes- und Verordnungsstufe eine Verbindlichkeit dieser Vorgaben in der Branche erreicht.

Das Bundesamt für Verkehr (BAV) hat im Zusammenhang mit der Umsetzung der NCS das Kompetenzzentrum Cybersicherheit in der Sektion Sicherheitstechnik aufgebaut. Kernaufgaben sind im Wesentlichen normative Tätigkeiten und die präventive Aufsicht im Rahmen der Bewilligungs- und Zulassungsverfahren. Zudem führt das Kompetenzzentrum eine risikoorientierte Überwachung der Sicherheit bei den Bahnunternehmen durch. Durch die themenspezifische Wissenskonzentration wird zudem die Expertise gegenüber der Branche und damit die Akzeptanz der Aufsicht verbessert.

Der Verband öffentlicher Verkehr (VöV) ist der nationale Dachverband der Transportunternehmen des öffentlichen Verkehrs. Nebst vielem anderem übernimmt er die Koordination der Transportunternehmen bei nationalen Aufgaben. Zudem präzisiert und ergänzt der VöV zusammen mit der Branche in verschiedenen Arbeitsgruppen und Kommissionen auch die hoheitlichen Vorgaben. Das BAV ist oftmals auch aktiver Partner in Arbeitsgruppen des VöV. Damit kann eine hohe Akzeptanz der Vorgaben in der Eisenbahnbranche erreicht und die Motivation zur deren Umsetzung auf einem hohen Niveau gehalten werden.

Verbindliche Vorgaben auf Gesetzesstufe, unterstützende Branchenstandards und -handbücher sowie die Konzentration von Fachwissen in einem Kompetenzzentrum sind Erfolgsfaktoren, welche den SKI positiv beeinflussen. Durch die Zusammenarbeit von Aufsicht und Betreibenden der kritischen Infrastrukturen werden beide Seiten befähigt, den SKI aktiv voranzutreiben.

4.2 Der Informationsfluss ist bei Cybereignissen ein Schlüsselfaktor

Die IKT ist ein sich schnell entwickelnder Bereich. Der Einsatz neuer Technologien, die Digitalisierung und die konsequente Vernetzung der Systeme erfolgen mit hoher Geschwindigkeit. Damit einher geht auch die Herausforderung, neuartige Cyberattacken schnell zu erkennen. Nebst dem Erkennen von Angriffen sowie der Beseitigung der Schwachstellen, ist eine rasche Kommunikation gegenüber den zuständigen Behörden und weiteren Betreibenden von kritischen Infrastrukturen von grosser Bedeutung. Nur so kann sichergestellt werden, dass die richtigen Massnahmen möglichst flächendeckend und schnell umgesetzt werden können.

Das Parlament hat am 29. September 2023 eine Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (ISG) verabschiedet, mit welcher die Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eingeführt werden soll. Da dies eine Totalrevision des 5. Kapitels des ISG bedingt, erfolgt der Erlass der Ausführungsbestimmungen voraussichtlich in der ersten Hälfte des Jahres 2024. Die Vorlage schafft die gesetzlichen Grundlagen zur Meldepflicht für Betreibende von kritischen Infrastrukturen und definiert die Aufgaben des Bundesamtes für Cybersicherheit (BACS), das als zentrale Meldestelle für Cyberangriffe vorgesehen ist.

Auf Bundesebene hat sich gezeigt, dass der Informationsfluss bei Cyberereignissen sowohl hinsichtlich der Kommunikationswege wie auch der Geschwindigkeit Verbesserungspotenzial aufweist. Ohne funktionierende Kommunikation besteht die Gefahr, dass wichtige Informationen zur Lagebeurteilung sowie zur Steuerung der Korrektur- resp. Sicherheitsmassnahmen fehlen. Dadurch resultieren Fehlentscheide und/oder es geht wertvolle Zeit verloren. Diese fehlt dann, um mögliche weitere Angriffe bzw. Ausbreitungen zu verhindern. Die sektorspezifischen Aufsichtsbehörden sind mitverantwortlich, um operative Vorgaben für die Kommunikation im Fall von Cyberangriffen zu erlassen und deren Umsetzung von den Betreibenden der kritischen Infrastrukturen einzufordern.

