EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der IKT-Resilienz kritischer Infrastrukturen – Umsetzung des Minimalstandards bei Sicherungsanlagen der Eisenbahn

Bundesamt für Verkehr, Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn

EFK-20389 | inkl. Stellungnahmen | 25. Februar 2021 | FinDel D2/2021

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.20389.802.00359
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung der IKT-Resilienz kritischer Infrastrukturen – Umsetzung des Minimalstandards bei Steuerungsanlagen der Eisenbahn

Bundesamt für Verkehr, Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn

Das Wesentliche in Kürze

Kritische Infrastrukturen (KI) stellen die Versorgung der Schweiz mit unverzichtbaren Gütern und Dienstleistungen sicher. Um diese KI zu schützen, muss eine möglichst permanente Funktionstüchtigkeit gewährleistet sein. In diesem Zusammenhang kommt der Resilienz der Informations- und Kommunikationstechnik (IKT) bzw. dem Schutz der kritischen Infrastrukturen (SKI) vor Cyberbedrohungen eine hohe Bedeutung zu. Der Bundesrat hat am 8. Dezember 2017 die nationale Strategie zum SKI (2018–2022) verabschiedet. Dazu gehört der Schienenverkehr. Der Bund gibt jährlich rund 4,5 Milliarden Franken für den Substanzerhalt und den Ausbau der Bahninfrastruktur aus.

Mittels einer Querschnittsprüfung hat die Eidgenössische Finanzkontrolle (EFK) bei vier Bahnunternehmen[1] die Einhaltung von Minimalanforderungen zum IKT-Schutz gegen Cyberangriffe geprüft. Dabei kam der vom Bundesamt für wirtschaftliche Landesversorgung (BWL) veröffentlichte «Minimalstandard zur Verbesserung der IKT-Resilienz» zum Einsatz. Dieser deckt im Wesentlichen die fünf Themenbereiche «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen» ab und bietet ein Bündel konkreter Massnahmen zur Umsetzung an. Das BWL empfiehlt den Betreibern von KI, den IKT-Minimalstandard umzusetzen.

Grosse Unterschiede beim Stand der Informationssicherheit

Im Hinblick auf die Maturität, welche das Schutzniveau beschreibt, hat die Prüfung ein heterogenes Bild ergeben: von «deutlich unter dem empfohlenen Minimalwert» bis «Minimalwert klar übertroffen». Bei der Umsetzung der Informationssicherheit gibt es bei allen Geprüften noch Handlungsbedarf.

Bereits im Bereich der Organisation der Informationssicherheit war festzustellen, dass bei drei der geprüften Bahnen die erforderlichen Rollen nicht oder nur ungenügend definiert sind. Auch die Wahrnehmung der IKT-Risiken ist bei den Mitarbeitenden sehr unterschiedlich.

Ein vollständiges Inventar der zu schützenden Informationen und Systeme stellt die wichtigste Grundlage zur Umsetzung der IKT-Sicherheit dar. Die Bahnunternehmen sind sich dessen bewusst und führen ein Inventar ihrer Werte. Teilweise sind diese noch in verschiedenen Datenquellen, ohne miteinander verknüpft zu sein. Diverse Projekte sollen diesen Zustand in Zukunft verbessern.

[1] Lausanne-Echallens-Bercher-Bahn, Freiburgische Verkehrsbetriebe, Zentralbahn und Rhätische Bahn

Das Zugriffmanagement muss bei drei Bahnen verbessert werden. Die Verwaltung der Benutzerkonten und die Vergabe der Rechte weisen in mancher Hinsicht erhebliche Mängel auf. Fernzugriffe durch Lieferanten müssen in der Kontrolle der Kunden sein und nachvollziehbar dokumentiert werden. Hier besteht für die betroffenen Bahnen ein umfangreicher Handlungsbedarf.

Der physischen und umgebungsbezogenen Sicherheit muss generell mehr Beachtung geschenkt werden. So ist in einem Fall der Zutritt zur Leitzentrale ungesichert, sodass die sich darin befindenden IKT-Systeme technisch nicht gegen unbefugte Zugriffe geschützt sind. Geräte für die Wartung des Rollmaterials sind teilweise unverschlossen zugänglich. Beim Brandschutz sind Massnahmen, die sich stark voneinander unterscheiden implementiert. Während verschiedene Stellwerke über keine Brand- oder Rauchmeldesysteme verfügen und die Löschmittel für eine allfällige Erstintervention fehlen, fand die EKF bei einer Bahn in den kritischen Anlagen redundante, automatische Löschsysteme vor.

Die Hälfte der geprüften Bahnen führt die Betriebszentralen mehrfach und an verschiedenen Standorten, wodurch der Betrieb bei einer Störung nicht beeinträchtigt werden sollte.

Das Testen von Notfallszenarien und Wiederherstellungsverfahren sollte als ständiger Prozess betrachtet werden. Damit kann sichergestellt werden, dass im Ereignisfall Systeme und Prozesse funktionieren. Um in diesem Bereich einen angemessenen Stand zu erreichen, muss bei vereinzelten Bahnen noch einiges aufgearbeitet werden.

Die Vorgaben zur Informationssicherheit: eine grosse Herausforderung für kleine Bahnbetriebe

Die Querschnittsprüfung hat gezeigt, dass grössere Bahnen hinsichtlich der IKT-Sicherheit besser aufgestellt sind als kleinere. Für kleine Betriebe stellt sie eine grosse finanzielle und personelle Herausforderung dar. Eine enge Zusammenarbeit mit grösseren Bahnen und der Bezug externer Dienstleistungen können aber eine positive Wirkung haben.

In diesem Jahr wurden die Ausführungsbestimmungen zur Eisenbahnverordnung durch das Bundesamt für Verkehr (BAV) überarbeitet und verabschiedet. Darin werden die Aspekte der Informationssicherheit erstmals explizit verankert. Mit dem Inkrafttreten der Vorgaben sind alle Bahnunternehmen ab dem 1. November 2020 verpflichtet, ein Informationssicherheitsmanagementsystem aufzubauen und zu betreiben. Das BAV spezifiziert allerdings weder die Mindestanforderungen noch die Frist zur Umsetzung. Indem es seine Erwartungen präzisiert und Arbeitsmittel zur Verfügung stellt, könnte das BAV den Bahnbetrieben eine wesentliche Unterstützung bieten.

Audit de la résilience informatique des infrastructures critiques – mise en œuvre des exigences minimales des installations de sécurité ferroviaire

Office fédéral des transports, Lausanne-Échallens-Bercher, Transports publics fribourgeois, Zentralbahn et Rhätische Bahn

L'essentiel en bref

Les infrastructures critiques (IC) garantissent l'approvisionnement de la Suisse en biens et services indispensables. Afin de protéger ces IC, il faut assurer leur fonctionnement si possible permanent. La résilience des technologies de l'information et de la communication (TIC), soit la protection des infrastructures critiques (PIC) face aux cybermenaces, revêt ici une grande importance. Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale PIC (2018–2022). Le trafic ferroviaire en fait partie. La Confédération consacre près de 4,5 milliards de francs par an à l'entretien de la substance de l'infrastructure ferroviaire et à l'extension du réseau.

Dans le cadre d'un audit transversal, le Contrôle fédéral des finances (CDF) a vérifié le respect des exigences minimales de protection des TIC face aux cyberattaques auprès de quatre compagnies ferroviaires[1]. La « norme minimale pour améliorer la résilience informatique », publiée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), a été utilisée à cet effet. Elle couvre en substance les cinq thèmes « identifier », « protéger », « détecter », « réagir » et « récupérer », et propose une série de mesures concrètes à mettre en œuvre. L'OFAE recommande aux exploitants d'IC de mettre en place cette norme minimale des TIC.

Grandes disparités en matière de sécurité de l'information

Selon l'audit, le niveau de protection en place est très hétérogène, son degré de maturité allant de « nettement en dessous de la valeur minimale recommandée » à « valeur minimale largement dépassée ». Toutes les compagnies auditées ont encore des efforts à réaliser dans la mise en œuvre de la sécurité de l'information.

D'un point de vue organisationnel, il est apparu que les rôles en matière de sécurité de l'information n'avaient pas ou pas suffisamment été définis dans trois des quatre compagnies auditées. De plus, leur personnel a une perception très différente des risques informatiques.

Un inventaire exhaustif des informations et systèmes à protéger est la base la plus importante pour la mise en œuvre de la sécurité des TIC. Les compagnies ferroviaires en sont conscientes et tiennent un inventaire de leurs valeurs. Ces dernières figurent en partie dans différentes sources de données sans être reliées entre elles. Divers projets doivent améliorer la situation à l'avenir.

[1] Compagnie du chemin de fer Lausanne-Échallens-Bercher, Transports publics fribourgeois, Zentralbahn et Rhätisch Bahn.

La gestion des accès doit être améliorée dans trois compagnies ferroviaires. Tant la gestion des comptes utilisateur que l'attribution des droits comportent à bien des égards de graves défauts. L'accès à distance par les fournisseurs doit être contrôlé par les clients et clairement documenté. Il y a là un grand besoin de prendre des mesures pour ces compagnies.

De façon générale, la sécurité tant physique que liée à l'environnement doivent faire l'objet d'une attention accrue. Dans un cas, l'accès à la centrale de régulation du trafic n'était pas sécurisé, de sorte que les systèmes TIC s'y trouvant n'étaient pas protégés contre des accès non autorisés. Les appareils servant à la maintenance du matériel roulant sont déverrouillés et accessibles dans certains cas. Quant à la protection anti-incendie, les mesures en place varient fortement d'un cas à l'autre. Alors que divers postes d'enclenchement sont dépourvus de tout système de détection de fumée et d'alarme en cas d'incendie ainsi que de matériel de première intervention (extincteurs), le CDF a repéré dans les équipements critiques d'une autre compagnie ferroviaire des dispositifs redondants d'extinction automatique.

La moitié des compagnies ferroviaires auditées gèrent des centrales de régulation du trafic redondantes situées à des endroits différents, de manière à ne pas perturber l'exploitation en cas de panne.

Tester des scénarios d'urgence et des procédures de restauration devrait être considéré comme un processus permanent. Il serait ainsi possible de s'assurer du fonctionnement des systèmes et processus en cas d'incident. Pour parvenir à un niveau adéquat dans ce domaine, il y a encore du travail à faire dans certaines compagnies.

Exigences de sécurité de l'information: un défi majeur pour les petites compagnies ferroviaires

L'audit transversal a montré que les grandes compagnies ferroviaires sont mieux parées en termes de sécurité des TIC que les petites. Ces dernières sont confrontées ici à un réel défi, en termes financiers et de personnel. Une étroite collaboration avec de grandes compagnies ferroviaires et le recours à des services externes peuvent toutefois avoir un effet positif.

Cette année, l'Office fédéral des transports (OFT) a révisé et adopté les dispositions d'exécution de l'ordonnance sur les chemins de fer. Pour la première fois, la question de la sécurité de l'information y est explicitement inscrite. Avec l'entrée en vigueur des nouvelles dispositions, toutes les entreprises ferroviaires sont tenues de mettre en place et d'exploiter un système de gestion de la sécurité de l'information depuis le 1er novembre 2020. Cependant, l'OFT ne précise ni les exigences minimales, ni le délai pour la mise en œuvre. En précisant ses attentes et en mettant à disposition des outils de travail, l'OFT pourrait apporter un soutien important aux entreprises ferroviaires.

Texte original en allemand

Verifica della resilienza delle TIC delle infrastrutture critiche – attuazione dello standard minimo per i sistemi di controllo ferroviario

Ufficio federale dei trasporti, ferrovia Lausanne-Echallens-Bercher, Trasporti pubblici friburghesi, Zentralbahn e Ferrovia retica

L'essenziale in breve

Le infrastrutture critiche (IC) garantiscono l'approvvigionamento della Svizzera in beni e servizi indispensabili. Al fine di proteggere queste IC occorre mantenere condizioni che garantiscano un funzionamento permanente. In questo contesto, la resilienza delle tecnologie dell'informazione e della comunicazione (TIC), ovvero la protezione delle infrastrutture critiche (PIC) contro le ciberminacce, riveste una grande importanza. L'8 dicembre 2017, il Consiglio federale ha varato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC) per il periodo 2018–2022, nella quale rientra il traffico ferroviario. La Confederazione spende circa 4,5 miliardi di franchi all'anno per il mantenimento della qualità delle infrastrutture ferroviarie e l'ampliamento della rete.

In occasione di una verifica trasversale presso quattro imprese ferroviarie[1], il Controllo federale delle finanze (CDF) ha esaminato se i requisiti minimi per la protezione delle TIC contro i ciberattacchi fossero osservati. A questo scopo è stato utilizzato lo «standard minimo per migliorare la resilienza delle TIC», concepito dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE). Questo standard ricopre sostanzialmente i cinque settori tematici seguenti: «identificare», «proteggere», «individuare», «reagire» e «ripristinare» e prevede una serie di misure concrete da attuare. L'UFAE raccomanda ai gestori di IC di applicare questo standard minimo per le TIC.

Grandi differenze in materia di sicurezza delle informazioni

Secondo la verifica, la protezione attuale dei dati è molto eterogenea: il suo livello è compreso tra «nettamente sotto il valore minimo raccomandato» e «valore minimo chiaramente superato». Per quanto concerne l'attuazione della sicurezza delle informazioni, sussiste necessità di intervento per tutte le imprese verificate.

Già nel settore dell'organizzazione della sicurezza delle informazioni, è risultato che per tre delle quattro imprese la definizione dei ruoli necessari è insufficiente o mancante. Anche la percezione dei rischi connessi alle TIC da parte dei collaboratori differisce molto.

Un inventario completo dei sistemi e delle informazioni da proteggere costituisce la base principale per attuare la sicurezza TIC. Le imprese ferroviarie ne sono coscienti e tengono un inventario dei propri valori. Questi valori si trovano in parte ancora in diverse fonti di dati senza essere collegati tra di loro. Diversi progetti si prefiggono di migliorare la situazione in futuro.

[1] Ferrovia Lausanne-Echallens-Bercher, Trasporti pubblici friburghesi, Zentralbahn e Ferrovia retica

La gestione degli accessi deve essere migliorata presso tre imprese ferroviarie. Riguardo ad alcuni aspetti, si riscontrano gravi lacune sia nella gestione dei conti utente che nell'assegnazione dei diritti di accesso. I clienti devono avere il controllo degli accessi remoti dei fornitori, che dovrebbero essere documentati in modo chiaro. Al riguardo sussiste una considerevole necessità di intervento per le imprese ferroviarie interessate.

In generale, occorre prestare maggiore attenzione alla sicurezza fisica e ambientale. In un caso, l'accesso alla centrale di gestione non è sicuro e quindi, dal punto di vista tecnico, i sistemi TIC al suo interno non sono protetti da accessi indebiti. I dispositivi per la manutenzione del materiale rotabile sono sbloccati e accessibili in alcuni casi. Per quanto concerne la protezione antincendio vengono attuate misure molto diverse tra loro. Mentre diverse cabine di manovra non dispongono di sistemi antincendio o di rilevamento del fumo e non hanno mezzi estinguenti per il primo intervento, il CDF ha constatato sistemi ridondanti di estinzione automatica negli impianti critici di un'impresa ferroviaria.

La metà delle imprese ferroviarie verificate gestisce diverse centrali operative in luoghi diversi, al fine di non compromettere l'esercizio dell'impianto in caso di guasto.

Sarebbe opportuno prevedere un processo continuo con l'obiettivo di testare scenari d'emergenza e procedure di ripristino. Ciò garantirebbe che, in caso di incidente, i sistemi e i processi continuino a funzionare. Rimane ancora molto da fare per alcune imprese ferroviarie prima di raggiungere un livello adeguato in questo settore.

Prescrizioni sulla sicurezza delle informazioni: una grande sfida per le piccole imprese ferroviarie

La verifica trasversale ha dimostrato che le imprese ferroviarie di maggiori dimensioni sono meglio organizzate in materia di sicurezza TIC rispetto a quelle piccole. A tale riguardo, le piccole imprese devono invece affrontare un'importante sfida in termini finanziari e di personale. Tuttavia, una stretta collaborazione con imprese ferroviarie più grandi e l'acquisto di servizi esterni possono sortire effetti positivi.

