EIDGENÖSSISCHE FINANZKONTROLLE

Prüfung des Schutzes kritischer Infrastrukturen – Umsetzung der Mindeststandards in der Flugsicherung

Skyguide

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	961.21408
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

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

Inhaltsverzeichnis

Prüfung des Schutzes kritischer Infrastrukturen – Umsetzung der Mindeststandards in der Flugsicherung

Skyguide

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 gehören auch die zivile Luftfahrt und die Flugsicherung. Skyguide besorgt im Auftrag des Bundes die zivile und militärische Flugsicherung in der Schweiz und in angrenzenden Gebieten. Der Bund ist Mehrheitsaktionär der Skyguide.

Die Eidgenössische Finanzkontrolle (EFK) hat die Einhaltung von Minimalanforderungen zum IKT-Schutz gegen Cyberangriffe bei Skyguide geprüft. Dabei kam der vom Bundesamt für wirtschaftliche Landesversorgung (BWL) für Betreiber von KI empfohlene «Minimalstandard zur Verbesserung der IKT-Resilienz» zum Einsatz. Dieser deckt im Wesentlichen die fünf Themenbereiche «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen» ab und bietet konkrete Massnahmen zur Umsetzung an.

Skyguide bearbeitet die fünf Themenbereiche systematisch. Das minimale Sicherheitsniveau, wie durch den IKT-Minimalstandard empfohlen, wird aktuell noch nicht vollständig erreicht. Der Grossteil der dazu noch notwendigen Arbeiten ist bereits identifiziert und angestossen. Die Prüfung der EFK hat jedoch zusätzliches Optimierungspotenzial erkannt.

Das Informationssicherheitsmanagement muss bereitstehen

Ein Information Security Management System (ISMS, engl. für «Managementsystem für Informationssicherheit») ist ein grundlegender Baustein der Informationssicherheit. Im ISMS sind Regeln, Verfahren, Massnahmen und Werkzeuge definiert, mit denen sich die Informationssicherheit steuern, kontrollieren, sicherstellen und optimieren lässt.

Bei Skyguide laufen nach Anforderungen des Bundesamts für Zivilluftfahrt zielführende Arbeiten zur Implementierung eines ISMS. Zum Zeitpunkt der Prüfung war dieses noch nicht fertiggestellt und die Umsetzung muss gewährleistet werden.

Zugriffsrechte, das Schwachstellenmanagement und eine konsequente Umsetzung von Vorgaben sind zu verbessern

Um Sicherheitsrisiken zu minimieren, sollte ein Benutzer nur über Berechtigungen verfügen, welche er für die Ausübung seiner Arbeit zwingend benötigt. Skyguide wendet dieses «Prinzip der geringsten Privilegien» an. Jedoch werden die vergebenen Zugriffsrechte nicht regelmässig überprüft. So ist nicht sichergestellt, dass nach Veränderungen der Aufgaben eines Benutzers (z. B. Abteilungs- oder Funktionswechsel) die Berechtigungen angepasst werden.

Administratoren verfügen über umfassende Berechtigungen, mit welchen Sicherheitsmassnahmen der Systeme verändert oder sogar ausgeschaltet werden können. Entsprechend sind Administratoren primäre Ziele für Angreifer. Administratoren müssen zum Thema IT-Sicherheit regelmässig sensibilisiert und geschult werden. Dies findet im Moment nicht systematisch statt.

Skyguide hat zur Erfassung von technischen Verwundbarkeiten ihrer Hard- und Software eine automatisierte Verwundbarkeitsanalyse implementiert. Jedoch müssen die Entwickler sowie Applikationsverantwortlichen noch besser im Umgang mit den Resultaten der Analysen geschult werden. Verwundbarkeiten sind zwingend zentral zu erfassen und zu kategorisieren, um sie anschliessend kontrolliert zu beheben.

Die EFK hat in einer Stichprobe festgestellt, dass nach Änderungen von Vorgaben die betroffenen Parameter auf einem bestehenden System nicht an die neuen Werte angepasst wurden. Skyguide muss im Rahmen des formellen Änderungsprozesses sicherstellen, dass alle Systeme an neue Anforderungen angepasst werden.

Fehlende Georedundanz könnte längere Serviceunterbrüche zur Folge haben

Die Systeme für die Flugsicherung sind redundant vorhanden, jedoch physisch nicht in verschiedenen Lokalitäten aufgebaut. Entsprechend wird beim Ausfall eines gesamten Standorts der Service unterbrochen, wodurch die Flugsicherung in der ganzen Schweiz nicht mehr sichergestellt ist. Zudem bestanden noch keine Business-Continuity- oder Disaster-Recovery-Pläne für ein solches Szenario, sodass Skyguide im Moment schlecht auf einen solchen Vorfall vorbereitet ist.

Eine Optimierung des Lieferantenmanagements ist nötig

Skyguide hat den Betrieb wichtiger Teile ihrer IKT-Infrastruktur an Dienstleister ausgelagert. Dies erhöht die Komplexität bei Änderungen an den Systemen und bedingt eine sehr gute Kommunikation und Zusammenarbeit, um Systemausfällen vorzubeugen. Ebenso müssen die Reaktionen auf Systemausfälle sehr gut vorbereitet werden. Verschiedene Vorfälle haben gezeigt, dass in diesem Bereich noch Optimierungspotenzial besteht.

Skyguide muss bei sämtlichen kritischen Dienstleistern die Risiken aus den Lieferketten adressieren.

Audit de la protection des infrastructures critiques – Mise en œuvre des exigences minimales dans le domaine du service de la navigation aérienne

Skyguide

L'essentiel en bref

Les infrastructures critiques (IC) assurent l'approvisionnement de la Suisse en biens et services indispensables. Pour protéger ces IC, il faut garantir un fonctionnement aussi permanent que possible. Dans ce contexte, la résilience des technologies de l'information et de la communication (TIC) ou la protection des infrastructures critiques (PIC) contre les cybermenaces revêtent une grande importance. Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale de PIC (2018–2022). L'aviation civile et les services de la navigation aérienne en font aussi partie. Sur mandat de la Confédération, Skyguide assure les services civils et militaires de la navigation aérienne en Suisse et dans les régions limitrophes. La Confédération est l'actionnaire majoritaire de Skyguide.

Le Contrôle fédéral des finances (CDF) a vérifié le respect par Skyguide des exigences minimales en matière de protection des TIC contre les cyberattaques. La « norme minimale pour améliorer la résilience informatique » recommandée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) pour les exploitants d'IC a été appliquée. Cette norme couvre essentiellement les cinq thèmes : identifier, protéger, détecter, réagir et récupérer et propose des mesures concrètes à mettre en œuvre.