4.3 Die Umsetzungskontrollen durch die Aufsicht weisen Verbesserungspotenzial auf

Die Aufsichtsbehörden und deren Kompetenzen werden in den sektorspezifischen Gesetzen und Verordnungen definiert. In der Regel werden diese Kompetenzen allgemein gehalten und es obliegt der zuständigen Behörde, ihre Aufsichtstätigkeiten risikoorientiert festzulegen.

Wie sich bei verschiedenen Prüfungen gezeigt hat, besteht Potenzial bei der Kontrolle und Aufsicht von Massnahmen zum SKI und zur Cybersicherheit. Auch wenn nicht in jedem Fall die Verbindlichkeit von SKI-Massnahmen gegenüber den Betreibenden von kritischen Infrastrukturen gegeben ist, sollte die jeweilige Aufsichtsbehörde die Umsetzung von Massnahmen präventiv kontrollieren. Damit besteht die Chance, die Betreibenden von kritischen Infrastrukturen für mehr Cybersicherheit zu sensibilisieren und zu motivieren und sich aktiv für den SKI einzusetzen.

ANHANG 1 – RECHTSGRUNDLAGEN

RECHTSTEXTE

Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020 (Stand am 1. April 2021), SR 120.73
Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 (Stand am 1. Januar 2024), SR 128
Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) vom 8. November 2023 (Stand am 1. Januar 2024), SR 128.1
Ausführungsbestimmungen zur Eisenbahnverordnung (AB-EBV) vom 1. November 2020, SR 742.141.11
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Si001 – IKT-Grundschutz in der Bundesverwaltung

STRATEGIEN

Nationale Strategie zum Schutz kritischer Infrastrukturen vom 16. Juni 2023
Nationale Cyberstrategie (NCS) vom April 2023

ANHANG 2 – ABKÜRZUNGEN

BABS	Bundesamt für Bevölkerungsschutz
BACS	Bundesamt für Cybersicherheit
BAV	Bundesamt für Verkehr
BCM	Business Continuity Management
BWL	Bundesamt für wirtschaftliche Landesversorgung
EFK	Eidgenössische Finanzkontrolle
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnologie
NCS	Nationale Cyberstrategie
OT	Operationstechnologie
SKI	Schutz kritische Infrastruktur
VöV	Verband öffentlicher Verkehr

ANHANG 3 – GLOSSAR

Firewall	Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
Firmware	Software, die in elektronischen Geräten eingebettet ist und dort grundlegende Funktionen leistet. Sie nimmt eine Zwischenstellung zwischen Hardware und der Anwendungssoftware ein.
Integrität	Der Begriff «Integrität» bedeutet, dass eine unerkannte Veränderung von Daten nicht möglich sein soll.
Intrusion Detection System	Ist ein System, das in der Lage ist, auf Computer, Server oder Netzwerke gerichtete Angriffe zu erkennen und darüber zu informieren.
Resilienz	Der SKI hat zum Ziel, die Resilienz (Widerstands-, Anpassungs- und Regenerationsfähigkeit) zu verbessern, damit gravierende Ausfälle möglichst verhindert oder im Ereignisfall die Auswirkungen reduziert werden können.