Nell'anno in oggetto, l'Ufficio federale dei trasporti (UFT) ha rivisto e adottato le disposizioni d'esecuzione dell'ordinanza sulle ferrovie. Per la prima volta, gli aspetti della sicurezza delle informazioni sono esplicitamente affrontati. Con l'entrata in vigore delle nuove disposizioni d'esecuzione, dal 1° novembre 2020 tutte le imprese ferroviarie sono tenute a sviluppare e attuare un sistema di gestione della sicurezza delle informazioni. Tuttavia, le disposizioni non specificano né i requisiti minimi né il termine da rispettare per l'attuazione. L'UFT sarebbe di grande aiuto alle imprese ferroviarie se precisasse le sue aspettative e mettesse a disposizione strumenti di lavoro adeguati.

Testo originale in tedesco

Audit of the ICT resilience of critical infrastructures – implementation of the minimum standard for railway control systems

Federal Office of Transport, Lausanne-Échallens-Bercher railway, Fribourg transport network, Zentralbahn and Rhaetian Railway

Key facts

Critical infrastructures (CIs) ensure the supply of indispensable goods and services in Switzerland. In order to protect these CIs, it is necessary to keep them functional at all times, insofar as possible. In this context, the resilience of information and communication technology (ICT) and critical infrastructure protection (CIP) against cyberthreats is of great importance. On 8 December 2017, the Federal Council adopted the national CIP strategy (2018–2022), which includes rail transport. The Confederation spends around CHF 4.5 billion annually on preserving value and expanding the railway infrastructure.

As part of a cross-sectional audit, the Swiss Federal Audit Office (SFAO) examined the compliance of four railway companies[1] with minimum requirements for ICT protection against cyberattacks. The minimum standard for improving ICT resilience, as published by the Federal Office for National Economic Supply (FONES), was used. This essentially covers the five topics of "identify", "protect", "detect", "respond" and "recover", and provides a set of concrete measures for implementation. The FONES recommends that CI operators implement the ICT minimum standard.

Major differences in information security

With regard to maturity, which describes the level of protection, the audit revealed a mixed picture, going from "significantly below the recommended minimum value" to "minimum value clearly exceeded". There is still a need for action in the implementation of information security at all audited organisations.

In terms of the organisation of information security, it was already apparent at three of the audited railway companies that the necessary roles were not defined or only insufficiently. The perception of ICT risks also varies greatly among employees.

A full inventory of the information and systems to be protected is the most important basis for implementing ICT security. The railway companies are aware of this and keep an inventory of their assets. In part, these are still in different data sources and are not linked to each other. Various projects should improve this situation in the future.

Access management needs to be improved at three companies. In some respects, there are considerable deficiencies concerning the administration of user accounts and the granting of rights. Clients must be able to control remote access by suppliers and this must be documented in a transparent manner. There is a need for extensive action here on the part of the railway companies concerned.

[1] Lausanne-Échallens-Bercher railway, Fribourg transport network, Zentralbahn and Rhaetian Railway

More attention must be paid to physical and environmental security in general. In one case, access to the control centre was unsecured, with the result that the ICT systems there were not technically protected against unauthorised access. Devices for the maintenance of rolling stock are unlocked and accessible in some cases. In terms of fire protection, widely differing measures have been implemented. While several signal boxes have no fire or smoke detection systems, and lack extinguishing resources for any initial response, the SFAO found redundant automatic extinguishing systems in the critical installations at one railway company.

Half of the railway companies audited have multiple control centres in different locations, which means that services should not be affected in the event of a fault.

The testing of emergency scenarios and recovery procedures should be considered an ongoing process. This ensures that systems and processes will work in the event of an incident. Some railways still need to catch up in order to achieve an adequate level of testing.

Information security requirements are a major challenge for small railway companies

The cross-sectional audit showed that larger companies are better positioned in terms of ICT security than smaller ones, for which it is a major challenge, both financially and in terms of personnel. However, close collaboration with larger railway companies and the procurement of external services can have a positive effect.

This year, the Federal Office of Transport (FOT) revised and adopted the implementing provisions for the Railways Ordinance. These explicitly enshrine information security aspects for the first time. With the entry into force of the regulations on 1 November 2020, all railway companies are obliged to set up and operate an information security management system. However, the FOT has not specified any minimum requirements or any deadline for implementation. By specifying its expectations and providing resources, the FOT could offer significant support to railway companies.

Original text in German

Generelle Stellungnahme der Lausanne-Echallens-Bercher-Bahn AG

Le Lausanne - Echallens - Bercher a confié la gestion opérationnelle de ses activités aux Transports publics de la région lausannoise (tl) sous la forme d'une convention de gestion. Cette organisation nécessite pour la compagnie LEB une meilleure définition des missions confiées à tl en matière de cybersécurité, mais elle permet à une "petite" compagnie de chemins de fer de bénéficier de ressources spécialisées. Le LEB et les tl ont pris conscience de l'importance de la cybersécurité, mais nous constatons que malgré les efforts consentis depuis quelques années dans ce domaine, il reste encore du travail pour atteindre le niveau minimal exigé. Les bases sont posées notamment dans les domaines Identify, Protect et Detect et de nombreux projets sont en cours dans ces domaines. Les recommandations faites suite à cet audit nous permettrons de prioriser nos actions notamment dans les domaines de Detect et Respond afin de répondre aux exigences miniales. Une collaboration avec d'autres compagnies de chemins de fer afin de partager les expériences dans ce domaine sera également recherchée.

Generelle Stellungnahme der Freiburgischen Verkehrsbetriebe AG

Les TPF ont conscience de l'importance que les cyberrisques représentent de nos jours, notamment dans le domaine des infrastructures critiques.

Ils remercient le CDF pour cet audit objectif qui s'est déroulé dans un cadre constructif. Les recommandations ont été reconnues comme des points d'amélioration positifs et permettront aux TPF d'aller plus loin dans le développement de la gestion et la surveillance dans ce domaine.

Les TPF saluent également la réalisation du "Manuel sur la cybersécurité destiné aux entreprises de transports public" sur mandat de l'Union des transports publics (UTP), qui permet d'avoir une base commune avec des recommandations sur la manière de réduire les cyberrisques pour toutes les entreprises de la branche.

Generelle Stellungnahme der zb Zentralbahn AG

Das erstmalige Audit der Zentralbahn durch die EFK hat uns verschiedene Aufpassfelder bei der IKT-Infrastruktur und Prozessen aufgezeigt. Die kritische Reflektion mit den Auditoren wird die IKT der Zentralbahn bezüglich der Security weiter verbessern. Dies unterstützt die Zentralbahn gegenüber Angriffen von aussen resilienter zu gestalten.

Generelle Stellungnahme der Rhätische Bahn AG

Die Rhätische Bahn dankt der EFK für ihre fundierte Prüfung und ihr stets kooperatives Vorgehen. Die Ergebnisse zeigen, dass sich die RhB mit ihrer IKT-Strategie auf dem richtigen Weg befindet. Sie zeigen aber auch, dass wir in unseren Bemühungen nicht nachlassen dürfen, damit im Zeitalter von Cyberbedrohungen die Infrastruktur der RhB zuverlässig zur Verfügung gestellt werden kann. Die RhB sieht die gefundenen Empfehlungen als Chance, um den Schutz der kritischen Infrastrukturen weiter zu optimieren. Die Ergebnisse und insbesondere die Empfehlungen werden gerne aufgenommen. Erste Schritte zur weiteren Verbesserung des Schutzes vor Cyberbedrohungen auch in neuen Medien und Kanälen wurden bereits eingeleitet.

Generelle Stellungnahme des Bundesamts für Verkehr

Die im EFK-Bericht aufgeworfenen Themen stehen seit längerem im Fokus des BAV.

Dem Schutz des Schienenverkehrs vor Cyberbedrohungen kommt mit der zunehmenden digitalen Vernetzung eine hohe Bedeutung zu. Dies sowohl beim BAV, wie auch bei anderen Aufsichtsbehörden im In- und Ausland. Das BAV ist in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) eingebunden.

Unsere Cybersicherheits-Aktivitäten werden in der Prävention (Sicherheitsvorschriften, Bewilligungen + Zulassungen) wie auch in der Überwachung (Audits und Betriebskontrollen) laufend intensiviert und vertieft. Die Hauptherausforderung besteht darin, die Lebensdauer der Systeme und die Erneuerungszyklen der Software in Einklang zu bringen.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Der Bahnverkehr ist ein Teil der kritischen Infrastruktur (KI) der Schweiz. Störungen im Schienenverkehr wirken sich auf nahezu alle Lebensbereiche aus. Betroffen ist insbesondere die Wirtschaft, aber auch die Bevölkerung wird durch länger anhaltende Störungen nachhaltig beeinträchtigt. Der Schienenverkehr ist stark von der Funktionsfähigkeit von technischen Infrastrukturdiensten, wie z. B. der Stromversorgung oder den Informations- und Kommunikationstechnologien (IKT), abhängig. Die Bahnunternehmen sind Partner im Rahmen des Sicherheitsverbunds Schweiz und in die Gesamtkoordination eingebunden. Die Verordnung über den Einsatz und die Aufgaben konzessionierter Transportunternehmen in besonderen und ausserordentlichen Lagen schreibt den Bahnunternehmen vor, welche Aufgaben sie in einem solchen Fall wahrzunehmen haben.

Mit dem Einsatz hochmoderner Steuerungs- und Überwachungssysteme, zum Beispiel dem European Train Control System (ETCS) und weiteren informatikgestützten (Sicherheits-)Systemen, entstehen unweigerlich auch neue Risiken.

Mittels einer Querschnittsprüfung kontrollierte die Eidgenössische Finanzkontrolle (EFK), ob die Sicherungsanlagen der Eisenbahninfrastruktur und der Zugleitsysteme den Mindestanforderungen zum IKT-Schutz gegen Cyberangriffe genügen. Die folgenden Bahnunternehmen wurden im Rahmen der Prüfung beurteilt:

- Lausanne-Echallens-Bercher-Bahn AG / Chemin de fer Lausanne-Echallens-Bercher SA (LEB)
- Freiburgische Verkehrsbetriebe AG / Transports publics fribourgeois SA (TPF)
- zb Zentralbahn AG (zb)
- Rhätische Bahn AG (RhB).

Mit der Neufassung der Ausführungsbestimmungen zur Eisenbahnverordnung (AB-EBV) hat das Bundesamt für Verkehr (BAV) erstmals die Anforderungen an die IKT-Sicherheit für Bahnbetreiber explizit verankert. Die EFK prüfte diesbezüglich, ob die Vorgaben die IKT-Sicherheit nachhaltig verbessern können.

1.2 Strategische Vorgaben

Nationale Strategie zum Schutz kritischer Infrastrukturen

Der Bundesrat (BR) hat am 8. Dezember 2017 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) für den Zeitraum 2018–2022 verabschiedet. In dieser sind 17 Massnahmen definiert, mit denen der BR die Versorgungssicherheit in der Schweiz erhalten und in wesentlichen Bereichen verbessern will. Unter anderen hat er den jeweils zuständigen Aufsichts- und Regulierungsbehörden den Auftrag erteilt, in allen Sektoren der KI zu prüfen, ob es erhebliche Risiken für gravierende Versorgungsstörungen gibt. Zudem sollen Massnahmen getroffen werden, um solche Risiken zu reduzieren.

Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

Zeitgleich mit der ersten SKI-Strategie von 2012 hat der BR auch die erste Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) verabschiedet. Die NCS zeigt auf, wie sich die Schweiz vor Cyberrisiken schützt und wie sich ihre Resilienz diesen gegenüber verbessert. Von 2012 bis 2017 wurden insgesamt 16 Massnahmen in den Bereichen Prävention, Reaktion und Kontinuität umgesetzt. Seit April 2018 gilt die neu erarbeitete NCS für die Jahre 2018–2022. Diese wurde in Zusammenarbeit mit allen Departementen, der Privatwirtschaft und den Kantonen entworfen. Der Schutz der KI vor Cyberrisiken ist ein wesentlicher Bestandteil der NCS. Sie deckt damit die Cyberaspekte der SKI-Strategie ab und setzt die entsprechenden Massnahmen in enger Koordination mit dieser um. Letztere baut auf den Arbeiten der ersten NCS auf, weitet diese wo nötig aus und ergänzt sie mit neuen Massnahmen, sodass sie der heutigen Bedrohungslage entspricht.

1.3 Prüfungsziel und -fragen

Mit der Prüfung soll den vier Bahnunternehmen aufgezeigt werden, wie sie hinsichtlich der Umsetzung der IKT-Sicherheitsanforderungen im Bereich der KI positioniert sind und wo es Verbesserungsbedarf gibt. Als übergeordnetes Prüfungsziel steht die Beurteilung, ob der Mindeststandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL) bezüglich IKT-Sicherheit bei den Bahnsicherungsanlagen eingehalten wird.

Die Prüffragen lauteten:

1. Werden bei den Bahnleitsystemen die IKT-Sicherheitsanforderungen des BWL eingehalten?
2. Werden die Schnittstellen zu anderen Infrastrukturbetreibern sicher und kontrolliert betrieben?
3. Genügen die (geplanten) Vorgaben des BAV, um die IKT-Sicherheitsstandards durchzusetzen?

Der Fokus zu diesen Fragen richtet sich hauptsächlich auf die für den Bahnbetrieb kritischen Netzwerke. Beim Zugsicherungssystem ETCS haben die geprüften Bahnen praktisch keine Handlungsmöglichkeiten. Einerseits bestehen für das ETCS internationale Vorgaben und andererseits sind in der Schweiz die Schweizerischen Bundesbahnen AG (SBB) in der Systemführerschaft. Für Meterspurbahnen ist ETCS nicht relevant. Sie setzen andere Systeme für die Zugbeeinflussung ein. Daher ist ETCS nicht im Fokus der Prüfung. Die Anschlussnetze für Büroanwendungen und bahnbetriebsnahe Systeme sind ausgeschlossen, sofern sie keine direkte und logische Verbindung zu den bahnbetriebskritischen Systemen haben.

1.4 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf die Netze und Infrastruktur für bahnbetriebskritische Anwendungen der vier Bahnunternehmen. Sie erfolgte anhand des Minimalstandards zur Verbesserung der IKT-Resilienz des BWL.

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 richtet sich vornehmlich an die Betreiber von KI, ist aber grundsätzlich für jedes Unternehmen anwendbar. Er kann als Nachschlagewerk dienen und vermittelt Hintergrundinformationen zur IKT-Sicherheit. Das Framework und das dazu gehörende Self-Assessment-Tool bietet den Anwendern, gegliedert nach den fünf Themenbereichen «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen», ein Bündel konkreter Massnahmen zur Umsetzung an.

Der IKT-Minimalstandard setzt dort an, wo sich die Gesellschaft Ausfälle am wenigsten leisten kann: bei den IKT-Systemen, welche für das Funktionieren der KI von Bedeutung sind. Betreibern von KI wird empfohlen, den vorliegenden IKT-Minimalstandard oder vergleichbare Vorgaben umzusetzen.

Der Standard kennt vier Stufen für die Bewertung der Maturität. Diese beschreiben das Schutzniveau, welches 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 Bedrohungsumgebung sowie rechtliche und regulatorische Anforderungen, Geschäftsziele und organisatorische Vorgaben genau kennen.

Für die Prüfung hat die EFK den über alle Branchen vorgeschlagenen Zielwert von 2.6 eingesetzt.

Weiter kamen die Empfehlungen der International Organization for Standardization (ISO/IEC) Standards 2700x zur Anwendung.

Die Prüfung wurde von Roland Gafner (Revisionsleiter) und Christian Brunner vom 10. August bis 25. September 2020 durchgeführt. Die Federführung lag bei Bernhard Hamberger. Das Revisionsteam wurde durch eine externe Firma unterstützt. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung ab Mitte Oktober 2020.