Skyguide traite ces cinq thèmes de manière systématique. Le niveau de sécurité minimal recommandé par la norme n'est actuellement pas encore complètement atteint. La plupart des travaux nécessaires à cet effet ont déjà été identifiés et lancés. L'audit du CDF a toutefois identifié un potentiel d'optimisation supplémentaire.

La gestion de la sécurité de l'information doit être opérationnelle

Un système de gestion de la sécurité de l'information (ISMS) est un élément fondamental de la sécurité de l'information. L'ISMS définit des règles, des procédures, des mesures et des outils qui permettent de gérer, de contrôler, de garantir et d'optimiser la sécurité de l'information.

Skyguide est en train de mettre en place un ISMS conforme aux exigences de l'Office fédéral de l'aviation civile. Lors de l'audit, celui-ci n'était pas encore finalisé et sa mise en œuvre doit être assurée.

Les droits d'accès, la gestion des vulnérabilités et la mise en œuvre cohérente des directives doivent être améliorés

Pour réduire les risques de sécurité, un utilisateur ne devrait disposer que des autorisations dont il a impérativement besoin pour effectuer son travail. Skyguide applique ce « principe

du moindre privilège ». Cependant, les droits d'accès attribués ne sont pas vérifiés régulièrement. Ainsi, il n'est pas garanti que les autorisations soient adaptées après des modifications des tâches d'un utilisateur (par exemple, changement de service ou de fonction).

Les administrateurs disposent d'autorisations étendues qui leur permettent de modifier ou même de désactiver les mesures de sécurité des systèmes. En conséquence, les administrateurs sont les premières cibles d'attaque. Les administrateurs doivent être régulièrement sensibilisés et formés à la sécurité informatique. Ce n'est pas encore systématique.

Skyguide a mis en place une analyse de vulnérabilité automatisée pour recenser les vulnérabilités techniques de son matériel et de ses logiciels. Cependant, les développeurs et les responsables d'applications doivent encore être mieux formés à l'utilisation des résultats des analyses. Les vulnérabilités doivent impérativement être recensées et catégorisées de manière centralisée pour pouvoir les éliminer ensuite de façon contrôlée.

Lors d'un contrôle aléatoire, le CDF a constaté qu'après des modifications de directives, les paramètres concernés dans un système existant n'avaient pas été adaptés aux nouvelles valeurs. Skyguide doit s'assurer, dans le cadre du processus de changement formel, que tous les systèmes sont adaptés aux nouvelles exigences.

L'absence de géoredondance pourrait entraîner de longues interruptions de service

Les systèmes pour les services de la navigation aérienne sont disponibles de manière redondante, mais ne sont pas physiquement installés dans différents lieux. En conséquence, si un site entier tombe en panne, le service est interrompu et le service de la navigation aérienne n'est plus assuré dans toute la Suisse. De plus, il n'existait pas encore de plan de gestion de la continuité des affaires ni de rétablissement après un sinistre pour un tel scénario, de sorte que Skyguide est actuellement mal préparé à un tel incident.

Une optimisation de la gestion des fournisseurs est nécessaire

Skyguide a externalisé l'exploitation d'importantes parties de son infrastructure TIC à des prestataires de services. Cela augmente la complexité des modifications apportées aux systèmes et nécessite une excellente communication et collaboration afin de prévenir les pannes de système. De même, les réactions aux pannes de système doivent être très bien préparées. Différents incidents ont montré qu'il existe encore un potentiel d'optimisation dans ce domaine.

Skyguide doit aborder les risques liés aux chaînes d'approvisionnement avec tous les prestataires de services critiques.

Texte original en allemand

Generelle Stellungnahme der Skyguide

Skyguide sieht diese EFK Prüfung als eine wertvolle Möglichkeit, um ihre Cyberresilienz und damit die Qualität des gesamten Unternehmens zu verbessern. Die Cyberresilienz ist ein wichtiger Pfeiler, der die Unternehmensstrategie im Kontext des Virtual Centre Programms und der weiteren Integration der schweizerischen Luftverkehrskontrolle in den Single European Sky unterstützt.

Der Bericht bewertet die Security und Initiativen als solide. Der Bericht bestätigt aber auch, dass die Skyguide noch nicht auf dem erforderlichen Security Niveau ist, um einerseits der Entwicklung der zu erwarteten Bedrohungslage ausreichend voraus zu sein und andererseits den strategischen Ambitionen Genüge zu tragen. Historisch ist Security bei Skyguide durch die bis anhin verwendete Technologie im Wesentlichen auf einen physischen oder digitalen Perimeterschutz limitiert gewesen. Dies hat sich fundamental mit der Einführung moderner Technologien im Umfeld neuer Betriebskonzepte und einer neuen Bedrohungslage verändert.

Skyguide holt in diesem Bereich mit einem dedizierten langfristigen Security Programm auf. Als solches begrüsst es Skyguide, dass die Eidgenössische Finanzkontrolle noch weitere Entwicklungsbereiche während der Prüfung unterstrichen hat und dabei die bereits systematisch identifizierten und angestossenen Arbeiten anerkennt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Kritische Infrastrukturen (KI) haben in unseren Gesellschaften die Funktion von Lebensadern. Wir sind darauf angewiesen, dass die Versorgung mit Energie und Wasser, mit Informationstechnik und Mobilität zuverlässig funktioniert. Fallen diese Systeme oder andere wichtige Infrastrukturen auch nur für kurze Zeit in grösserem Umfang aus, so kann dies schwerwiegende Auswirkungen für die Schweiz haben. Das Spektrum der kritischen Infrastrukturen umfasst neun Sektoren, unterteilt in 27 Teilsektoren (Branchen).

Der Luftverkehr umfasst den Personen- und Güterverkehr mithilfe von Luftfahrzeugen, insbesondere Flugzeugen. In diesem Teilsektor wird u. a. auch die bodengestützte Abwicklung des Luftverkehrs und die Flugsicherung, wie sie der Skyguide obliegt, berücksichtigt. Skyguide hat diese Aufgabe nicht nur im zivilen gewerblichen und im privaten Luftverkehr, sondern auch im militärischen. Sie spielt eine wichtige Rolle bei der Wahrung der Souveränität des schweizerischen Luftraums. Von der militärischen Einsatzzentrale aus gewährleistet sie die militärische Flugsicherung im Auftrag der schweizerischen Luftwaffe. Skyguide unterstützt Aufgaben der Luftverteidigung und Sicherheitseinsätze und führt Militärflugzeuge bei Trainingseinsätzen und Missionen sicher durch den zivilen Luftraum.