ANHANG 4 – AUSGEWÄHLTE PRÜFUNGEN

Nr.	Titel
23734	Bundesamt für Verkehr, BLS AG, Baselland Transport AG, Matterhorn-Gotthard-Bahn und Schweizerische Bundesbahnen AG – Prüfung des Schutzes kritischer Infrastrukturen – Fahrzeuge bei der Eisenbahn
23703	Nationales Zentrum für Cybersicherheit – Querschnittsprüfung der Erkennung von Sicherheitsvorfällen
22314	Bundesamt für Strassen – Prüfung des Schutzes kritischer Infrastrukturen – IT-Sicherheit der Verkehrsmanagementzentrale in Emmen
22116	Bundesamt für Bevölkerungsschutz – Prüfung des Schutzes kritischer Infrastrukturen – Governance und integrales Risikomanagement
21408	Skyguide – Prüfung des Schutzes kritischer Infrastrukturen – Umsetzung der Mindeststandards in der Flugsicherung
21306	Swissgrid – Prüfung des Schutzes kritischer Infrastrukturen – Umsetzung der Minimalstandards im Schweizer Höchstspannungsnetz
21070	Nationales Zentrum für Cybersicherheit – Prüfung der Wirksamkeit der Vorfallbewältigung beim Schutz der Bundes-IKT vor Cyberrisiken
20389	Bundesamt für Verkehr, Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn – Prüfung der IKT-Resilienz kritischer Infrastrukturen – Umsetzung des Minimalstandards bei Sicherungsanlagen der Eisenbahn
20013	Eidgenössische Finanzmarktaufsicht – Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern

ANHANG 5 – PRÜFUNGSABDECKUNG SEKTOREN / TEILSEKTOREN

Nachstehende Tabelle zeigt die Sektoren und Teilsektoren der kritischen Infrastrukturen sowie die mit den ausgewählten EFK-Prüfungen berührten Teilsektoren (mit X gekennzeichnet).

Nicht aufgeführt sind das BACS (vormals NCSC) wie auch das Staatssekretariat für Sicherheitspolitik (SEPOS), da diese im Zusammenhang mit dem SKI wichtige Querschnittsfunktionen über alle Sektoren erfüllen.

Das BACS ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der NCS.

Das SEPOS ist gemäss ISG verantwortlich für die Fachstellen Informationssicherheit, für die Personensicherheitsprüfungen und für die Betriebssicherheitsverfahren. Diese können für die kritischen Infrastrukturen der Bundesverwaltung beraten, Vorgaben erlassen und Überprüfungen durchführen.

Sektor	Teilsektor	Zuständige Bundesstelle (nicht abschliessend)	Ausgewählte EFK-Prüfungen								
			23734	23703	22116	22314	21408	21306	21070	20389	20013
Behörden	Forschung und Lehre	SBFI									
	Kulturgüter	BABS, BAK									
	Parlament, Regierung, Justiz, Verwaltung	PD, PK, EDA, Meteo Schweiz, fedpol, IOS, NDB, EFV, ISB und LE, BAFU		X					X		
Energie	Erdgasversorgung	BFE, ERI, BWL									
	Erdölversorgung	BFE, ERI, BWL									
	Stromversorgung	BFE, ELCOM, ESTI, ENSI, BWL						X			
	Fern- und Prozesswärme	BFE									
Entsorgung	Abfälle	BAFU									
	Abwasser	BAFU									
Finanzen	Finanzdienstleistungen	FINMA, EFV, SIF, BWL, BAKOM									X
	Versicherungsdienstleistungen	FINMA, EFV, SIF, BSV									
Gesundheit	Medizinische Versorgung	KSD, BAG									
	Labordienstleistungen	BAG, BLV, BABS									
	Chemie und Heilmittel	BWL, Swissmedic, Armeeapotheke			X						
Information und Kommunikation	IT-Dienstleistungen	BWL, ISB									
	Telekommunikation	BAKOM, BWL									
	Medien	BAKOM									
	Postdienste	BAKOM, BWL									
Nahrung	Lebensmittelversorgung	BWL, BLW									
	Wasserversorgung	BAFU, BWL									
Öffentliche Sicherheit	Armee	Gruppe Verteidigung		X							
	Baulichtorganisationen (Polizei, Feuerwehr, Sanität)	fedpol, BABS									
	Zivilschutz	BABS									
Verkehr	Luftverkehr	BAZL, BWL					X				
	Schienenverkehr	BAV, BWL	X							X	
	Schiffsverkehr	BAV, BWL									
	Strassenverkehr	ASTRA, BWL				X					

Tabelle 1: Von EFK-Prüfungen berührte Sektoren und Teilsektoren (Quelle: Auszugsweise – Nationale Strategie zum Schutz kritischer Infrastrukturen, Darstellung EFK)