1.5 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den geprüften Bahnunternehmen und dem BAV umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.6 Schlussbesprechungen

Die Schlussbesprechungen fanden wie folgt statt:

RhB, 2. Dezember 2020: Teilgenommen haben vonseiten RhB, der Direktor, der Stellvertretende Direktor und Leiter Infrastruktur, der Leiter Elektrotechnische Anlagen, der Leiter

Smart Rail RhB, der IT-Security Verantwortliche, der Leiter Qualität/Prozesse, der Leiter Sicherheit/Risk und der externe Auditkoordinator. Seitens der EFK haben der zuständige Mandatsleiter, der zuständige Fachbereichsleiter und der Revisionsleiter teilgenommen.

LEB, 4. Décembre 2020 : Celui-ci était représenté par le Directeur adjoint et responsable d'unité Management du Réseau, le Responsable de l'unité LEB et membre de la direction et la Responsable des infrastructures LEB. Le CDF était représenté par le responsable des mandats, le cadre responsable et le responsable de révision.

TPF, 9. Décembre 2020 : Celui-ci était représenté par le Directeur général adjoint, Responsable du département Finances et Achats, le Secrétaire général, Transports publics fribourgeois Holding, le Responsable du département Informatique, Transports publics fribourgeois Holding, le Responsable du département Centre d'exploitation, Transports publics fribourgeois Infrastructure, le Responsable du département Gestion des installations, Transports publics fribourgeois Infrastructure, le Responsable du département Travaux, Transports publics fribourgeois Infrastructure et le Chef du service qualité, risques, sécurité et sûreté, Transports publics fribourgeois Holding. Le CDF était représenté par le responsable des mandats, le cadre responsable et le responsable de révision.

zb, 15. Dezember 2020: Teilgenommen haben vonseiten zb, der Geschäftsführer, der Leiter Infrastruktur, die Leiterin Finanzen und IT, der Leiter Informatik, der Verantwortliche Qualität, Sicherheit und Umwelt sowie der Leiter interne Revision der SBB Seitens der EFK haben der zuständige Mandatsleiter, der Federführende und der Revisionsleiter teilgenommen.

BAV, 3. Dezember 2020: Teilgenommen haben vonseiten BAV, der Sektionschef Sicherheitstechnik, der Fachspezialist Sicherungsanlagen und der Ingenieur Cyber-Sicherheit und Telematik. Seitens der EFK haben der zuständige Mandatsleiter, der Federführende und der Revisionsleiter teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Geschäftsleitungen (GL) bzw. den Verwaltungsräten (VR) der geprüften Unternehmen und für das BAV der Amtsleitung bzw. dem Generalsekretariat obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Compagnie du chemin de fer Lausanne-Échallens-Bercher SA

La compagnie du chemin de fer Lausanne-Échallens-Bercher (ci-après « le LEB ») exploite une ligne privée à voie étroite (écartement métrique des rails) dans le canton de Vaud. Longue de quelque 24 kilomètres, cette ligne part du centre de Lausanne, dessert les agglomérations situées au nord de la ville et va jusqu'à Échallens et Bercher, dans le Gros de Vaud. En 2019, le LEB a transporté environ 3,7 millions de passagers et a dégagé un revenu d'exploitation de près de 30 millions de francs.

Le LEB travaille en étroite collaboration avec les Transports publics lausannois (TL). Ainsi, le directeur du LEB est subordonné à celui des TL. Les services informatiques du LEB sont aussi fournis par les TL. Ensemble, les TL et le LEB comptent quelque 1600 collaborateurs, dont environ 100 travaillant exclusivement pour le LEB. En dépit de leur étroite collaboration, notamment dans le domaine de la sécurité, le LEB et les TL sont deux entreprises indépendantes. Cette structure complique cependant une séparation nette des deux organisations.

2.1 Évaluation de la maturité fondée sur le *framework*

En collaboration avec les TL, le LEB s'est concentré davantage sur la sécurité des installations ferroviaires, du matériel roulant et de la bureautique au cours de ces deux à trois dernières années. Cela a requis des analyses de fond et une multitude de projets, dont quelques-uns ont déjà été réalisés. Il s'agit de projets d'infrastructure qui ne font pas partie du présent audit, mais aussi de projets visant à améliorer le niveau de sécurité actuel de l'organisation. Malgré l'attention accrue et divers projets de sécurité, le niveau de sécurité actuel du LEB n'atteint pas encore le niveau recommandé par la norme informatique minimale (voir le graphique ci-dessous). Les responsabilités de base et une stratégie adéquate en matière de sécurité de l'information n'ont par exemple pas encore été définies ou n'ont pas encore été validées par la direction. D'une manière générale, le LEB n'atteint le niveau de sécurité minimal dans aucune des cinq fonctions prévues par la norme informatique minimale.

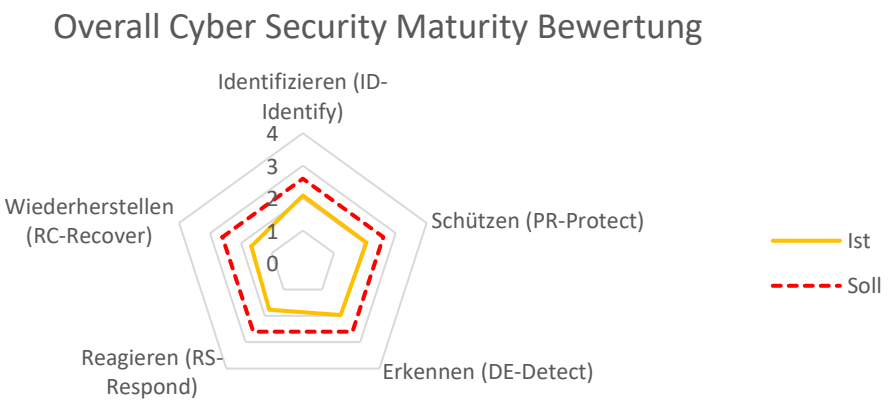


Illustration 1 : Evaluation de l'ensemble des domaines d'audit (voir l'annexe 4).

2.2 L'organisme responsable de la sécurité de l'information doit être renforcé

Au LEB, la cybersécurité a gagné en importance et a fait l'objet de davantage d'attention au cours de ces deux dernières années. Aux TL, un poste muni de responsabilités appropriées a été attribué à la cybersécurité, même si cela n'a pas été consigné. En revanche, le LEB n'a défini aucun rôle ni aucune responsabilité à cet égard. La collaboration et l'utilisation des synergies potentielles entre le LEB et les TL n'ont pas encore été clarifiées.

Le LEB n'a pas défini de processus de sécurité de l'information de bout en bout. Lors de l'audit, il n'avait qu'un processus ad hoc et peu formalisé. La direction et le conseil d'administration ne sont pas informés systématiquement de l'état de la cybersécurité. La définition systématique et stratégique des enjeux en matière de sécurité de l'information n'est que limitée.

Outre les lacunes du processus de sécurité de l'information, la définition formelle d'une stratégie, de directives, de plans et d'une documentation des processus est insuffisante. Certains processus du LEB sont éprouvés (par ex. commande manuelle d'un poste d'enclenchement, gestion du renouvellement du matériel roulant) et bien documentés. En revanche, en ce qui concerne la sécurité de l'information, il existe peu de processus et, par conséquent, peu de documents. Bien qu'une stratégie de sécurité de l'information soit en cours d'élaboration depuis 2017, elle n'a encore jamais été approuvée par la direction ou le conseil d'administration.

Appréciation

En principe, les rôles et les responsabilités en matière de sécurité de l'information de l'infrastructure critique doivent être définis et consignés tant dans le domaine informatique qu'au niveau des systèmes SCADA. Une définition claire de ces rôles et des responsabilités qui en découlent est requise afin que les travaux nécessaires puissent être exécutés à moyen et à long terme. De plus, le LEB et les TL doivent clarifier leurs responsabilités propres et déterminer leur collaboration en matière de sécurité de l'information.

Un système de gestion de la sécurité de l'information (SGSI) constitue un outil efficace pour garantir la sécurité de l'information dans l'ensemble de l'organisation et pour utiliser au mieux les synergies existantes (voir aussi le chapitre 6.1). En l'absence de SGSI, la sécurité de l'information ne repose sur aucun système ni sur aucune stratégie, et le LEB risque, dans l'état actuel, de faire du surplace.

Recommandation 1 (priorité 1)

Le CDF recommande au LEB de définir la gouvernance de la sécurité de l'information au moyen d'un SGSI, ainsi que les rôles les plus importants et les responsabilités qui en découlent. Il faut créer à cet effet les processus et les documents nécessaires.

Prise de position du LEB

Définition des processus tl, des rôles et des responsabilités suite à la réorganisation du service informatique. En cours de validation au sein des tl.

Evaluation des ressources et des compétences nécessaires (service informatique et système ferroviaire)

Formalisation du mandat LEB à tl dans le domaine de la cybersécurité

2.3 La sécurité physique et la sécurité liée à l'environnement présentent des défauts majeurs

Le bâtiment principal du LEB est protégé par une porte commandée au moyen d'un lecteur de cartes, par contre la centrale de régulation du trafic n'a pas de dispositif de verrouillage complémentaire. Ainsi, toute personne dans le bâtiment principal peut se rendre à la centrale. À l'origine, l'accès à cette dernière était fermé par une porte qui pouvait être ouverte uniquement à l'aide d'une clef et par les ayants droit. Or la serrure a été retirée.

Aucun dispositif n'empêche des tiers d'entrer dans l'atelier du matériel roulant pendant les heures d'exploitation. L'infrastructure pour les travaux de maintenance et les clés USB avec les versions logicielles pour le matériel roulant ne sont pas protégées dans ces locaux et peuvent donc être manipulées sans entrave par des tiers. Le nouveau plan de protection des contrôles d'accès prévoit d'améliorer l'accès physique à ces clés et à la centrale de régulation du trafic.

Certains postes d'enclenchement n'ont pas d'installation de détection d'incendie. En outre, il n'y a pas d'extincteurs ni d'autres moyens de lutte contre l'incendie.

L'absence de redondances et de solutions de repli peut causer des pannes assez longues

La centrale de régulation du trafic du LEB n'a pas un deuxième site pouvant servir de solution de repli en cas de panne de l'infrastructure. L'absence de redondances entraîne inévitablement l'arrêt de l'exploitation ferroviaire en cas d'incident. Dans un tel cas de figure, le transport des passagers pourrait être assuré par un service de bus. Quelques serveurs nécessaires à l'exploitation sont en libre accès et ils ne sont pas protégés dans la centrale de régulation du trafic. Des dégâts dus aux appareils de climatisation qui se trouvent au-dessus des serveurs ou à des actes involontaires du personnel d'exploitation constituent un risque supplémentaire.

Appréciation

La centrale de régulation du trafic est le noyau du LEB. Elle est nécessaire au bon fonctionnement du trafic ferroviaire au quotidien. Le fait qu'une personne non autorisée puisse y accéder constitue un risque élevé, qui doit être prévenu le mieux possible. L'accès à la zone de maintenance ne peut quasiment pas être empêché pendant les heures d'exploitation. Il est donc indispensable de protéger les outils critiques. En particulier, les clés USB contenant les logiciels pour le matériel roulant et les ordinateurs portables destinés à la maintenance doivent être protégés contre toute possibilité d'accès par des tiers. Le LEB traite cette question dans son nouveau plan de protection des contrôles d'accès. C'est pourquoi le CDF ne fait pas de recommandation à cet égard.

L'absence d'installations de détection d'incendie dans les postes d'enclenchement peut causer de sérieux dommages aux installations et des blessures aux collaborateurs. L'identification et la prévention des dommages dus au feu ont une importance majeure pour les installations électroniques.

Sans centrale de régulation performante, le trafic ferroviaire ne peut pas être assuré ou que de manière extrêmement limitée. Le niveau de sécurité de la centrale devrait être remanié en profondeur et les mesures appropriées devraient être mises en œuvre.

Recommandation 2 (priorité 2)

Le CDF recommande au LEB de planifier et d'installer rapidement des systèmes de détection d'incendie et des moyens de lutte contre les incendies dans tous les postes d'enclenchement.

Prise de position du LEB

Analyse des moyens nécessaires avec plan d'action à court et moyen terme

Financement des mesures à discuter avec l'OFT

Recommandation 3 (priorité 1)

Le CDF recommande au LEB d'identifier les systèmes critiques et, dans la mesure du possible, d'assurer leur fonctionnement par des moyens appropriés en cas d'incident.

Prise de position du LEB

Plan d'action pour redondance physique et géographique des équipements liés au centre de régulation LEB

2.4 La protection des accès et la gestion des mots de passe doivent être améliorées

Le personnel de la centrale de régulation du trafic n'utilise pas de comptes d'utilisateurs individuels pour accéder aux systèmes de commande. Le recours à des comptes collectifs empêche de suivre les actes de chacun ou ne permet qu'un suivi limité.

Les ordinateurs portables utilisés pour l'entretien du matériel roulant sont sécurisés au moyen d'un compte à privilèges élevés (compte d'administrateur). Ils servent à la maintenance du matériel roulant et ont par là même un accès direct à des composantes critiques. L'accès à ces appareils ne requiert aucun mot de passe. Ceux-ci ne sont donc protégés ni contre l'accès physique d'un tiers (voir le chapitre 2.3), ni par un mot de passe adéquat. Les ordinateurs portables ne sont connectés à aucun réseau, ce qui empêche tout accès externe. Toutefois, un accès physique ne peut être exclu.

Le LEB est fortement tributaire de la collaboration avec ses fournisseurs. Ceux-ci apportent des modifications aux systèmes en utilisant un accès à distance à l'infrastructure des systèmes de guidage et de contrôle. Toutefois, l'accès n'est pas possible en permanence, mais doit être validé à chaque fois. Il appartient aux fournisseurs de contrôler ce processus, qui peuvent s'octroyer eux-mêmes un accès sans que le LEB en ait connaissance. Le LEB n'est pas averti des accès au préalable et n'a pas la possibilité de vérifier les travaux effectués à l'heure actuelle. Les accès à distance se font au moyen de comptes de maintenance et ne sont pas personnels. Il n'y a donc aucune possibilité de suivi.

Appréciation

Les comptes collectifs utilisés pour l'accès et le contrôle du trafic ferroviaire ne sont appropriés ni sur le plan de la sécurité, ni, en particulier, sur le plan du suivi. L'accès aux applications critiques d'un point de vue ferroviaire doit être sécurisé au moyen d'un compte personnel. C'est la seule manière de pouvoir identifier les éventuelles erreurs de manipulation et les personnes qui en sont responsables.

Le fait que les appareils de maintenance ne soient connectés à aucun réseau permet d'empêcher tout accès indésirable de l'extérieur. Néanmoins, un accès physique aux appareils n'est pas exclu. C'est pourquoi ils doivent être protégés par un mot de passe individuel.

L'accès des fournisseurs à des fins de maintenance est inévitable dans ce contexte. Il est d'autant plus important que les solutions d'accès mises en place garantissent la sécurité et le suivi. Les accès et les travaux exécutés doivent être approuvés et contrôlés par le LEB. Les fournisseurs ne devraient obtenir l'accès qu'après indication du motif et avec l'accord du LEB. Il faut aussi s'assurer à cet égard que tous les collaborateurs des fournisseurs disposent de comptes d'utilisateurs individuels afin de garantir un suivi.

Recommandation 4 (priorité 1)

Le CDF recommande au LEB de créer et d'appliquer un plan de protection des accès et de gestion des mots de passe. Ce plan doit garantir que seuls des comptes personnels assortis de droits limités soient utilisés.

Prise de position du LEB

Projet de gestion des accès déployé au LEB en 2021

Directives pour utilisation des mots de passe individuels par les chefs de circulation

Inventaire des PC maintenance et gestion des accès (liste des ayants-droits et mots de passe)

Recommandation 5 (priorité 1)

Le CDF recommande au LEB d'élaborer et de mettre en place un processus qui permette de sécuriser et de suivre l'accès aux systèmes à distance.

Prise de position du LEB

Procédure de sécurisation de l'accès VPN pour les fournisseurs définie et appliquée. Ouverture sur demande par personne habilitée tl (6 personnes). Demande de fermeture nécessaire, si manque fermeture par service informatique.