Grundvoraussetzung für eine moderne Wirtschaft, die auf die Mobilität von Gütern und Personen angewiesen ist, ist ein funktionsfähiges und leistungsfähiges Transport- und Verkehrssystem. Mit zunehmender Globalisierung von Produktion und Absatz sowie der Entwicklung im internationalen Personenverkehr hat sich die Infrastruktur Luftverkehr zu einem wichtigen Faktor für die Versorgung von Staat und Bevölkerung entwickelt.

Diese Bedeutung lässt sich auch unmittelbar aus dem « Kurzbericht des Bundesrates über die Erreichung der strategischen Ziele im Jahr 2019» herauslesen. 2019 gab es in der Schweiz, verteilt auf die nationalen und regionalen Flughäfen, 1,3 Millionen[1] Flugbewegungen.

Störungen im Flugverkehr wirken sich auf viele Lebensbereiche aus, insbesondere die Wirtschaft (Verzögerungen bei Produktion und Warenauslieferung, Verfügbarkeit von Personal), die Regierung (Beschränkte Mobilität der nationalen und internationalen Behördenvertreter) als auch die Bevölkerung (unzureichende Versorgung mit frischen Gütern und Postdienstleistungen aus Übersee, mögliche Auswirkungen auf Rettungs- und Gesundheitswesen, fehlende Mobilität im Arbeits- und Freizeitbereich etc.) werden durch länger anhaltende Störungen nachhaltig beeinträchtigt.

Gleichzeitig ist der Luftverkehr auf die Funktionsfähigkeit anderer Teilsektoren zwingend angewiesen, wie z. B. die Erdöl- und Stromversorgung sowie die Informations- und Kommunikationstechnologie.

Hinzu kommt im Flugverkehr die Tatsache, dass schon kleine Störungen von flugbetriebskritischen Systemen ein erhöhtes Potenzial zur Gefährdung von Menschen und Umwelt haben können.

[1] https://www.uvek.admin.ch/dam/uvek/de/dokumente/dasuvek/kurzbericht-br-skyguide.pdf.download.pdf/Kurzbericht_DE%20des%20BR%20f%C3%BCr%20Skyguide.pdf, abgefragt am 30.08.2021

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, den Kantonen und der Privatwirtschaft 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. Die aktuelle NCS baut auf den Arbeiten der ersten auf, weitet diese wo nötig aus und ergänzt sie mit neuen Massnahmen, sodass sie der heutigen Bedrohungslage entspricht. Auch der in diesem Audit verwendete Standard (IKT-Minimalstandard) wurde im Rahmen der NCS erarbeitet.

1.3 Prüfungsziel und -fragen

Mit der Prüfung soll Skyguide aufgezeigt werden, wie sie hinsichtlich der Umsetzung der IKT-Sicherheitsanforderungen im Bereich der KI positioniert ist und wo es Verbesserungsbedarf gibt.

Die Prüffragen lauten:

1. Wird der Minimalstandard des BWL zur Verbesserung der IKT-Resilienz eingehalten?
2. Werden die Schnittstellen zu anderen Infrastrukturbetreibern sicher und kontrolliert betrieben?
3. Genügen die Vorgaben des Bundesamts für Zivilluftfahrt (BAZL), um die IKT-Sicherheitsstandards durchzusetzen?
4. Wurden die Empfehlungen 19120.001 und 19120.003 umgesetzt?

Diese Fragen fokussieren sich hauptsächlich auf die für den Flugbetrieb kritischen Systeme und Netzwerke. Die Anschlussnetze für Büroanwendungen und flugbetriebsnahe Systeme sind ausgeschlossen, sofern sie keine direkte und logische Verbindung zu den flugbetriebskritischen Systemen haben.

1.4 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf die Netze und die Infrastruktur von Skyguide.

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, die für das Funktionieren der KI ausschlaggebend 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, das ein Unternehmen umgesetzt hat:

0 Nicht umgesetzt

1 Partiell umgesetzt, nicht vollständig definiert und abgenommen

2 Partiell umgesetzt, vollständig definiert und abgenommen

3 Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch

4 Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert

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

Für die Prüfung hat die EFK den vom BWL über alle Branchen vorgeschlagenen Zielwert von 2.6 angewendet. Die EFK ist der Meinung, dass dieser Wert für einen Betreiber der Flugsicherung wie Skyguide bei 3 oder höher liegen sollte. Grundsätzlich müssten die einzelnen Themen mittels einer Risikoanalyse bewertet und danach die angestrebte Maturität je Thema definiert werden.

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

Die Prüfung wurde von Christian Brunner (Revisionsleiter) und Warren Paulus vom 5. Juli bis 3. September 2021 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Das Revisionsteam wurde durch eine externe Firma unterstützt. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.5 Unterlagen und Auskunftserteilung

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

1.6 Schlussbesprechung

Die Schlussbesprechung fand am 9. Dezember 2021 statt. Teilgenommen haben vonseiten Skyguide der Chief Technology Officer, der Head of Security, der Deputy Chief Safety Officer, der Head of Corporate Audit, der Head of CNS Services, der Head of IT Infrastructure Services und der Chief Information Architect. Seitens der EFK haben der zuständige Fachbereichsleiter und der Revisionsleiter teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Geschäftsleitung (GL) bzw. des Verwaltungsrats (VR) der Skyguide und für das BAZL der Amtsleitung bzw. dem Generalsekretariat obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Umsetzung IKT-Minimalstandard

Die Skyguide ist eine privatrechtliche Aktiengesellschaft, die im Auftrag und Eigentum der Schweizer Eidgenossenschaft für die Sicherheit des gesamten Luftraums der Schweiz sowie des angrenzenden Luftraumes tätig ist. Im Schweizer Luftraum umfasst dies sowohl die zivile als auch die militärische Flugsicherung, Letztere im Auftrag der Schweizer Luftwaffe. Die jährlich rund 1,3 Millionen zivilen und militärischen Flüge werden durch die 1500 Mitarbeitenden an 14 Standorten sicher und effizient durch einen der komplexesten Lufträume Europas geführt.[2]

Das Unternehmen untersteht der Aufsicht des BAZL. Hauptaktionärin (und einzige relevante Aktionärin) mit 99,94 Prozent der Anteile und 100 Prozent der Stimmrechte am Skyguide-Aktienkapital ist die Schweizerische Eidgenossenschaft.