2.5 L'absence de processus de rétablissement menace la poursuite de l'exploitation en cas d'incident

À l'heure actuelle, le LEB dispose de possibilités de réaction limitées face aux cyberrisques et n'a aucun processus de rétablissement. Bien qu'à l'étude, ces processus ne sont pas documentés. Il n'existe que peu de plans concernant la manière de réagir par exemple à une panne des systèmes critiques tels que le système de guidage, le système de contrôle ou le système d'information des clients et sur la façon de rétablir ces systèmes. En principe, cette situation touche la majorité des systèmes informatiques et systèmes SCADA critiques et moins critiques. Le LEB dispose d'un plan de continuité de sorte que, en cas de panne des systèmes critiques, le trafic ferroviaire peut être remplacé par des bus. La question du rétablissement des systèmes informatiques et des systèmes SCADA importants après un incident est peu traitée actuellement.

Appréciation

La poursuite de l'exploitation et le rétablissement des systèmes tombés en panne ou ciblés par des maliciels ne fonctionnent bien que si des mesures de réaction sont définies et testées à l'avance. Il est donc indispensable d'identifier les systèmes critiques et d'élaborer des scénarios de panne. Pour cela, il est nécessaire de documenter les plans de réaction et de rétablissement et de les tester en conséquence. Ces plans ont une importance particulière vu l'absence de redondances (voir le chapitre 2.3).

Recommandation 6 (priorité 1)

Le CDF recommande au LEB d'élaborer des plans de réaction et de récupération, de les tester régulièrement et de les améliorer lorsque cela est nécessaire.

Prise de position du LEB

Définition des plans de réaction et de récupération pour les installations de sécurité ferroviaires

Tests de récupération

3 Transports publics fribourgeois SA

Les Transports publics fribourgeois (TPF) exploitent le trafic de proximité par des trains, des bus et des lignes urbaines pour l'ensemble du canton de Fribourg. Le réseau ferroviaire comprend environ 100 kilomètres et se compose de voie à écartement normal et métrique. Les TPF ont transporté en 2019 environ 34 millions de passagers. En 2019, l'entreprise employait environ 1100 collaborateurs et a dégagé un revenu d'exploitation de 157 millions de francs. Le groupe TPF est organisé sous forme de holding. Il est chargé de la coordination des trois filiales[2], dont les tâches et le financement sont distincts.

Les TIC et les composants industriels pour les postes d'enclenchement et la technique de commande sont strictement séparés les uns des autres sur les plans logique et physique. Les systèmes sont développés, installés sur place et entretenus par les fournisseurs. Les TPF n'accèdent qu'aux applications de technique de commande. L'accès au réseau, aux serveurs, etc. des postes d'enclenchement et de la technique de commande est réservé aux fournisseurs. Ces derniers ont un accès permanent à distance. L'accès à distance est utilisé à des fins de surveillance et de maintenance des systèmes. Les changements qui sont requis pour des questions de sécurité sont réalisés sur place.

Le réseau de bureautique est surveillé en collaboration avec le Security Operations Center (SOC) d'un autre fournisseur externe.

3.1 Évaluation de la maturité fondée sur le *framework*

Dans l'ensemble, le niveau de maturité des TPF est solide. Dans trois des cinq fonctions prévues par la norme informatique minimale, les TPF atteignent le niveau de sécurité minimal recommandé par la Confédération et les associations professionnelles. Pour identifier les incidents, les TPF misent sur un SOC ainsi qu'une solution complète de surveillance du réseau et des composants. À l'heure actuelle, les TPF corrigent encore quelques points faibles afin de continuer à rehausser le niveau de maturité. Dans les domaines « Réagir » et « Récupérer », les TPF sont aussi préparés correctement. Ils disposent des capacités de réaction et de récupération appropriées. L'audit a identifié un besoin d'optimisation dans les fonctions de gouvernance en matière de sécurité de l'information et de gestion des risques.

[2] TPF Trafic, TPF Infra et TPF Immo.

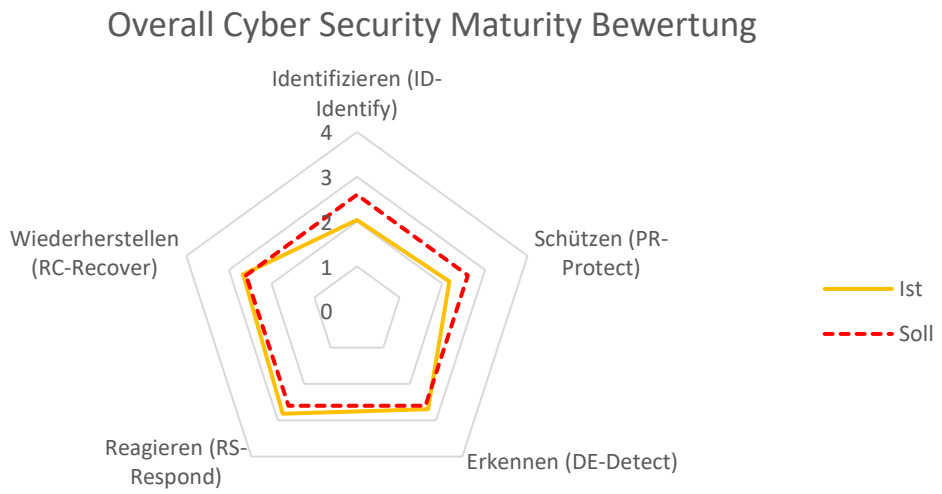


Illustration 2 : Evaluation de l'ensemble des domaines d'audit (voir annexe 5).

3.2 Les éléments importants de la gouvernance de sécurité sont en place, mais les rôles en matière de sécurité informatique doivent encore être définis

Les TPF n'ont pas défini de rôles et de responsabilités stratégiques pour la sécurité informatique de l'infrastructure critique au niveau de la direction ou dans le domaine technique. Les directives concrètes portant sur les objectifs, les tâches et les activités en matière de sécurité informatique ne sont que partiellement définies et documentées dans le domaine de l'infrastructure critique. Les TPF ne connaissent que très peu, voire pas du tout, les mécanismes précis relatifs à la sécurité informatique des postes d'enclenchement et de la technique de commande. La fonction de responsable de la sécurité de l'information n'a été créée qu'en 2019 à la suite d'une attaque par rançongiciel. Les TPF n'ont pas subi de dommages importants dans ce contexte et ont été en mesure de poursuivre l'exploitation informatique avec quelques restrictions. Les systèmes SCADA n'ont pas été touchés par le rançongiciel. Après cet incident, une formation à des fins de sensibilisation à la sécurité de l'information a été lancée. Elle est consacrée à un large éventail de thèmes relatifs à la sécurité. Au moment de l'audit, tous les collaborateurs qui travaillent avec un ordinateur avaient déjà suivi cette formation. En complément à la formation, les TPF réalisent aussi régulièrement des campagnes d'information sur l'hameçonnage. Le nombre des collaborateurs victimes d'un courriel d'hameçonnage s'est réduit au fil du temps.

Les TPF prévoient d'établir un SGSI et ont discuté des ressources. Ils comptent l'introduire à la fin de l'année 2021.

Les contrats de maintenance qui ont été conclus avec les fournisseurs des postes d'enclenchement et des techniques de commande ne contiennent pas des Service Level Agreements sur les cyberrisques. Étant donné qu'il n'existe pas de rôle responsable des systèmes SCADA dans le domaine de la sécurité de l'information des TPF, il manque des connaissances en ce qui concerne le plan de réaction des fournisseurs en cas d'incident. Ces processus des fournisseurs ne sont pas pris en considération et aucun plan de communication clair n'a été établi entre les TPF et les fournisseurs.

Appréciation

Les rôles et les responsabilités qui font défaut dans le domaine de la sécurité de l'information des systèmes SCADA sont à définir et à consigner tant sur le plan opérationnel que sur le plan stratégique. Seule une définition claire de ces rôles et des responsabilités qui en découlent permettra de garantir les aspects organisationnels de sécurité de l'infrastructure critique à moyen et à long termes.

Le CDF considère que les différentes mesures visant la sensibilisation des collaborateurs sont pertinentes. En effet, la sécurité peut être améliorée durablement grâce à une sensibilisation régulière à des thèmes concernant la sécurité dans le domaine de l'informatique de l'entreprise et les risques encourus pendant le travail quotidien.

L'absence d'échanges réguliers avec les fournisseurs sur la sécurité des systèmes SCADA empêche toute compréhension du dispositif de sécurité des systèmes. Ainsi, les éventuelles constatations ne peuvent guère être reprises dans le processus d'analyse de risques des TPF.

Recommandation 7 (priorité 2)

Le CDF recommande aux TPF de créer un rôle approprié pour la sécurité des systèmes SCADA dans leur organisation et de mettre à disposition les ressources y nécessaires.

Prise de position des TPF

Le département IT a mis en place une gestion contre les cyberrisques pour les systèmes informatiques qui sont sous sa responsabilité. Par contre, les systèmes SCADA qui sont gérés par des fournisseurs n'ont pas été intégrés dans cette gestion. Les TPF veulent dorénavant avoir une vision d'ensemble de la sécurité informatique et une gouvernance transverse. Ils vont pour cela attribuer les responsabilités internes au sein des différents départements et les ressources nécessaires pour y parvenir. Le département IT apportera son soutien et ses connaissances techniques.

3.3 Les cyberrisques doivent être davantage intégrés dans la gestion des risques de l'entreprise

Les processus de gestion des risques sont établis et gérés de manière active. La responsabilité de la réalisation d'une évaluation des risques au niveau de l'entreprise relève du conseil d'administration. Des analyses de risques sont effectuées chaque année dans tous les domaines. Les risques sont répertoriés et analysés en collaboration avec les responsables de département, les propriétaires des risques et chargé de gestion des risques. Ce faisant, ils sont répartis dans différents domaines (risques à l'échelon de l'entreprise, risques financiers, opérationnels ou basés sur des événements). Les risques identifiés et traités sont discutés au sein de la direction, puis du comité Audit et Risques. Ils font ensuite l'objet d'une présentation et d'un rapport destiné au conseil d'administration, qui évalue et approuve les risques. Depuis 2015, les TPF utilisent un outil de gestion des risques. Cet outil leur permet de saisir les risques et les mesures prises, et de surveiller la mise en œuvre de ces dernières.

L'analyse de risques des TPF tient compte des cyberrisques du département informatique, mais pas ceux de la sécurité des systèmes SCADA. Les postes d'enclenchement et la technique de commande sont entièrement gérés par des fournisseurs externes. Ainsi, les TPF partent du principe que les analyses de risques de ces systèmes sont réalisées par les fournisseurs.

Appréciation

Le CDF considère que la gestion des risques est établie et organisée de manière appropriée au sein des TPF.

Toutefois, les cyberrisques doivent aussi être recueillis et consignés systématiquement pour les systèmes SCADA. Cela permet de garantir que les points faibles et les risques potentiels pourront être identifiés de manière précoce.

Le fait que le matériel et les logiciels soient exploités par des partenaires externes n'exonère pas les TPF de leur responsabilité de traitement systématique des risques. Une gestion intégrale des risques devrait également prendre en compte la sécurité dans la chaîne d'approvisionnement et les risques qui y sont liés.

Recommandation 8 (priorité 1)

Le CDF recommande aux TPF de saisir les cyberrisques pour les systèmes SCADA de manière systématique et de les intégrer dans la gestion des risques de l'entreprise. Un échange d'informations entre les fournisseurs externes et les TPF doit être garanti à cet effet.

Prise de position des TPF

Les TPF ont introduit ce risque en octobre 2020 dans leur système de gestion des risques, qui a été validé par le Conseil d'administration.

La mise en œuvre est fortement liée à la recommandation 7, nous vous prions de vous référer à notre prise de position y relative.

3.4 Un inventaire complet constitue une base importante pour la sécurité informatique

L'infrastructure informatique pertinente pour l'exploitation ferroviaire est fournie intégralement par des partenaires externes. Ce sont eux qui dressent l'inventaire. À la fin des projets, les documents sont remis aux TPF, qui intègrent ensuite les informations dans leur gestion des inventaires. Les TPF gèrent deux banques de données d'inventaire. Les ressources provenant de projets (d'extension ou de rénovation) sont saisies dans une banque de données Microsoft Access, où un niveau de criticité leur est attribué. Pour chaque objet saisi, l'espérance de vie est définie.

Pour la deuxième banque de données, il s'agit d'un outil de gestion des équipements qui permet notamment de piloter la maintenance. Le cycle de maintenance y est défini. Les deux banques de données sont reliées, mais de manière non dynamique, car la mise à jour se fait manuellement. L'inventaire ne comprend que les composants matériels, les plateformes logicielles et les licences correspondantes n'étant pas gérées de façon centralisée.

Appréciation

Un inventaire complet constitue la base principale pour la mise en œuvre de la sécurité informatique. Comme l'utilisation de la banque de données Access se trouve en phase de démonstration de faisabilité *(proof of concept)*, l'exhaustivité et l'exactitude de l'inventaire ne sont pas encore garanties. Les processus d'établissement de l'inventaire et leur documentation sont en cours de développement. Pour un aperçu complet, il est indispensable de dresser l'inventaire des logiciels et des licences, en plus de celui des composants matériels.

Recommandation 9 (priorité 1)

Le CDF recommande aux TPF de créer un inventaire uniforme des composants matériels et des logiciels destinés à l'exploitation ferroviaire à l'échelle de toute l'entreprise, et de définir et d'appliquer des processus correspondants pour leur gestion.

Prise de position des TPF

Les TPF sont d'accord avec cette recommandation et mettent en œuvre les mesures correspondantes.

3.5 La gestion des accès doit être améliorée

En ce qui concerne la technique de commande, le centre d'exploitation dispose de deux systèmes de plusieurs fournisseurs pour les voies normales et métriques. Les systèmes et les réseaux des deux fournisseurs sont séparés physiquement.

Les opérateurs du trafic ferroviaire qui utilisent ces techniques de commande sont contrôlés par l'Office fédéral des transports (OFT). En outre, ils sont soumis à un contrôle de sécurité relatif aux personnes avant leur engagement. Une fois le contrôle réussi, ils reçoivent une autorisation pour utiliser les systèmes. En ce qui concerne le système de voie normale, chaque utilisateur bénéficie d'un compte personnel. Les informations d'enregistrement peuvent être modifiées. Pour le système de voie métrique, des comptes génériques sont utilisés pour la gestion des utilisateurs. Les fournisseurs installent les postes de travail et assurent la gestion des utilisateurs, à laquelle les TPF ne peuvent apporter aucun changement. Les mots de passe des postes de travail n'ont pas été modifiés depuis l'installation. Il est possible de modifier les comptes et les mots de passe, en faisant appel au fournisseur.

Les systèmes des deux fournisseurs disposent d'une fonctionnalité de journalisation, mais une panne de l'interface web lors de l'audit n'a pas permis d'accéder à la journalisation du système de surveillance de la voie métrique.

Appréciation

Une protection efficace des accès est assurée notamment par une définition adéquate des rôles et des droits d'utilisateur et par une directive appropriée régissant les mots de passe. Celle-ci devrait non seulement déterminer la complexité des mots de passe, mais aussi leur durée de vie. Dans le système de voie métrique, il faut garantir que les mots de passe soient changés au plus tard après le départ d'un opérateur du trafic ferroviaire ou son changement de fonction dans l'organisation.

Les comptes génériques d'utilisateurs rendent impossible toute traçabilité des actions réalisées, ils ne doivent donc pas être utilisés. Suite à une panne de l'interface web lors de l'audit, il n'a pas été possible d'accéder à la journalisation du système de surveillance de la voie métrique et de vérifier son bon fonctionnement.

Recommandation 10 (priorité 1)

Le CDF recommande aux TPF de travailler exclusivement avec des comptes personnels sur les systèmes de la centrale d'exploitation et d'enregistrer leurs activités. En outre, un processus doit garantir l'application des exigences liées aux mots de passe.

Prise de position des TPF

Les TPF sont d'accord avec cette recommandation et mettent en œuvre les mesures correctives.

3.6 La disponibilité et la redondance en voie d'amélioration

Les systèmes de technique de commande sont équipés de stations de travail redondantes. Grâce à cette redondance, il est possible, en cas d'incident, de gérer le trafic de manière décentralisée depuis certaines gares. Au moment de l'audit, les TPF rénovaient plusieurs gares et des tronçons du réseau ferré. Lors de ces rénovations, les TPF ont reconnu l'importance de la redondance des systèmes et l'intègrent dans la planification architectonique. Ainsi, les TPF examinent s'ils peuvent garantir à l'avenir la disponibilité des postes d'enclenchement et de la technique de commande par une topologie de réseau en anneau. Par conséquent, à l'avenir, une panne des postes d'enclenchement ne devrait pas avoir d'incidence sur l'ensemble de l'exploitation du réseau ferroviaire. De plus, les TPF se sont fixés comme objectif de réaliser un second site pour les serveurs de la technique de commande, ce qui assurera une géoredondance.

Appréciation

Les TPF sont en train d'examiner s'ils peuvent garantir la disponibilité des postes d'enclenchement et de la technique de commande au moyen d'une topologie de réseau en anneau. Ainsi, au moment de l'audit, il ne manque qu'une géoredondance de l'infrastructure des serveurs. Pour assurer le bon fonctionnement de l'exploitation en cas d'incident majeur (par exemple inondation, incendie, etc.), il est indispensable de mettre en place une infrastructure critique des serveurs sous une forme géoredondante.

Le Contrôle fédéral des finances (CDF) note qu'un projet de géoredondance a été initialisé et s'abstient de faire une recommandation.

3.7 La sécurité des ordinateurs portables de maintenance doit être améliorée

Les collaborateurs disposent de deux ordinateurs portables pour assurer la maintenance des systèmes dans les trains. Ces ordinateurs portables n'ont pas de correctifs, avec un ancien système d'exploitation (Windows XP) sans protection contre les maliciels. L'assistance de Windows XP a été arrêtée par Microsoft, raison pour laquelle il n'existe plus aucune mise à jour de sécurité. L'utilisation de Windows XP constitue donc un risque considérable en termes de sécurité. Les deux ordinateurs portables disposent d'un accès à Internet et d'une application de maintenance à distance qui permet d'établir d'éventuelles connexions avec le fournisseur. L'accès aux deux ordinateurs portables se fait par un utilisateur local générique. Ainsi, une gestion ciblée des utilisateurs est impossible et les TPF ne peuvent pas savoir qui a utilisé ces ordinateurs portables.

L'utilisation des appareils se limite à la lecture de données et à l'installation de nouvelles versions des logiciels (nouvelles fonctions, améliorations ou traitement des erreurs) pour le matériel roulant. Les configurations des systèmes de sécurité dans les trains ne peuvent être effectuées que par les fournisseurs. Les activités susmentionnées ne peuvent être réalisées que dans le train. Pour ce faire, un ordinateur portable est raccordé physiquement

par un câble aux systèmes. Aucun accès à distance n'est possible pour les systèmes de sécurité des trains.

Appréciation

En tant qu'interface avec le matériel roulant, les appareils de maintenance constituent un vecteur potentiel d'attaque. Des appareils compromis pourraient amener des logiciels malveillants dans les trains.

Les systèmes d'exploitation qui ne sont plus pris en charge par les fournisseurs présentent des risques élevés en termes de sécurité. Ce genre de systèmes doit être remplacé par des nouveaux systèmes bénéficiant d'une assistance garantie à long terme du fournisseur. Le fait que ces appareils soient connectés à Internet accroît considérablement le risque d'un piratage. Une protection appropriée contre les maliciels doit être installée sur tous les systèmes.

Recommandation 11 (priorité 1)

Le CDF recommande aux TPF de renouveler les appareils de maintenance, de les équiper d'une protection appropriée contre les maliciels et de ne permettre des accès qu'avec des comptes personnels.

Prise de position des TPF

Les TPF sont d'accord avec cette recommandation et mettent en œuvre les mesures correctives.

4 Die zb Zentralbahn AG

Die zb ist eine Eisenbahngesellschaft, die 2005 aus der Integration der Brünigbahn in die Gesellschaft Luzern-Stans-Engelberg-Bahn entstanden ist. Sie betreibt die meterspurige Strecke Luzern-Interlaken Ost und Luzern- Engelberg. Die zb ist eine eigenständige Tochtergesellschaft der SBB (66,0 %), des Bundes (16,1 %), der Kantone Nidwalden (11,8 %) und Obwalden (5,0 %), der Gemeinde Engelberg (1,0 %) sowie Privataktionären (0,1 %).

Auf dem rund 100 Kilometer langen Streckennetz beförderte die zb im letzten Jahr 10,1 Millionen Fahrgäste. Mit ihren 380 Mitarbeitenden erwirtschaftete die zb im Jahr 2019 einen Betriebsertrag von ca. 130 Millionen Franken.

Die Informatik ist in zwei Bereiche aufgeteilt. Die Büroautomation und die für den Bahnbetrieb relevanten Systeme sind logisch getrennt, laufen aber über dasselbe Glasfasernetz. Dieses Netz wird von der SBB betrieben und ist redundant aufgebaut. Die Leittechnik wird durch einen externen Partner installiert und ebenfalls durch die SBB betrieben. Für die Büroautomation sind drei Mitarbeitende der zb verantwortlich. Die benötigten Services werden von externen Partnern bezogen und mittels verschiedener Werkzeuge überwacht.

4.1 Einschätzung der Maturität aus dem Framework

Die zb ist im Bereich des Betriebs der KI grundsätzlich gut aufgestellt. Sie hat dennoch Handlungsbedarf erkannt. Zum Beispiel den Aufbau eines Asset-Managements oder das Erstellen von Business-Continuity–Plänen (BCP). Weiterer Handlungsbedarf liegt vor allem in den Bereichen Wiederherstellen, bei den Rollen und Verantwortlichkeiten sowie in der Optimierung der physischen Sicherheit der Stellwerke.

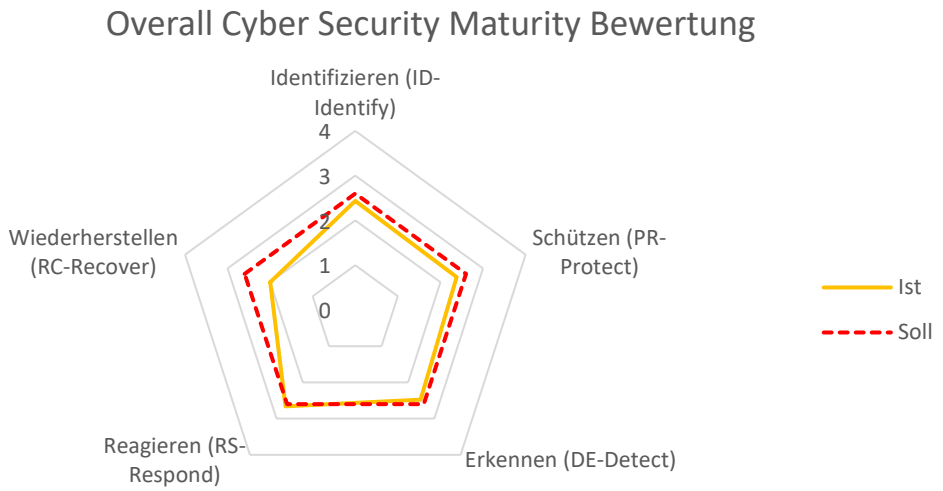


Abbildung 3: Assessment-Auswertung über alle Prüfbereiche (Details siehe Anhang 6)

4.2 Rollen im Bereich der IKT-Sicherheit sind nicht formalisiert

Für die Rolle des «Verantwortlichen Informationssicherheit» ist keine Stellenbeschreibung vorhanden. Nur für die des Sicherheitsbeauftragten (Safety) und die Risikomanagerin ist dies der Fall. Die Rolle des «Verantwortlichen Informationssicherheit» wird zum Prüfzeitpunk vom Leiter IKT ausgeübt. Er hat dieses Thema in der GL vorgebracht und in der Folge den Auftrag erhalten, diese Funktion auszuüben. Um die Rolle des «Verantwortlichen Informationssicherheit» zu etablieren, müsste zuerst eine Security Governance erstellt werden, welche die Rollen und deren Verantwortung festhält. Im Moment definiert die zb Cybersecurity und Security als zwei Themen. In den Bereich Cybersecurity fällt alles ausserhalb des Perimeters der zb. Security beginnt folglich nach der Firewall, also im internen Netz. Die KI befindet sich gemäss Definition folglich nicht im Cyberbereich.

Beurteilung

Die Fertigstellung der Security Governance sollte forciert werden. Danach muss die Rolle des «Verantwortlichen Informationssicherheit» definiert und etabliert werden. Weiter ist sicherzustellen, dass diese auch die IKT-Sicherheit bei den SCADA-Systemen überprüft.

Empfehlung 12 (Priorität 1)

Die EFK empfiehlt der zb, eine Security Governance inkl. Beschreibung der nötigen Rollen zu forcieren. Diese sind zu institutionalisieren und die entsprechenden Ressourcen müssen zur Verfügung stehen.

Stellungnahme der zb

Die Sicherheitsorganisation ist im Prozess der Zentralbahn 1.50 (Sicherheit) festgelegt (gültig seit 04.09.17) und wird aktuell nach einem Hinweis durch das BAV vom 26.11.2020 komplett überarbeitet. Darin ist die Zuständigkeit für die Sicherheit von IT / Daten bei der zb dem Leiter IT zugeordnet. Für die Umsetzung hat die zb eine ICT-Security Governance verabschiedet und per 5. Februar 2021 für gültig erklärt. Darin werden die ICT-Security Rollen beschrieben. Die Ressourcen stehen zur Verfügung.

4.3 Ein zentrales und automatisiertes Asset-Management ist im Aufbau

Das Asset-Inventar wird derzeit in einem Enterprise-Resource-Planning-System geführt. Die periodischen Auszüge dienen als Grundlage für die Wartung der Systeme. Wenn Komponenten ersetzt oder erweitert werden, erfolgt eine manuelle Erfassung im System. Ein automatisierter Prozess für die Inventarisierung besteht im Moment nicht. Zudem ist der Prozess für die Inventarisierung nicht im zentralen Prozessmanagement abgebildet. Künftig soll ein Werkzeug zum Einsatz kommen, um die Inventarisierung und Wartung zu automatisieren. Ein Projekt für die Einführung des Anlagemanagements ist am Laufen. Mit diesem kann eine Optimierung der Infrastruktur, der Qualität und der Kosten erreicht werden. Auch die Sicherheit soll damit verbessert werden, dies durch bessere Kenntnisse über den Zustand der Anlagen und durch eine Reduktion der Risiken. Je nach gewählter Variante soll das Projekt noch in diesem Jahr oder im Juli 2021 abgeschlossen werden.

Beurteilung

Ein vollständiges Inventar stellt die wichtigste Grundlage für die Umsetzung der IKT-Sicherheit dar. Mit der Einführung des zentralisierten Asset-Managements können die Systeme entsprechend ihres Schutzbedarfs erfasst werden. Zudem können die Risiken und Wartungsintervalle hinterlegt werden. Da die zb den Handlungsbedarf erkannt hat und das Projekt bereits in der Einführungsphase ist, verzichtet die EFK auf eine Empfehlung.

4.4 Ein mangelhaftes User Access Management kann zu unberechtigten Zugriffen führen

Die Zugriffvergabe auf das Integrale Leit- und Informationssystem[3] erfolgt durch den Leiter «Elektrotechnische Anlagen». Ein Prozess für die Vergabe der Rechte liegt vor, wobei es bei der zb eigentlich nur zwei Administratoren und rund 25 Benutzer gibt. Hinzu kommen noch Benutzer der SBB und des Lieferanten. Die Benutzer und ihre Berechtigungen werden in einer Tabelle geführt. Ein eigentliches Rollenkonzept ist nicht vorhanden. Mutationen der Benutzer finden in der Regel nicht sofort statt, insbesondere Austritte werden erst dann mutiert, wenn der nächste Neueintritt erfasst wird.

Des Weiteren wurde festgestellt, dass die Passwörter für die Zugänge auf die Informationssysteme der Züge unverschlüsselt auf dem SharePoint abgelegt sind.

Beurteilung

Die Vergabe von Rechten sollte durch einen Personalprozess (z. B. Ein-/Austritt) angestossen werden. Die Rechte sollten gemäss einer entsprechend definierten Rolle vergeben werden. Damit kann sichergestellt werden, dass auch bei internen Übertritten die Rechte angepasst werden und keine unberechtigten Zugriffe bestehen bleiben.

Die unverschlüsselte Ablage von Passwortlisten stellt ein Risiko dar. Mit dem Einsatz eines Passwortmanagementsystems kann diesem Umstand entgegengewirkt werden. Zudem kann die Umsetzung der Vorgaben automatisiert sichergestellt und überprüft werden.

Empfehlung 13 (Priorität 1)

Die EFK empfiehlt der zb, die Implementierung eines unternehmensweiten und zweckmässigen User Access Managements für alle Zugriffe inkl. Protokollierung der Handlungen umzusetzen. Dabei müssen auch die Aspekte des Passwortmanagements berücksichtigt werden.

Stellungnahme der zb

Da aus Sicherheitsgründen die kritischen Infrastrukturen nicht mit anderen Systemen vernetzt sind, kann ein User Access Management nur organisatorisch und nicht systemgestützt erfolgen. Die zb ist sich der Wichtigkeit bewusst und überprüft die Prozesse «Ein-/Austritt» sowie «Funktionswechsel» und nimmt wo nötig Anpassungen vor.

Die Rollen I-EA (Zugriff Stellwerk-Leitsystem und ILTIS) haben wir inzwischen definiert und müssen jetzt noch den Personen/Funktionen zu geordnet werden - Durch die Rollenverteilung, ergibt sich der Zugriff mit den unterschiedlichsten Bedien- oder Funktionsmöglichkeiten.

[3] ILTIS: ein durch Siemens Schweiz entwickeltes Leit- und Informationssystem zur automatisierten Betriebsabwicklung einer Bahnlinie

4.5 Nicht getestete Wiederherstellungsverfahren können im Störungsfall zu Datenverlust führen

Im Konzept zu Backup und Restore der Kommunikationsinfrastruktur sind die gerätespezifischen Anforderungen beschrieben. Die Datensicherung erfolgt regelmässig. Tests zur Datenwiederherstellung werden nur bei der Inbetriebnahme und später nicht mehr systematisch durchgeführt. Wenn die Wiederherstellung erforderlich wird und funktioniert, werden später keine weiteren Tests gemacht.

Bei den Sicherungsanlagen werden keine Restore-Tests gemacht. Solange die Software zur Verfügung steht, kann sie bei einer Störung auf ein neues System aufgespielt werden. Danach sollen alle gewünschten Funktionen wieder verfügbar sein.

Beurteilung

Die zb ist sich der Wichtigkeit von Backups bewusst und hat solche konzeptionell auch angemessen umgesetzt. Allerdings wird die Wiederherstellung der Kommunikationsinfrastruktur aus dem Backup nicht systematisch und regelmässig geprobt. Nur mittels regelmässiger Tests der Datenwiederherstellung kann sichergestellt werden, dass im Störfall auf erprobte Prozesse zurückgegriffen werden kann und diese auch funktionieren.

Empfehlung 14 (Priorität 2)

Die EFK empfiehlt der zb, Tests im Rahmen der Wiederherstellungsverfahren zum Netzwerkmanagement zu planen und regelmässig durchzuführen.

Stellungnahme der zb

Das zb IT Netzwerk ist nicht redundant ausgelegt. Deswegen kann die Wiederherstellung aus dem Backup nicht ohne Betriebsunterbruch durchgeführt werden. Um systematische und regelmässige Tests der Datenwiederherstellung bei der Kommunikationsinfrastruktur durchführen zu können, muss die Netzwerkinfrastruktur entsprechend ausgebaut werden. Die zb ermittelt Lösungsvarianten um die Anforderungen zu erfüllen.

4.6 Die physische Sicherheit der Stellwerke muss verbessert werden

Mindestens ein Stellwerk verfügt über keine Brand- bzw. Rauchmeldeanlage, Löschmittel sind auch nicht vorhanden. Da das Stellwerk in einem separaten Bau ausserhalb des Betriebsgebäudes ist, könnte ein allfälliger Brand erst zu einem späten Zeitpunkt erkannt werden.

Die Klimaanlage und die Temperatursensoren in den Serverschränken werden hingegen überwacht und allfällige Alarme werden an die Betriebszentrale übermittelt.