2.1 Einschätzung der Maturität gemäss Framework

Die Skyguide wird im Bereich der Informationssicherheit durch das BAZL reguliert. Dieses erlässt in Zusammenarbeit mit internationalen Aviatik-Organisationen Regulationen und setzt diese durch. Für das durch die EFK durchgeführte Audit sind insbesondere der «ICAO Annex 17, Security Annex[3]» und von diesem Standard 4.9.1 die Recommendation 4.9.2 von Interesse. Diese beiden Bestimmungen umfassen die spezifischen regulatorischen Kontrollen hinsichtlich Informationssicherheit und sind seit dem 16. November 2018 gültig. Basierend auf dieser Regulation sowie dem «National Civil Aviation Security Programme» (NASP), Kapitel 19 des BAZL, werden regelmässig Audits bei Aviatik-Organisationen durchgeführt.

Die regulatorische Tätigkeit des BAZL bietet den Rahmen, in welchem sich Skyguide hinsichtlich Informationssicherheit bewegt und ist ein wesentlicher Treiber diverser informationssicherheitsrelevanter Arbeiten bei Skyguide. Die durch das BAZL angeordneten Massnahmen, gemeinsam mit den proaktiv durch die Skyguide initiierten Arbeiten, bilden im Wesentlichen die Grundlage für das bestehende Maturitätsniveau.

Als Gesamtfazit kann festgehalten werden, dass Skyguide die Themenbereiche des Minimalstandards systematisch bearbeitet. Das minimale Sicherheitsniveau, wie durch den IKT-Minimalstandard empfohlen, wird aktuell noch nicht vollständig erreicht. Jedoch sind durch die Audits des BAZL und die Proaktivität von Skyguide ein Grossteil der dazu noch notwendigen Arbeiten bereits identifiziert und angestossen. Im Rahmen des vorliegenden Audits hat die EFK zusätzliches Optimierungspotenzial erkannt.

[2] Webseite der Skyguide - https://www.skyguide.ch/de/company/ueber-skyguide/vision-mission/, abgefragt 26.08.2021

[3] https://www.bazl.admin.ch/dam/bazl/de/dokumente/Fachleute/Regulationen_und_Grundlagen/icao-annex/icao_annex_17_security.pdf.download.pdf/icao_annex_17_security.pdf, abgefragt am 30.08.2021

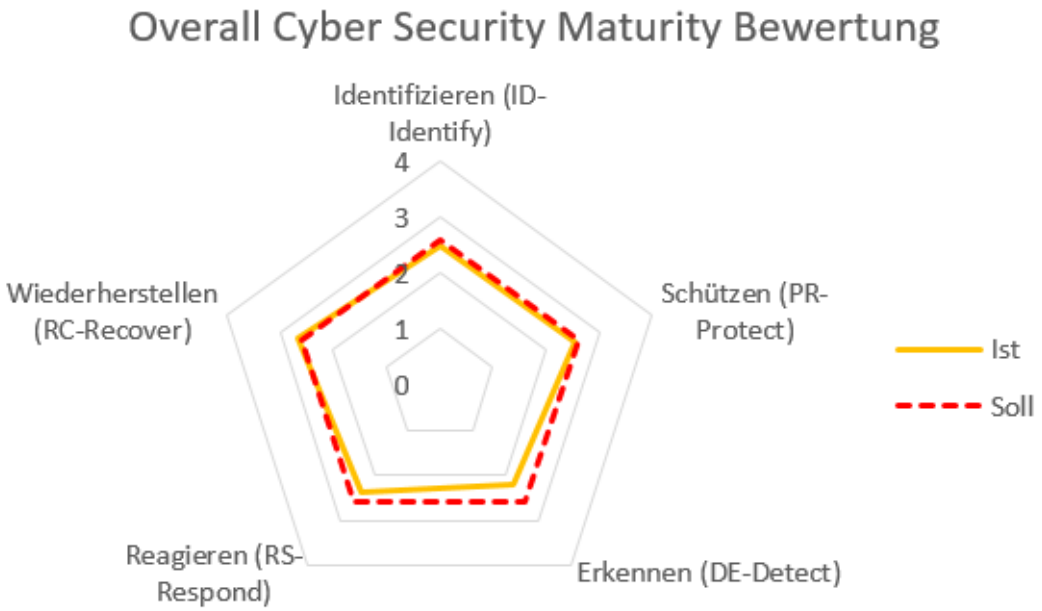


Abbildung 1: Auswertung über alle Prüfbereiche (Details siehe Anhang 4)

Beurteilung

Die Skyguide hat in den letzten Jahren eine Vielzahl von Sicherheitsmassnahmen neu priorisiert oder zusätzlich identifiziert. Zu den durch eigenes Sicherheitsbewusstsein und proaktiv angestossenen Massnahmen gehört die Verbesserung der Monitoring- und Reaktionsfähigkeiten durch ein Security Operation Center (SOC) sowie der Aufbau eines Computer Security Incident Response Team (CSIRT).

Zu den wichtigen durch das BAZL angeordneten Massnahmen gehören beispielsweise die Umsetzung eines gesamtorganisatorischen Information Security Management System (ISMS, engl. für «Managementsystem für Informationssicherheit») sowie ein noch stärkerer Fokus auf das Erstellen von Business-Continuity- und Disaster-Recovery-Plänen (BCP und DRP).

Da zum Prüfungszeitpunkt ein Grossteil der Sicherheitsmassnahmen noch nicht vollständig umgesetzt sind, entspricht das Maturitätsniveau noch nicht ganz den Anforderungen des IKT-Minimalstandards. Hinzu kommt, dass die Prüfung der EFK zusätzliche Schwachstellen identifiziert hat, welche Skyguide adressieren muss, bevor der IKT-Minimalstandard vollständig erreicht wird. Dazu gehören beispielsweise regelmässig durchgeführte Überprüfungen der vergebenen Benutzer-Berechtigungen sowie die Verbesserung des Schwachstellen- und Patch-Management-Prozesses.

Die EFK stellt jedoch fest, dass die angestossenen Arbeiten in die richtige Richtung gehen. Durch konsequentes Adressieren der erkannten Schwachstellen kann ein Maturitätsniveau erreicht werden, das deutlich oberhalb des Minimalniveaus liegt.