Beurteilung

Da ein Ausfall des Stellwerks einen Unterbruch des Bahnverkehrs zur Folge haben kann, ist es nicht nachvollziehbar, weshalb keine Brand- bzw. Rauchmeldeanlage installiert ist. Fehlende Brandmeldesysteme in Stellwerken können sowohl zu unerkannten und damit grösseren Schäden an Anlagen, aber auch zu Verletzungen von Mitarbeitenden führen. Das Erkennen und Verhindern von Schäden durch Feuer sind in elektronischen Anlagen von grosser Bedeutung.

Empfehlung 15 (Priorität 2)

Die EFK empfiehlt der zb, in allen Stellwerken, zusätzlich zu der bestehenden Überwachung, Brand- bzw. Rauchmeldesysteme und Brandbekämpfungsmittel zu planen und zeitnah zu installieren.

Stellungnahme der zb

Die Zentralbahn wird intern eine Risikobeurteilung für die Stellwerksräume durchführen und daraus erforderliche Massnahmen ableiten und umsetzen.

4.7 Das operative Kontinuitäts- und das Krisenmanagement sind nur teilweise auf Durchführbarkeit überprüft

Ein Konzept für das Krisen- und das betriebliche Kontinuitätsmanagement ist vorhanden. Auf einer Webplattform sind Dokumente und Informationen verlinkt und verfügbar. Eine ausgedruckte Version der Dokumente und Checklisten ist nicht vorhanden. Die Mitglieder der Krisenorganisation können die Dokumente online abrufen oder auch herunterladen. Damit immer die aktuelle Version vorhanden ist, müssten die entsprechenden Daten jedoch mittels Offlinedateiensynchronisation auf dem Arbeitsgerät gespeichert sein. Die wichtigsten Punkte sollen künftig auf einem Faltblatt zusammengefasst werden.

Die Schnittstellen zu internen Funktionen und externen Organen sind festgelegt. Die zb verfügt jedoch über keine Business-Impact-Analyse (BIA) und damit über keine Dokumentation wie die Überlegungen in die bestehenden BCP (Business Continuity Strategie und Plan) eingeflossen sind. Es wurden bereits diverse Szenarien definiert und Massnahmen zur Krisenbewältigung erarbeitet, diese wurden aber nicht auf ihre Durchführbarkeit überprüft. Ausserdem wurde nicht definiert, welche Systeme als Erstes wieder funktionieren müssen. Die zb verfügt über einen Ausweichstandort bei der SBB in Luzern. Bisher wurden keine Tests der dortigen Infrastruktur durchgeführt. Zum Prüfungszeitpunkt wurde ein externer Partner beauftragt, eine Offerte für die Erarbeitung der BCP zu erstellen. Sie liegt der EFK noch nicht vor.

Eine Absprache oder Übungen mit der SBB als Leistungserbringer finden nur im Rahmen von übergeordneten Prüfungen, wie zum Beispiel der Sicherheitsverbundsübung (SVU19) statt. Die Krisenkommunikation ist definiert und die Zusammenarbeit mit weiteren Stellen (z. B. Blaulichtorganisationen oder Medien) ist etabliert.

Beurteilung

Für das Krisenmanagement sind ein Portal sowie diverse Hilfsmittel und Checklisten auf einer Online-Plattform vorhanden. Das Problem dabei ist, dass die Mitglieder des Krisenstabs sicherstellen müssen, dass sie die Offlinesynchronisation auch aktiviert haben. Bei einem Stromausfall oder Verbindungsproblemen sind das Portal und somit die Unterlagen nicht verfügbar. Die Mitglieder des Krisenstabs müssen entsprechend geschult und sensibilisiert werden.

Es ist unerlässlich, BCP zu erstellen. Die entsprechenden Szenarien müssen definiert und die erarbeitete Problemlösung auf ihre Umsetzbarkeit überprüft werden. Mittels regelmässiger Übungen kann die Wirksamkeit festgestellt und allfällige Verbesserungen umgesetzt werden. Dabei sollte auch die SBB involviert werden. Da die Zusammenarbeit der beiden Bahnen sehr eng ist, könnten Synergien genutzt werden.

Die Verfügbarkeit eines Ausweichstandortes ist wichtig. Dieser sollte jedoch periodisch in Betrieb genommen werden, um zu gewährleisten, dass bei einem Notfall alle Systeme einsatzfähig sind.

Empfehlung 16 (Priorität 1)

Die EFK empfiehlt der zb, das operative Kontinuitätsmanagement zu schärfen und mittels einer BIA die Prozesse und Funktionen innerhalb der Organisation zu identifizieren und zu bewerten.

Stellungnahme der zb

Die zb wendet die Konzernrichtlinie der SBB K 015.3 - «BCM Policy SBB» an, welche den verbindlichen Rahmen zur Ausrichtung ihres geschäftsspezifischen BCM darstellt. Die Policy ist für den Konzern bindend und gemäss den Bestimmungen der K 562.1 «Weisung Beteiligungsmanagment» für die Tochtergesellschaften anzuwenden. Zwischen dem Risikomanagement und dem BCM besteht eine wechselseitige Beziehung. Einerseits liefern die Risiken, welche im Risikoprozess der Zentralbahn identifiziert werden, Inputs für mögliche Ansatzpunkte des BCM. Dabei kommen vor allem diejenigen Risiken in Frage, welche ein sehr hohes Schadensausmass aufweisen, gleichzeitig aber mit einer sehr tiefen Eintretenswahrscheinlichkeit bewertet sind. Ein Konzept für das Krisen- und das betriebliche Kontinuitätsmanagement ist vorhanden. Auf einer Webplattform sind Dokumente und Informationen verlinkt und verfügbar. Für alle Mitglieder des Krisenstabes stehen die wichtigsten Unterlagen auch in Papierform zur Verfügung.

Es finden regelmässig Krisenstabsübungen statt, woraus Massnahmen definiert und umgesetzt werden. Ende 2020 wurden in Zusammenarbeit mit einer externen Firma die Prozesse und Organisation auf Grund der Krisenstabübung 2019 überprüft und ein physischer Behelf erstellt. Zur Schärfung ist eine Intensivschulung im Jahr 2021 terminiert. Weiter sind wir an der Evaluation und Bedürfnisklärung unterstützender Tools, welche eine BIA und daraus ableitend die nötig zu erstellenden BCP enthalten.

Empfehlung 17 (Priorität 1)

Die EFK empfiehlt der zb, mittels periodischer Übungen die Einsatzfähigkeit der Ausweichstandorte zu prüfen, um im Krisenfall deren Betrieb sicherzustellen.

Stellungnahme der zb

Am Donnerstag, 28.01.2021 wurde ein Test Evakuation der Leitstelle mit vier Mitarbeitenden durchgeführt. Ziele waren: Instruktion / Refresher Weg und Ort Rückfallebene

- Anwendung Schlüsselmanagement ZSW und Rechnerraum SSTA
- Test Kommunikation
- Grundlagen und Erkenntnisse für Notfallhandbuch Leitstelle
- Erkenntnisse über weitere Massnahmen
- Nachweis der Funktionsfähigkeit

Die Funktionsfähigkeit konnte nachgewiesen werden. Die anwesenden Fdl konnten sich mit den in Stansstad dafür vorhandenen Schlüssel Zutritt verschaffen und das ILTIS in Betrieb nehmen und bedienen. (Auszug aus dem Bedienungsprotokoll vorhanden). Die periodische Anwendung ist in der Instruktionskontrolle neue Mitarbeitende BF und neu mit Eintrag Schulungen BF sichergestellt.

Die Evakuationsübung wird künftig ein Mal pro Jahr wiederholt.

5 Die Rhätische Bahn AG

Die RhB ist eine privatrechtlich organisierte Aktiengesellschaft mit Sitz in Chur. Die Hauptaktionäre sind mit rund 51 % der Kanton Graubünden und mit 43 % der Bund. Die restlichen ca. 6 % teilen sich die Gemeinden und private Investoren auf. Im Geschäftsjahr 2019 beschäftigte das Unternehmen etwa 1500 Mitarbeitende und erwirtschaftete einen Betriebsertrag von 393 Millionen Franken.

Das 384 Kilometer lange meterspurige Streckennetz, mit Ausnahme eines kleinen Teils in Italien, liegt überwiegend im Kanton Graubünden und hat den Status eines UNESCO-Welterbes. Jährlich befördert die RhB 12 Millionen Fahrgäste, etwa 530 000 Fahrzeuge und 563 000 Tonnen Güter.

5.1 Einschätzung der Maturität aus dem Framework

Die Auswertung der Maturität gegenüber dem IKT-Minimalstandard zeigt, dass die RhB in allen Bereichen den Anforderungen entspricht oder diese übertrifft (siehe Abbildung 4). Die Informatikumgebung und bahnbetriebsrelevanten Infrastrukturen weisen in fast allen Bereichen eine überdurchschnittliche Maturität aus.

Detaillierte unternehmensweite Vorgaben stehen allen Mitarbeitenden zur Verfügung. Die Ziele, Aufgaben und Aktivitäten im Bereich der Informationssicherheit sind innerhalb der Strategie festgehalten und werden im ordentlichen Prozess jährlich oder bei Bedarf überprüft. Die Rollen und Verantwortlichkeiten für die IKT-Sicherheit, den Datenschutz und das Risikomanagement (RM) sind unternehmensweit definiert und werden gelebt. Die Qualitätssysteme sind sehr umfangreich und die daraus hervorgehenden Massnahmen werden umgehend bewertet und zur Umsetzung weitergeleitet.

IKT-Sicherheitsthemen sind im Unternehmen breit adressiert, dennoch ist die Sensibilisierung bei einzelnen Mitarbeitenden noch nicht auf einem angemessenen Stand. Der IKT-Sicherheit in Projekten muss ein grösserer Stellenwert beigemessen werden.

Die Infrastrukturen für den Bahnbetrieb und die allgemeine IKT sind auf hohe Verfügbarkeit ausgerichtet und daher auch mehrfach redundant aufgebaut. Die RhB hat eine hohe Segmentierung des Netzwerks, sowohl auf logischer wie auch auf physischer Ebene. Die Überwachung der Netze erfolgt in verschiedenen Bereichen, noch sind die Auswertungen allerdings nicht zentral institutionalisiert.

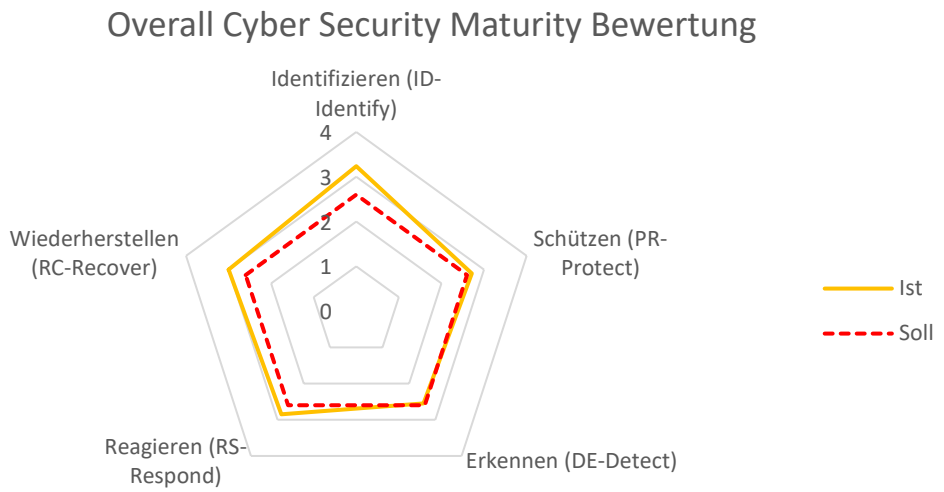


Abbildung 4: Assessment-Auswertung über alle Prüfbereiche (Details siehe Anhang 7)

5.2 Bei Projekten wird der Informationssicherheit nicht systematisch Rechnung getragen

Die RhB verfügt über ein umfangreiches Projektportfolio über alle Bereiche des Unternehmens. Ein Leitfaden und das Programm Cockpit unterstützen die Projektleitenden im Projektmanagement. Der Prozess dazu ist im Intranet abgelegt. Die RhB führt Projekte nach einem allgemeingültigen Phasenablauf. In einzelnen Detailphasen wird zwischen Infrastruktur-, Rollmaterial- und Informatikprojekten differenziert. In den allgemeinen Projektphasen ist kein Beizug eines IT-Security Spezialisten gefordert, auch sind keine Pflichtdokumente wie Schutzbedarfserhebungen gefordert. Allerdings wird im Projektantrag und im Projektbeschrieb auf einen Bezug zur IT eingegangen. Bei den Phasenübergängen ist eine institutionalisierte Kontrolle der Umsetzung von Sicherheitsanforderungen nicht etabliert.

Das Handbuch für IT-Projektmanagement adressiert die IKT-Sicherheit marginal und verweist auf übergeordnete Vorgaben. In diesen sind jedoch keine konkreten Anforderungen an das Projektmanagement ersichtlich. Die Prüfung der Schutzwürdigkeit der Datenbestände wird erst in der Detailphase gefordert.

Beurteilung

Der Aufbau und die Weiterentwicklung komplexer technischer Infrastrukturen erfolgen durch Projekte. Die Eingriffe der Projekte in die zunehmend miteinander verknüpften IKT-Landschaften bedeuten immer auch Eingriffe in bestehende Sicherheitsstrukturen. Bei Projekten müssen Vorgaben zur IKT-Sicherheit vorhanden sein und Sicherheitsspezialisten von Anfang an beigezogen werden. Nur so kann sichergestellt werden, dass die Sicherheit angemessen berücksichtigt wird. Erfahrungsgemäss sind die Ergebnisse unbefriedigend und kostenintensiv, wenn diese Aspekte erst in späten Phasen des Projekts adressiert werden.

Empfehlung 18 (Priorität 1)

Die EFK empfiehlt der RhB, IKT-Sicherheitsvorgaben für Projekte zu erlassen und deren Umsetzung in den unterschiedlichen Projektphasen in geeigneter Weise sicherzustellen.

Stellungnahme der RhB

Die RhB bringt jedes Jahr eine Vielzahl von unterschiedlichen Projekten erfolgreich zum Abschluss. Bei diesen Projekten wurden entsprechende Fachspezialisten zu Rate gezogen, die auch die Sicherheitsprüfung vorgenommen haben. Ziel der RhB ist es, dass spezifische Vorgaben zur IKT-Sicherheit in jedem einzelnen Projekt der RhB beachtet und systematisch geprüft werden. Innerhalb der Branche steht zusätzlich im Rahmen der RAILplus AG ein Fachspezialist zur Verfügung, welcher die einzelnen Bahnen unterstützt.

5.3 Der Faktor Mensch ist für die Informationssicherheit von zentraler Bedeutung

Die Sensibilisierung für die Belange der IKT-Sicherheit erfolgt im Rahmen eines allgemeinen Einführungstags beim Stellenantritt. Weitere Sensibilisierungen der Mitarbeitenden werden nur rudimentär durchgeführt. Durch gelegentliche News im Intranet werden den Mitarbeitenden zu spezifischen Themen Informationen zur Verfügung gestellt. Nachhaltige und stufengerechte Schulungen finden während der Anstellung nicht mehr statt, auch keine dedizierten Massnahmen für Führungskräfte oder Spezialfunktionen. Jedoch bemüht sich die RhB IT die Geschäftsleitung auf Security-Themen zu sensibilisieren, indem sie immer wieder aktuelle externe Cybervorfälle aufbereitet und präsentiert. Mittels eines jährlich erstellten Berichtes informiert die IT die Unternehmensleitung zum Stand der Informationssicherheit. Die Sensibilisierung der Lieferanten erfolgt indirekt durch Verträge und Betriebsvorschriften.

Die freiwillig und periodisch durchgeführten Phishing-Kampagnen zeigen, dass die RhB im Vergleich zu anderen Unternehmen eher schlecht abgeschnitten hat und sich im letzten Jahr sogar verschlechterte. Dieser Umstand hat allerdings zu unterschiedlichen technischen Massnahmen, wie etwa der Einführung einer Multifaktor-Authentisierung geführt.