2.2 Das Informationssicherheitsmanagement muss gestärkt werden

Skyguide ist im Flugverkehr tätig, d. h. in einer komplexen und hochregulierten Branche mit hohen Sicherheitsanforderungen. Während in den letzten Jahrzehnten insbesondere der Sicherheitsaspekt (Safety, Vermeidung der Gefährdung von Mensch und Umwelt) im Vordergrund stand, gewinnt die Informationssicherheit aufgrund der grösseren Abhängigkeit von IKT-Systemen zunehmend an Gewicht. Letzterem wurde bei Skyguide zwar in gewissem Masse Rechnung getragen, jedoch nicht auf eine systematische Art und Weise. Um dies zu verbessern, hat das BAZL angeordnet, ein ISMS entsprechend den regulatorischen Vorgaben zu erstellen. Die Skyguide überprüft aktuell die eigenen Sicherheitsprozesse und -dokumente und erstellt ein solches ISMS. Zum Zeitpunkt des Audits waren diese Arbeiten noch nicht abgeschlossen.

Beurteilung

Ein ISMS ist ein grundlegender Baustein der Informationssicherheit und ermöglicht einen systematischen Ansatz hinsichtlich der Informationssicherheit. Skyguide verfügt über eine Vielzahl von aktualisierten und sicherheitsrelevanten Dokumenten. Zudem hat sie die entsprechenden Rollen, Verantwortlichkeiten und Sicherheitsprozesse grösstenteils definiert. Die durch das BAZL angeordneten und aktuell durch Skyguide ausgeführten Arbeiten zur Erstellung und Verbesserung ihres ISMS erscheinen sinnvoll und entsprechen den «best practices». Es gilt nun, diese Arbeiten fortzuführen und abzuschliessen.

2.3 Die Kontrolle über Zugriffsrechte muss erhöht werden

Skyguide verfügt über einen Prozess, um Mitarbeitenden Zugriffe auf die benötigten Applikationen und Daten zu gewähren. Insbesondere Arbeitsplatz- und Funktionswechsel sowie auch Abgänge können jedoch Änderungen bei den vergebenen Berechtigungen nach sich ziehen.

Skyguide gibt sich selbst die Einhaltung des Prinzips der geringsten Privilegien als Ziel vor. Dementsprechend soll ein Benutzer nur über jene Rechte verfügen, die er für die Ausübung seiner Arbeit zwingend benötigt. Diese Vorgabe entspricht einem «best practice»-Ansatz. Damit diese Vorgabe umgesetzt und auch überprüft werden kann, braucht es eine regelmässige Kontrolle der vergebenen Rechte. Skyguide überprüft dies jedoch weder bei seinen regulären Benutzern noch bei Systemadministratoren. Somit kann Skyguide nicht sicherstellen, dass Nutzer oder Administratoren tatsächlich nur über jene Rechte verfügen, welche für sie notwendig sind. Als Ausnahme muss hier DXC[4] erwähnt werden. Dieser ist ein wichtiger IT-Dienstleister von Skyguide, bei welchem entsprechende Access Reviews regelmässig stattfinden.

Beurteilung

Da keine regelmässige Überprüfung der Benutzerechte stattfindet, kann Skyguide das Einhalten des selbst vorgegebenen Ziels nicht sicherstellen. Es besteht somit keine Gewissheit, ob Benutzer oder Administratoren tatsächlich über die korrekten Rechte verfügen, oder ob diese zu umfangreich sind. Insbesondere hinsichtlich der Administratorenrechte stellt dies ein Risiko dar.

[4] https://dxc.com/

Da bei einem der externen Dienstleister die Kontrolle bereits durchgeführt wird, sollte dieser Prozess auch auf die restlichen Ressourcen adaptiert werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt Skyguide, eine regelmässige Überprüfung der vergebenen Rechte von allen Benutzern durchzuführen und entsprechend zu dokumentieren.

Die Empfehlung ist akzeptiert.

Stellungnahme Skyguide

Der existierende Prozess wird analysiert und entsprechend angepasst auf die restlichen Ressourcen ausgeweitet. Die Implementierung wird in Phasen stattfinden.

Systemadministratoren erhalten im Moment keine regelmässigen Schulungen betreffend IT-Sicherheit. So fehlt auch die Sensibilität dafür, dass mit weitreichenden Berechtigungen auch erhöhte Verantwortlichkeiten einhergehen.

Beurteilung

Eine Vielzahl von Angriffen zielt darauf ab, Schwachstellen bei regulären Nutzern auszunutzen und danach weitergehende Berechtigungen zu erlangen («privilege escalation» – Rechteausweitung). Erlangt ein Angreifer die Berechtigungen eines Systemadministrators, kann er oft auf weitere Systeme und Netze zugreifen.

Administratoren haben eine grosse Verantwortung, da mit ihren Rechten schlimmstenfalls sämtliche Systeme übernommen und unbemerkt Änderungen durchgeführt werden können. Deshalb ist es wichtig, das Thema IT-Sicherheit durch regelmässige Schulungen auf einem aktuellen Stand zu halten. Zusätzlich sollten entsprechende Verhaltensanweisungen definiert und eingeführt werden.

2.4 Eine konsequentere Behebung von Schwachstellen ist nötig

Zur Erfassung von technischen Verwundbarkeiten ihrer Hard- und Software verwendet Skyguide automatisierte Verwundbarkeitsanalysen. Aktuell werden Verwundbarkeiten identifiziert, jedoch werden diese weder bewertet noch systematisch und nachvollziehbar adressiert.

Skyguide verfügt derzeit über eine Liste, in welcher alle Verwundbarkeiten erfasst werden, eine qualitative Auswertung der Verwundbarkeiten findet aber nicht statt. Das bedeutet, dass keine Einteilung der Verwundbarkeiten entsprechend ihrer Kritikalität (z. B. kritisch, hoch, mittel, tief) gemacht wird. So kann auch keine Priorisierung der Behandlung der Schwachstellen vorgenommen werden. Es ist auch nicht geregelt, nach welchen Kriterien Verwundbarkeiten allenfalls akzeptiert und von der Verwundbarkeitsliste entfernt werden könnten.

Die Verwundbarkeiten werden nicht in einen systematischen und nachvollziehbaren Patchmanagement-Prozess zu deren Behebung überführt. Skyguide zählt auf die selbstmotivierte Umsetzung zum Beheben der entdeckten Verwundbarkeiten durch Entwickler und Applikationsverantwortliche. Der Prozess ist grundsätzlich vorhanden, wird jedoch nicht systematisch angestossen oder dessen Initiierung überprüft. Die Betroffenen und Beteiligten werden nicht im Umgang mit Verwundbarkeiten geschult. Auch besteht keine Vorgabe,

wie mit Verwundbarkeiten umzugehen ist und wie der Patchmanagement-Prozess konkret auszusehen hat.

Beurteilung

Die Implementierung der automatisierten Verwundbarkeitsanalysen ist ein sinnvoller Ansatz. Die Behebung der gefundenen Verwundbarkeiten ist jedoch unzureichend geregelt.

Es sollte eine Gesamtübersicht der vorhandenen Verwundbarkeiten erstellt und diese entsprechend kategorisiert werden. Danach muss definiert werden, in welcher Reihenfolge und Zeitdauer diese behoben werden sollen und wer die Umsetzung überprüft. Diese Vorgehensweise kann in den Patchmanagement-Prozess integriert werden und muss mit dem formellen Änderungsprozess abgestimmt sein.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt Skyguide sicherzustellen, dass alle erkannten Verwundbarkeiten, beispielsweise im Patchmanagement-Prozess, systematisch erfasst, priorisiert und behoben werden. Der Prozess soll auch eine Überprüfung der Umsetzung enthalten.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Die einzelnen Komponenten einer systematischen und priorisierten Erfassung und Behebung von Verwundbarkeiten sind gegeben. Diese werden im Zuge der Implementierung der automatisierten Verwundbarkeitsanalysen in den Patch-Management-Prozess integriert.

Nicht implementierte Änderung nach Anpassen der Vorgaben

Bei der Überprüfung der Firewall – Logs fand die EFK eine Verbindung, bei welcher eine veraltete kryptographische Hashfunktion konfiguriert war. Die EFK hat diese potenziell unsichere Einstellung mit den Vorgaben von Skyguide verglichen und festgestellt, dass dieser Hash nicht mehr zulässig war. Abklärungen haben ergeben, dass die Konfiguration der Verbindung 2017 erstellt wurde. Der Standard «Cryptographic Algorithms, Functions and Keys» der Skyguide wurde 2019 in Kraft gesetzt. Der Hash-Wert wurde noch während der Prüfung angepasst und die Verbindung wird in den nächsten Monaten abgebaut, da sie auf eine andere Plattform migriert wird.

Beurteilung

Die der EFK bei der Prüfung zur Verfügung gestellten Vorgaben befanden sich auf einem aktuellen Stand und werden regelmässig angepasst. Entsprechend ist es wichtig, sicherzustellen, dass Änderungen an Einstellungen oder Parametern nach Inkrafttreten von neuen Vorgaben auf den Systemen auch implementiert werden.

Gemäss Skyguide soll ein Prozess mithilfe des oben erwähnten Tools zur Verwundbarkeitsanalyse aufgebaut werden. Aus diesem Grund sieht die EFK von einer Empfehlung ab.

2.5 Fehlende Georedundanz für Luftverkehrsmanagement-relevante Server

Skyguide betreibt ihre Hardware für die Applikationen des Luftverkehrsmanagements, das sog. ATM (Air Traffic Management), nur an einem Standort. Zwar sind dort die Systeme virtualisiert in zweifacher Ausführung, also redundant vorhanden. Jedoch werden diese

Server nicht georedundant betrieben. Das bedeutet, dass wichtige Applikationen zur Flugsicherung, bei einem Brand im Rechenzentrum oder allfälliger Sabotage durch einen Innentäter, nicht mehr weiterbetrieben werden können. Eine vom Rechenzentrum geografisch abgesetzte Örtlichkeit zum Betrieb einer georedundant ausgerichteten Server-Infrastruktur steht nicht zur Verfügung.

Beurteilung

Der Betrieb von flugsicherungsrelevanten Servern und Applikationen ohne Georedundanz stellt ein erhöhtes Risiko hinsichtlich der Verfügbarkeit der Systeme dar. Durch ein lokales Ereignis könnte bereits der ganze Flugverkehr verunmöglicht werden. Georedundant ausgelegte Rechenzentren stellen eine wichtige Massnahme dar, um solche «Single Points of Failure» (SPOF) zu adressieren. Dadurch könnte Skyguide auch bei Sabotageakten oder physischen Einwirkungen ihre Kerndienstleistungen besser aufrechterhalten.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt Skyguide, eine georedundant ausgelegte Server-Infrastruktur zu prüfen und allenfalls umzusetzen.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Skyguide wird eine Georedundanz der flugsicherungsrelevanten Systeme im Zuge der geplanten Business- und Service-Continuity und abgestimmt mit der Virtual Center Philosophie (Ortsunabhängigkeit) einführen.

2.6 Das Corporate Risk Management sollte harmonisiert werden

Skyguide erhebt Risiken in unterschiedlicher Detaillierungsstufe. Auf Fachebene werden detaillierte und teilweise technische Risiken erfasst. Aktuell bestehen 16 unterschiedliche Risikoeinheiten (Risk Units), in welchen detaillierte Risiken in grosser Anzahl festgehalten werden. Auf Managementebene besteht ein übergeordnetes Risikomanagement, bei welchem die für das Unternehmen wichtigsten Risiken managementgerecht erfasst und dargestellt werden. Das übergeordnete Risikomanagement dient insbesondere zur Kommunikation an die Geschäftsleitung und an den Verwaltungsrat.

Die beiden Risikomanagement-Welten (Risk Units gegenüber dem übergeordneten Risikomanagement) sind aktuell nur beschränkt zusammen integriert. Informationen und Risiken aus den Risk Units finden ihren Weg nur beschränkt und nicht systematisch bis ins übergeordnete Risikomanagementregister. Durch die fehlende systematische Integration der beiden Risiko-Welten wird die Arbeit, die im Rahmen der Risk Units durchgeführt wird, nicht wirksam für die Organisation genutzt. Ein Link bestand vor der Reorganisation des Top Risk Managements.

Beurteilung

Zur Aggregierung der Risiken, die im Rahmen der Risk Units in das übergeordnete Risikomanagement erfasst werden, hat Skyguide keinen Prozess definiert. Aktuell besteht das Risikomanagement aus einer hohen Anzahl von Risk Units sowie zwei voneinander stark getrennten Risiko-Welten. Das erhöht die Komplexität betreffend Risikomanagement unnötig und kann dazu führen, dass Risiken nicht erkannt oder falsch priorisiert werden.