Beurteilung

Die beste Technik und Software nutzen wenig, solange der Mensch diese wieder ausser Kraft setzt. Daher gilt es, das Sicherheitsbewusstsein jedes einzelnen Mitarbeitenden zu schärfen. Die Sensibilisierung für Themen rund um die Sicherheit in Bezug auf die IKT des Unternehmens und die Gefahren, die während der alltäglichen Arbeit lauern, kann diese nachhaltig verbessern. Die in den letzten Jahren durchgeführten Phishing-Kampagnen sind ein geeignetes Mittel, um einen Bereich der Awareness zu prüfen. Ohne flankierende Massnahmen oder einer gezielten Kampagne zeigen diese jedoch kaum Wirkung.

Empfehlung 19 (Priorität 1)

Die EFK empfiehlt der RhB, durch periodische und stufengerechte Sensibilisierungskampagnen die Mitarbeitenden über alle Bereiche in den Belangen der IKT-Sicherheit zu schulen.

Stellungnahme der RhB

Es ist für jeden von uns herausfordernd, ein Bewusstsein für die Gefahren zu entwickeln, welche die immer noch recht jungen digitalen Technologien mit sich bringen. Die RhB sensibilisiert bereits heute ihre Mitarbeitenden mit einzelnen Kampagnen. Zukünftig werden weitere Massnahmen erarbeitet, mit denen die Mitarbeitenden bei der Entwicklung eines ausgeprägten Sicherheitsverständnisses unterstützt werden.

5.4 Durch eine zentrale Netzwerküberwachung können Vorfälle rascher erkannt werden

Die Datennetze der RhB werden jeweils mittels Netzmanagementsystemen überwacht. Damit werden Statusmeldungen der Netzwerkgeräte ausgewertet und primär die Verfügbarkeit überprüft. Inhaltliche Auswertungen auf applikatorischer Ebene des Netzwerkverkehrs finden nur zu forensischen Zwecken statt. Das Performancemonitoring erfolgt durch Sensoren, die Daten laufend in das Netzwerkmanagementsystem melden. Die Informationen werden für allfällige Alarmierungen verwendet. Ein Pikettdienst hat Zugriff auf das System und kann zeitnah entsprechende Massnahmen einleiten. Die Netzüberwachung obliegt der Abteilung «Elektrontechnische Anlagen», die IT-Abteilung ist hier in gewisser Weise ein Leistungsbezüger.

Die RhB hat bisher keine zentrale Überwachung des gesamten Netzes implementiert. Die Daten aus den verschiedenen Systemen werden zum Prüfungszeitpunkt mit einem Datenanalysewerkzeug unzureichend ausgewertet.

Bei laufenden Projekten beabsichtigt die RhB die unternehmensweiten Daten zu zentralisieren und mit einem geeigneten Werkzeug für verschiedene Zwecke auszuwerten. Im Fokus stehen aktuell betriebswirtschaftlich relevante Daten wie beispielsweise Informationen zum eingesetzten Rollmaterial. Die Auswertung der Informationen aus den verschiedenen Netzwerküberwachungen soll im Rahmen der Einführung auch adressiert werden. Im Projekt sollen zudem die Schnittstellen zu den verschiedenen Quellen erhoben und entsprechend angebunden werden. Mit dieser Massnahme wird die RhB in der Lage sein, künftig den Einsatz von IKT-Sicherheitssystemen im Unternehmen zu vereinfachen und die Analyse von Ereignissen zu verbessern.

Beurteilung

Dass die verschiedenen Bereiche im Betrieb der Netze und der darauf installierten Dienste Überwachungen durchführen, ist unumgänglich. Voneinander losgelöste Auswertungen erlauben jedoch kein Gesamtbild. Grössere Bedrohungen können daher erst spät oder nur in einem begrenzten Raum erkannt werden. Die zentrale Haltung der Daten und eine entsprechende Auswertung können für die IKT-Sicherheit einen echten Mehrwert darstellen.

Die Anbindung und zentrale Auswertung der verschiedenen Datenquellen können im Rahmen des laufenden Projekts bewerkstelligt werden und sollten unbedingt eine zentrale Rolle spielen. Mit dieser Massnahme wird die RhB künftig in der Lage sein, mittels eines Gesamtbilds des Netzwerkverkehrs besser auf mögliche Unregelmässigkeiten zu reagieren.

Empfehlung 20 (Priorität 1)

Die EFK empfiehlt der RhB im Rahmen des Projekts zur zentralen Datenhaltung die Aspekte der IKT-Sicherheit hinsichtlich der Datenauswertung festzulegen und umzusetzen.

Stellungnahme der RhB

Schon heute findet eine Vielzahl von Auswertungen bei der RhB dezentral statt. Mit laufenden Projekten sollen die dabei erhobenen Daten weiter zentralisiert werden, um für zukünftige Analysen den Rundumblick effizient zu gewährleisten. Besondere Beachtung werden dabei systematische Auswertungen für die IKT-Sicherheit finden. Die zuständigen Personen werden zu einem Gremium zusammengeführt.

5.5 Eine Kategorisierung von Sicherheitsvorfällen ist für die Feststellung der Auswirkungen erforderlich

Für die Bearbeitung von Sicherheitsvorfällen setzt die RhB ein Computer Emergency Response Team (CERT) ein. Dieses wird durch die Fachstelle IT-Sicherheit koordiniert und besteht aus Spezialisten und Fachpersonen aus den relevanten Bereichen. Bei Bedarf kann das CERT durch externe Spezialisten verstärkt werden. Zu den Aufgaben gehören die Beurteilung aktueller Sicherheitsvorfälle, die Eindämmung von Gefahren aus Sicherheitsvorfällen sowie die Behebung der Störungen. Eine weitere wichtige Aufgabe des CERT ist die Klärung des Hergangs eines Vorfalls und die forensische Aufarbeitung.

Eine Kategorisierung für Vorfälle ist nicht vordefiniert. Daher ist eine zeitnahe Abgrenzung des Schweregrads beschränkt. Die Unterscheidung zwischen Störungen, Sicherheitsvorfällen und Notfällen oder Krisen ist dadurch erschwert.

Beurteilung

Die Sicherheitsorganisation der RhB ist grundsätzlich zielführend aufgestellt. Die Bearbeitung von Vorfällen ist durch den Einsatz eines CERT angemessen gelöst.

Informationssicherheitsereignisse müssen bewertet werden. Die zuständige Stelle soll jedes Ereignis mittels eines vordefinierten Klassifizierungsschemas bewerten und entscheiden, ob das Ereignis als Vorfall eingestuft werden soll. Die Klassifizierung und Priorisierung von Vorfällen können helfen, die Auswirkungen und das Ausmass eines Vorfalls festzustellen. Die RhB hat das Potenzial der Klassifizierung erkannt und adressiert, daher verzichtet die EFK auf eine Empfehlung.

6 Neue Vorgaben zur IKT-Sicherheit für Bahnunternehmen

6.1 Revidierte Ausführungsbestimmungen zur Eisenbahnverordnung

Die Eisenbahnverordnung (EBV) und ihre Ausführungsbestimmungen (AB-EBV) gelten für sämtliche Eisenbahnen, die der schweizerischen Eisenbahngesetzgebung unterstellt sind. In diesem Jahr wurden die beiden Dokumente durch das BAV umfassend überarbeitet, sie treten auf den 1. November 2020 in Kraft. Die Schwerpunkte der Revisionsrunde adressierten in erster Linie technische Themen und die Übernahme weiterer EU-Rechtsakte. Die Wichtigkeit der IKT-Sicherheit wurde vom BAV erkannt und in den Ausführungsbestimmungen entsprechend präzisiert.

So müssen Anlagen, Systeme und Fahrzeuge, die IKT-Systeme verwenden oder enthalten, gegen missbräuchliche Eingriffe geschützt werden. Basierend auf einer Risikoanalyse soll ein Schutzkonzept erstellt, umgesetzt und laufend aktualisiert werden.[4]

Mit dem Aufbau eines ISMS sollen ausserdem hinreichende Massnahmen zur Beherrschung des Risikos von missbräuchlichen Eingriffen in IKT-Systeme über den Lebenszyklus gewährleistet werden. Die Konformität mit der Norm ISO/IEC 27001 und wo relevant mit deren spezifischen Ausprägung IEC 62443 sind dabei anzustreben.[5]

6.2 Die Umsetzung der Vorgaben stellt kleine Bahnen vor grosse Herausforderungen

Gemäss den Ausführungsbestimmungen müssen künftig sämtliche Bahnbetreiber ein ISMS aufbauen und betreiben. Eine entsprechende Vorgabe gilt europaweit. Der Aufwand für die Einführung eines ISMS kann recht hoch sein. Es ist unklar, wie kleine Unternehmen diese Anforderung mit angemessenem Aufwand umsetzen sollen. Das BAV hat keine weiteren Vorgaben zur Ausführung gemacht. Auch ist nicht geregelt, bis wann diese Anforderung umgesetzt werden muss. Gerade für kleine Unternehmen, die weder über Rollen in der IKT-Sicherheit noch über das Wissen zur Umsetzung verfügen, stellt das eine erhebliche Herausforderung dar. Die Kosten für eine allfällige externe Unterstützung bei der Erstellung eines ISMS sind dabei nicht zu unterschätzen.

Zum Prüfungszeitpunkt ist auch nicht definiert, wie das BAV die Umsetzung der Vorgabe überprüfen wird.

Beurteilung

Die Verankerung der IKT-Sicherheit in den AB-EBV erachtet die EFK als zielführend. Durch den Einsatz eines ISMS kann die Sensibilisierung gefördert und die IKT-Sicherheit nachhaltig verbessert werden.

[4] AB-EBV 5c.1.1
[5] AB-EBV 5c.1.2

Die wirksame Einführung eines ISMS nach der Norm ISO/IEC 27001 für kleine Bahnen erachtet die EFK nur mit einem mittel- bis langfristigen Zeithorizont als realistisch. Mit minimalen Anforderungen (z. B. Inventar der kritischen Komponenten, Risikoanalysen usw.), die dafür kurzfristig und konsequent umgesetzt und in die betrieblichen Abläufe eingebunden werden, könnten die Bahnen stufenweise eine höhere IKT-Sicherheit erlangen.

Mit der zusätzlich empfohlenen Umsetzung des Branchenstandards «Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs» durch alle Bahnen, kann bei einer zu formalistischen Umsetzung eine erhebliche Belastung für kleinere Betriebe entstehen (siehe Kapitel 6.3).

Die Querschnittsprüfung hat gezeigt, dass grössere Bahnen bezüglich der IKT-Sicherheit recht gut aufgestellt sind. Für kleine Betriebe stellt dieser Aspekt eine grosse Herausforderung dar. Durch die bestehenden personellen und finanziellen Ressourcen sind diese kaum in der Lage, die Situation mittelfristig auf ein angemessenes Niveau zu heben. Wie das Beispiel der zb zeigt, kann eine enge Zusammenarbeit mit grösseren Bahnen und der Bezug von Dienstleitungen (wie SOC) diesem Umstand positiv entgegenwirken. Auch die Branchenorganisationen (etwa VöV oder RAILplus) können durch eine vertiefte Zusammenarbeit nachhaltiges Synergiepotenzial generieren.

Empfehlung 21 (Priorität 1)

Die EFK empfiehlt dem BAV, die minimalen Anforderungen an ein ISMS zu spezifizieren und, in Absprache mit den Branchenverbänden, geeignete Hilfsmittel zu erarbeiten. Eine Zusammenarbeit unter den Infrastrukturbetreibern ist dabei wo möglich zu fördern.

Stellungnahme des BAV

Das BAV hat bereits begonnen, die minimalen Anforderungen an ein ISMS zu spezifizieren. Das ISMS soll gemäss der AB-EBV:2020 Teil des Sicherheitsmanagementsystems (SMS) sein.

Die bestehenden Umsetzungshilfen, welche auf bav.admin.ch abrufbar sind, werden unter Einbezug der Branche laufend angepasst und wo nötig erweitert.

6.3 Umsetzung des IKT-Minimalstandards für den öffentlichen Verkehr

Der Verband öffentlicher Verkehr (VöV) ist ein Schweizer Verband in der Rechtsform einer Genossenschaft mit Sitz in Bern. Als Branchenverband vertritt er die vielfältigen Anliegen und Interessen der Verkehrsunternehmen des öffentlichen Verkehrs (öV) gegenüber Behörden, Politik, Verwaltung, Industrie und Dritten. Die Kommission Infrastruktur (KIS) ist die Plattform für die Infrastrukturunternehmen der Schweizerischen Eisenbahnen. Sie unterstützt den unternehmensübergreifenden Wissensaustausch in verschiedenen Themenbereichen. Die KIS hat eine Arbeitsgruppe bestehend aus Branchen- und Fachexperten des BAV eingesetzt, welche das «Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs» auf Basis des IKT-Minimalstandard des BWL ausgearbeitet hat.

Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs

Das Branchendokument «Handbuch Cybersecurity» ist ein Leitfaden zum Aufbau der Cybersecurity im Unternehmen. Es stützt sich auf den IKT-Minimalstandard des BWL und spezifiziert die Empfehlungen für den öV. Der Branchenstandard wurde im August 2020 durch

den Vorstand des VöV verabschiedet. Die Bahnen sind nun angehalten, die Empfehlungen umzusetzen. Grundsätzlich ist die Bereitschaft hierzu bei den Kadern der Bahnen vorhanden. Der Verband wird sie mittels Schulungen, Onlinetrainings und persönlicher Beratung durch die Sachverständigen der Arbeitsgruppe unterstützen. Zudem sollen je nach Bedarf einheitliche Vorlagen und Hilfsmittel zu verschiedenen Themen angeboten werden. Hierfür muss aber zunächst abgeklärt werden, in welchen Bereichen der Umsetzungsempfehlungen des Handbuches Cybersecurity ein Bedarf besteht und auf welchem Maturitätslevel sich die Bahnen heute befinden.

Beurteilung

Die EFK begrüsst die Ausarbeitung und Spezifizierung eines Branchenhandbuchs für den öV. Die Umsetzung des Standards wird die IKT-Sicherheit aller Bahnen in der Schweiz verbessern. Damit diese Ziele erreicht werden können, ist es unabdingbar, dass die kleinen Bahnen eine möglichst umfassende Unterstützung durch die verschiedenen Branchenverbände in Anspruch nehmen können (siehe auch Kapitel 6.2).

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV) vom 23. November 1983 (Stand am 1. November 2020), SR 742.141.1
Ausführungsbestimmungen zur EBV – AB-EBV (Stand am 1. November 2020), SR 742.141.11
Strategien
Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 vom 8. Dezember 2017
Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022 vom 18. April 2018

Anhang 2: Abkürzungen

AB-EBV	Ausführungsbestimmungen zur Eisenbahnverordnung
BAV	Bundesamt für Verkehr
BCP	Business-Continuity-Pläne (business continuity planning)
BIA	Business-Impact-Analyse
BR	Bundesrat
BWL	Bundesamt für wirtschaftliche Landesversorgung
CDF	Contrôle fédéral des finances
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
DB	Datenbank
EBV	Verordnung über Bau und Betrieb der Eisenbahnen
EFK	Eidgenössische Finanzkontrolle
ETCS	European Train Control System (siehe Glossar)
GL	Geschäftsleitung
IKT	Informations- und Kommunikationstechnik
ISO/IEC	International Organization for Standardization (siehe Glossar)
ISMS	Information Security Management System (siehe Glossar)
KI	Kritische Infrastruktur (siehe Glossar)
LEB	Lausanne-Echallens-Bercher Bahn AG / Chemin de fer Lausanne-Echallens-Bercher SA
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
OFT	Office fédéral des transports
ÖV	Öffentlicher Verkehr
RhB	Rhätische Bahn AG

RM	Risikomanagement
SBB	Schweizerische Bundesbahnen AG
SCADA	Supervisory Control and Data Acquisition (siehe Glossar)
SGSI	Système de gestion de la sécurité de l'information
SKI	(Nationale Strategie zum) Schutz kritischer Infrastrukturen
SOC	Security Operations Center
TL	Transports publics de la région lausannoise
TPF	Freiburgische Verkehrsbetriebe AG / Transports publics fribourgeois SA
VöV	Verband öffentlicher Verkehr
VR	Verwaltungsrat
zb	Zentralbahn AG
ZBMS	Zugbeeinflussung für Meter- und Spezialspurbahnen (siehe Glossar)

Anhang 3: Glossar

DIN ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
Enterprise-Resource-Planning-System	Bezeichnung für die unternehmerische Aufgabe, Ressourcen wie Kapital, Personal, Betriebsmittel, Material und Informations- und Kommunikationstechnik im Sinne des Unternehmenszwecks rechtzeitig und bedarfsgerecht zu planen, steuern und verwalten.
ETCS	Das European Train Control System ist ein Zugbeeinflussungssystem. ETCS ist ein grundlegender Bestandteil des zukünftigen interoperablen, europäischen Zugbeeinflussungs- und Zugleitsystems.
Firewall	Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten externen Netzwerkzugriffen schützt.
Georedundanz	Einsatz von zwei oder mehreren vollständig funktionsfähigen Rechenzentren an unterschiedlichen Standorten.
IEC 62443	Die internationale Normenreihe IEC 62443 befasst sich mit der Cybersecurity von Industrial Automation and Control Systems» (IACS) und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.
Information Security Management System	Verfahren und Vorgaben innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.
Kritische Infrastruktur	Als KI werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.
Logging	Automatische Erstellung eines Protokolls von Softwareprozessen
Meterspur	Der Begriff Meterspur bezeichnet bei Eisen- und Strassenbahnen eine Variante der Schmalspur mit einer Spurweite von einem Meter.
Netzwerkmanagement	Verwaltung, Betriebstechnik und Überwachung von IT-Netzwerken und Telekommunikationsnetzen.

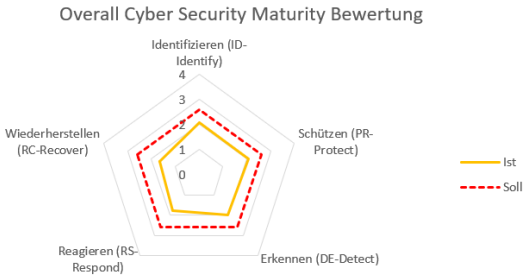
Phishing	Der Begriff Phishing beschreibt Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.
Ransomware	Erpressungssoftware oder Verschlüsselungstrojaner sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff auf die Daten eines Computers verunmöglicht.
Supervisory Control and Data Acquisition	Technische Komponenten bzw. Computersysteme zur Überwachung und Steuerung technischer Prozesse
Systemführerschaft	Ein Eisenbahninfrastrukturunternehmen kann übergeordnete Aufgaben des Betriebs oder der Entwicklung für mehrere Eisenbahninfrastrukturunternehmen wahrnehmen.
UNESCO-Welterbe	Bezeichnung für Denkmäler, Orte sowie Naturgebilde, geologische Erscheinungsformen und Naturstätten von aussergewöhnlichem weltweitem Wert
Zugbeeinflussung für Meter- und Spezialspurbahnen	2013 legte das BAV einen verbindlichen Standard für die Zugbeeinflussung für Meter- und Spezialspurbahnen (ZBMS-Standard) fest.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

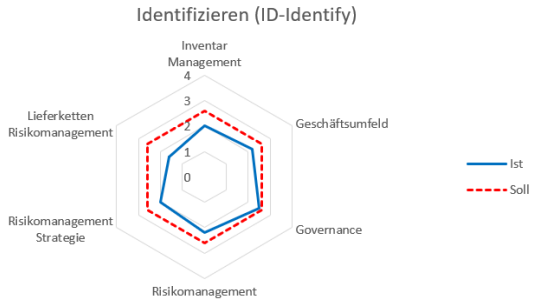
Anhang 4: Assessment-Auswertung LEB

Übersicht:

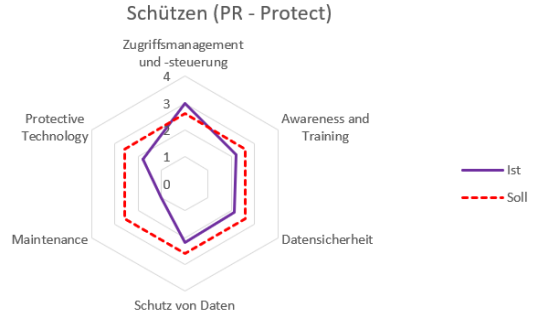


Overall Cyber Security Maturity	Ist	Soll
Identifizieren (ID-Identify)	2.1	2.6
Schützen (PR-Protect)	2.1	2.6
Erkennen (DE-Detect)	2.0	2.6
Reagieren (RS-Respond)	1.8	2.6
Wiederherstellen (RC-Recover)	1.7	2.6

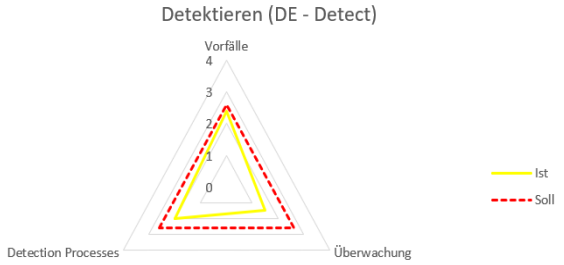
Die fünf Prüffelder im Detail:



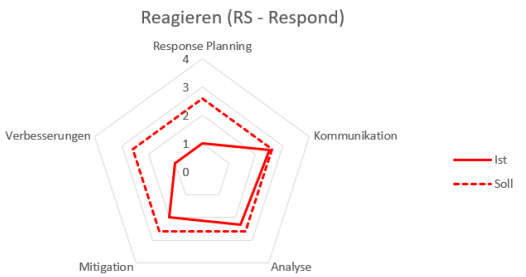
Empfehlung 1



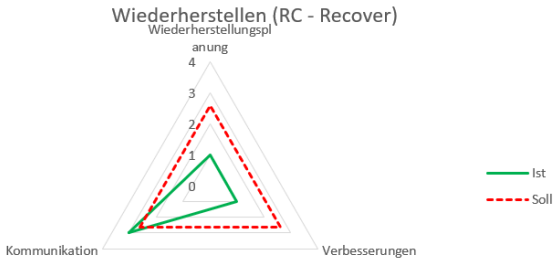
Empfehlung 2, 3, 4



Empfehlung 5



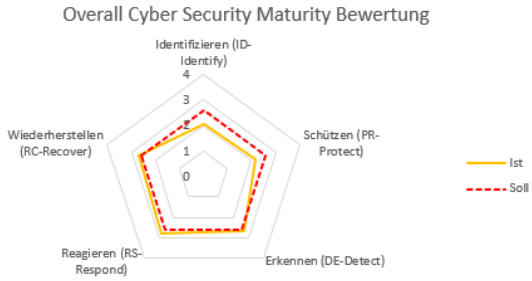
Keine Empfehlung



Empfehlung 4, 6

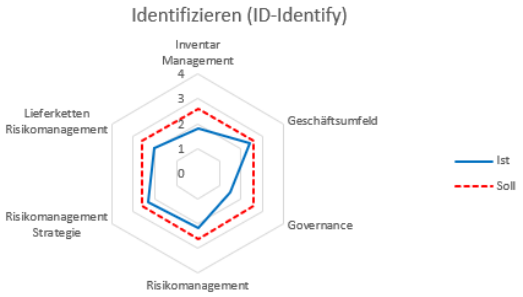
Anhang 5: Assessment-Auswertung TPF

Übersicht:



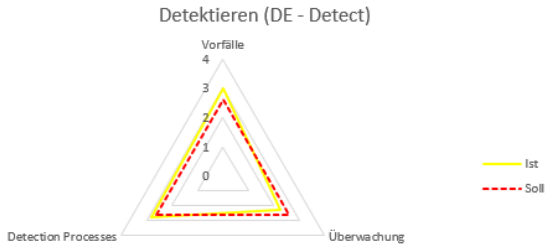
Overall Cyber Security Maturity	Ist	Soll
Identifizieren (ID-Identify)	2.0	2.6
Schützen (PR-Protect)	2.2	2.6
Erkennen (DE-Detect)	2.7	2.6
Reagieren (RS-Respond)	2.8	2.6
Wiederherstellen (RC-Recover)	2.7	2.6

Die fünf Prüffelder im Detail:

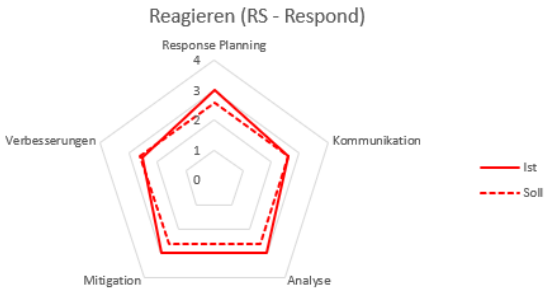


Empfehlung 7, 8, 9

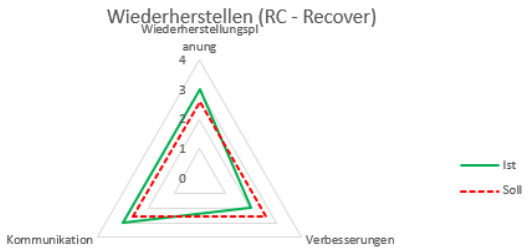
Empfehlung 10, 11



Keine Empfehlung



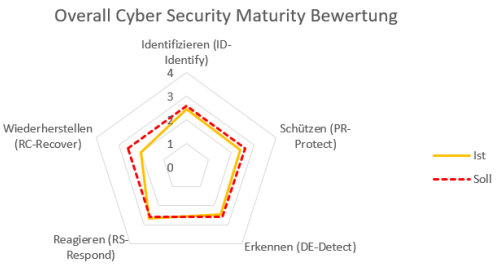
Keine Empfehlung



Keine Empfehlung

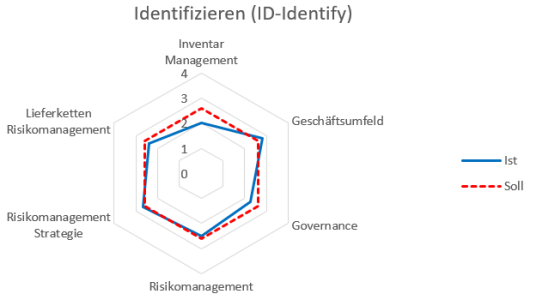
Anhang 6: Assessment-Auswertung zb

Übersicht:

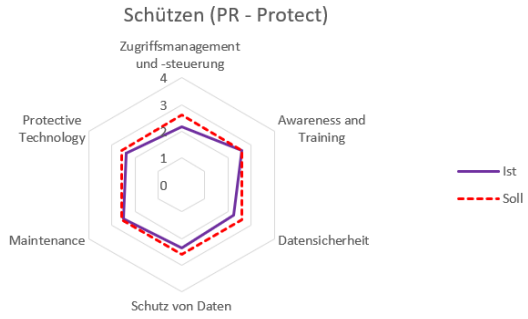


Overall Cyber Security Maturity	Ist	Soll
Identifizieren (ID-Identify)	2.4	2.6
Schützen (PR-Protect)	2.4	2.6
Erkennen (DE-Detect)	2.5	2.6
Reagieren (RS-Respond)	2.7	2.6
Wiederherstellen (RC-Recover)	2.0	2.6

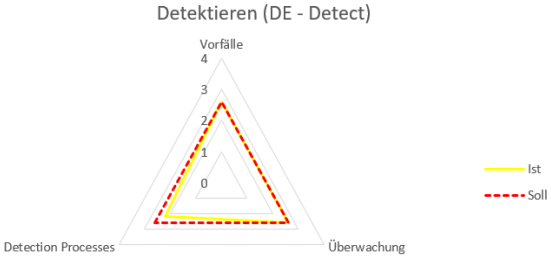
Die fünf Prüffelder im Detail:



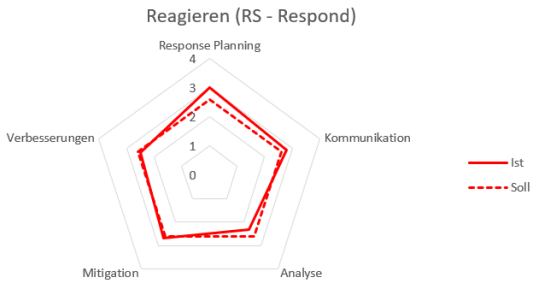
Empfehlung 12



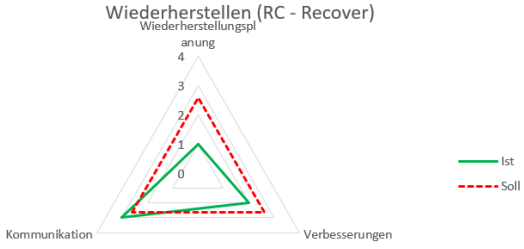
Empfehlung 13, 14, 15



Keine Empfehlung



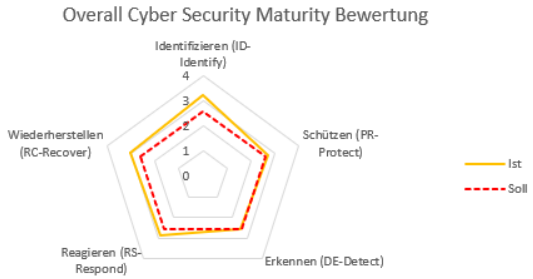
Empfehlung 16, 17



Empfehlung 16, 17

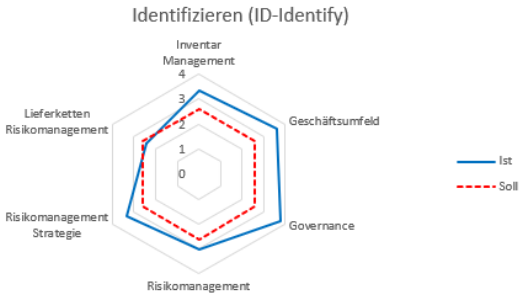
Anhang 7: Assessment-Auswertung RhB

Übersicht:

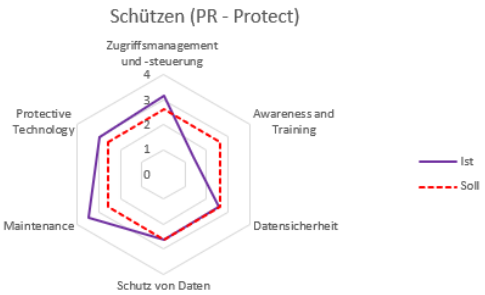


Overall Cyber Security Maturity	Ist	Soll
Identifizieren (ID-Identify)	3.2	2.6
Schützen (PR-Protect)	2.7	2.6
Erkennen (DE-Detect)	2.6	2.6
Reagieren (RS-Respond)	2.9	2.6
Wiederherstellen (RC-Recover)	3.0	2.6

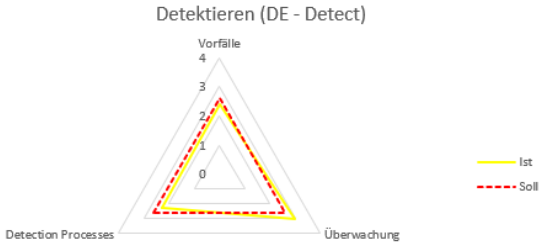
Die fünf Prüffelder im Detail:



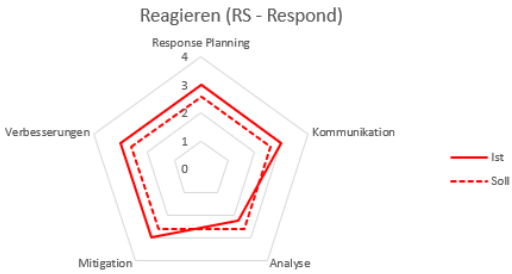
Empfehlung 18



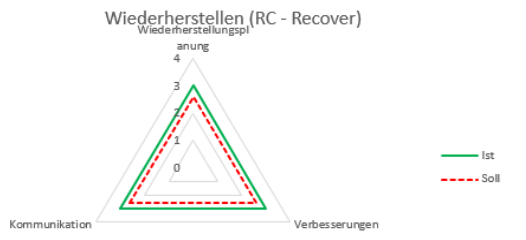
Empfehlung 19



Empfehlung 20



Keine Empfehlung



Keine Empfehlung