Im Rahmen einer Optimierung des Risikomanagements plant Skyguide die Anzahl von Risk Units zu verringern und einen Prozess zur systematischen Aggregation der Risiken im übergeordneten Risikomanagement zu etablieren. Aus diesem Grund sieht die EFK von einer Empfehlung ab.

2.7 Weitere Optimierung des Supply-Chain-Risikomanagements

Skyguide hat in den letzten Monaten eine Vielzahl von Massnahmen definiert und implementiert, um Risiken bei einem ihrer wichtigsten Dienstleister, DXC, zu adressieren. DXC stellt Dienstleistungen für die Hardwarebereitstellung und Wartung von flugverkehrsrelevanten Systemen zur Verfügung (z. B. Bereitstellung und Wartung der virtualisierten Infrastruktur für das Virtual Center[5], welches 2019 von der EFK geprüft wurde[6]).

Zu diesen Massnahmen gehören beispielsweise die dedizierte Ausbildung (Awareness-Training) von DXC-Mitarbeitenden bis hin zur Ausbildung von DXC-Security Champions. Die DXC-Mitarbeitenden erhalten erst nach der Ausbildung und dem Absolvieren einer Prüfung Zugriff auf die Systeme, die im Rechenzentrum der Skyguide stehen. Ausserdem werden die Zugriffsberechtigungen von DXC-Mitarbeitenden periodisch überprüft und es finden regelmässig Service Management Meetings statt (siehe auch Kapitel 2.3).

Trotzdem gab es in der letzten Zeit mehrere Vorfälle aufgrund von mangelhafter Kommunikation sowie unklarer Rollen und Verantwortlichkeiten zwischen DXC und Skyguide. Die Vorfälle konnten rasch wieder behoben werden, dennoch besteht die Gefahr, dass der Flugbetrieb und die Flugsicherheit durch solche Fehler beeinträchtigt werden.

Beurteilung

Skyguide ist sich der Wichtigkeit von DXC bewusst und hat entsprechende Massnahmen definiert. Das Vorgehen Security Champions vertieft auszubilden, welche dann ihrerseits die anderen DXC-Mitarbeitenden ausbilden, ist grundsätzlich zielführend. Das Problem ist jedoch, dass auf Seiten DXC relativ viele Mitarbeitende (Stand März 2021 waren 87 Accounts aktiv) involviert sind. Wie viele davon sich im Bereich der Luftverkehrsüberwachung wirklich auskennen, ist nicht klar. Entsprechend ist auch nicht sichergestellt, dass sich die involvierten Personen bewusst sind, was es für Auswirkungen auf den Flugbetrieb haben kann, wenn sie Wartungsarbeiten an einem System vornehmen. Deshalb ist es wichtig, genaue Regeln aufzustellen, wie und wann eine Änderung gemacht werden darf.

Das vergleichsweise hohe Maturitätsniveau betreffend Zusammenarbeit mit DXC wird in dieser Art nicht bei anderen, ebenfalls als kritisch eingestuften Lieferanten erreicht. Folglich besteht aktuell ein deutlicher Unterschied in der Adressierung von Supply-Chain-Risiken zwischen DXC und den anderen Lieferanten. Der neuentwickelte Ansatz im Umgang mit Lieferanten ist ein guter Ansatz. Dieser sollte bei den anderen kritischen Lieferanten nach Möglichkeit auch angewendet werden.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt Skyguide, die Zusammenarbeit mit DXC kontinuierlich zu überprüfen und gegebenenfalls anzupassen. Insbesondere der bestehende Change-Prozess bedingt klarere Absprachen.

[5] https://www.skyguide.ch/de/unternehmen/innovation/virtual-centre, abgefragt am 30.08.2021.
[6] Der Prüfbericht PA 19120 ist auf der Webseite der EFK abrufbar.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Die Zusammenarbeit mit DXC wird jährlich assessiert und Operationen kontinuierlich analysiert und entsprechend angepasst. Die Zusammenarbeit im Change-Prozess mit der DXC ist dabei ein Schwerpunkt und wird besonderer Bedeutung zugemessen. Mit der Einführung der kommenden Plattform Generation werden diese Prozesse überprüft und implementiert sein.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt Skyguide zu überprüfen, inwieweit die für DXC implementierten Sicherheitsmassnahmen auch bei weiteren kritischen Dienstleistern angewendet werden können.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Skyguide ist dabei, ihre Supply Management Organisation umzugestalten und ein Supplier Management System einzuführen. Im Zuge dieser Einführung werden die weiteren kritischen Dienstleister überprüft und die etablierten Sicherheitsmassnahmen bei der DXC gegebenfalls übernommen.

2.8 Fehlende Business-Continuity- und Disaster-Recovery-Pläne

Trotz erhöhtem Fokus auf die Zusammenarbeit mit dem Partner DXC bestehen aktuell keine spezifischen BCP oder DRP für die daraus resultierenden Risiken. Ein physischer Ausfall der Virtualisierungsinfrastruktur kann zu einem Ausfall von kritischen Anwendungen führen. Wenn ein System bei einer Störung ausgetauscht werden muss, wird DXC einen weiteren Partner beauftragen, dies vor Ort durchzuführen. Die Mitarbeitenden dieses Partners können nur in Begleitung und unter der Aufsicht von speziell ausgebildeten «Air Traffic Safety Electronics Personnel» (ATSEP) der Skyguide arbeiten.

Beurteilung

Trotz erhöhtem Fokus auf die Zusammenarbeit mit DXC besteht aktuell kein BCP oder DRP mit DXC. Ein physischer Ausfall der von DXC betreuten Virtualisierungsinfrastruktur bedingt eine enge Kooperation und klare Koordination zwischen drei Parteien (Skyguide, DXC und deren Partner). Die Zusammenarbeit mit zwei weiteren Parteien bei einem Vorfall erhöht die Komplexität erheblich und wird am besten durch einen DRP und/oder einem BCP geregelt.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt Skyguide, im Rahmen der geplanten Weiterentwicklung der Disaster-Recovery-Pläne (DRP) die Thematik der externen Dienstleister spezifisch zu regeln.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Vorschlag: Im Rahmen der aktuellen Entwicklung der Disaster-Recovery-Pläne (DRP) werden externe Dienstleister wie DXC ebenfalls miteinbezogen.

2.9 Das Service- und Security-Monitoring weist Optimierungspotenzial auf

Skyguide verfügt schon seit Längerem über eine historisch gewachsene Tool-Landschaft, um Services (bspw. Netzwerkdienste, Systemressourcen oder Anwendungsdienste) zu überwachen. Mit ihren Service Monitoring Tools überwacht Skyguide insbesondere die ATM-relevanten Prozesse und Systeme. Das System Monitoring & Control (SMC) Team ist dafür sogar physisch im Arbeitsbereich der «Air Traffic Controller» präsent und steht diesen als ständiger Ansprechpartner zur Verfügung. Für dieses Service-Monitoring nutzt Skyguide mehrere Werkzeuge unterschiedlicher Hersteller. Diese Monitoring-Tools decken mehr oder weniger dasselbe Monitoringspektrum ab und werden daher grösstenteils parallel verwendet. Die Resultate dieser Tools lassen sich nur mit entsprechendem Aufwand aggregieren. Das führt dazu, dass Skyguide hinsichtlich Service-Monitoring ineffizient unterwegs ist.

Neben dem Service-Monitoring betreibt Skyguide auch ein Security-Monitoring. Dieses stellt sicher, dass Angriffe und Anomalien erkannt und adressiert werden können. Die eingesetzten Tools scheinen in Anzahl und Umfang sinnvoll. Jedoch werden Resultate aus dem Service-Monitoring nicht durch Security Teams verwendet und das aktuell im Incident-Prozess als Dreh- und Angelpunkt fungierende SMC Team hat keinen Zugriff auf Informationen aus den Security Monitoring Tools.

Beurteilung

Aktuell betreibt die Skyguide zwei voneinander getrennte Monitoring-Umgebungen, die grundsätzlich ähnliche Arbeiten durchführen und voneinander profitieren könnten (Synergiepotenzial). Das Service-Monitoring, welches aktuell aus einer komplexen Tool-Landschaft besteht, verfügt über keinen direkten Zugriff auf Resultate aus dem Security-Monitoring. Auch umgekehrt fliessen Informationen aus dem Service-Monitoring lediglich beschränkt in das Security-Monitoring ein. Nur durch ein konsolidiertes Monitoring kann ein Gesamtbild aus allen verfügbaren Daten erstellt werden. Skyguide sollte die Tool-Landschaft weiter vereinheitlichen und mögliches Synergiepotenzial zwischen Service- und Security-Monitoring ausschöpfen.

2.10 Uneinheitliches Vorgehen beim Einsatz von kryptografischen Verfahren

Skyguide verfügt über keinen einheitlichen Ansatz betreffend den Einsatz von kryptografischen Verfahren. Obschon ein Klassifizierungskonzept besteht, das die Klassifizierung von

Daten vorgibt, gibt es keine entsprechende Weisung (Kryptokonzept), welche die Umsetzung vorgibt. So verwenden einige Mitarbeitende zertifikatsbasierte Verschlüsselung für E-Mails mit gewissen Kunden. Dies scheint jedoch ad hoc adressiert zu werden und ist nicht einheitlich geregelt. Auch die Verschlüsselung der gespeicherten Daten auf den Fileablagen ist nicht einheitlich geregelt.

Beurteilung

Die kryptografischen Verfahren spielen eine zentrale Rolle in der Sicherstellung der Vertraulichkeit und Integrität. Sie sichern Informationen während der Übertragung ab und schützen diese im Falle eines ungewollten Abflusses vor Missbrauch. Aktuell besteht bei der Skyguide keine einheitliche Herangehensweise in Bezug auf die Verwendung von kryptografischen Verfahren.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt Skyguide, einen systematischen Ansatz hinsichtlich der Verwendung von kryptografischen Verfahren umzusetzen. Dazu gehört das Erarbeiten einer Weisung zum Umgang mit kryptografischen Verfahren (Kryptokonzept) sowie die Sicherstellung der Anwendung (Umsetzung des Konzepts).

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Existierende Direktiven und Standards bezüglich der Anwendung kryptografischer Verfahren werden analysiert und – wo notwendig – ergänzt und angepasst. Basierend darauf werden ein Kryptokonzept sowie ein Plan für dessen Umsetzung ausgearbeitet.

2.11 Unklare Verantwortlichkeiten im Incident-Response-Prozess

Bedingt durch regulatorische Vorgaben verfügt Skyguide über drei wichtige Organisationsteile im Incident-Response-Prozess. Das SMC ist die zentrale Meldestelle für alle Arten von Vorfällen (neu auch Informationssicherheitsvorfälle), da es eine 24/7-Verfügbarkeit sicherstellt. Obschon das SMC durch Fachpersonen mit einer Informatik (oder verwandten) Ausbildung besetzt ist, werden Informationssicherheitsvorfälle grundsätzlich ohne Bearbeitung einfach weitergeleitet. Das SMC nimmt keine qualitative Einstufung eines Informationssicherheitsvorfalls vor. Tickets werden zuerst ans Team «TP Operational Bridge» weitergeleitet. Dieses besteht aus Personal, das im Sinne eines «second / third level supports», über vertiefte Kenntnisse der Systeme verfügt. TP Operational Bridge verfügt aktuell nur über eine beschränkte Spezialisierung hinsichtlich Informationssicherheit. Daher ist dieses Team unzureichend handlungsfähig und stark abhängig vom CSIRT. Ausserdem läuft der Incident-Prozess doppelspurig ab. Das heisst, das parallel zum oben beschriebenem Prozess, auch das CSIRT direkt informiert und allenfalls mit Handlungen beauftragt wird.

Beurteilung

Das Cyber Defense Center (CDC) der Skyguide (siehe Kapitel 2.12) und mit ihm das CSIRT sind neue Elemente, welche das Sicherheitsniveau positiv beeinflussen. Jedoch bedeuten diese neuen Elemente auch, dass der Incident-Response-Prozess entsprechend angepasst und die Verantwortlichkeiten überdacht werden müssen. Das ist noch nicht geschehen und sorgt für Doppelspurigkeiten und Effizienzverlust. Zudem müssten die Leute von TP Operational Bridge im Umgang mit Informationssicherheitsvorfällen geschult werden.

Empfehlung 8 (Priorität 2)

Die EFK empfiehlt Skyguide, die Rollen und Verantwortlichkeiten des SMC, TP Operational Bridge und CSIRT sowie deren Zusammenarbeit im Rahmen des Incident-Response-Prozesses zu bereinigen.

Die Empfehlung ist akzeptiert.

Stellungnahme der Skyguide

Der Incident-Response-Prozess wird analysiert und einer höheren Effizienz folgend entsprechend angepasst und kontinuierlich weiterentwickelt.

2.12 Die Implementierung des Cyber Defense Centers ist noch nicht abgeschlossen

Skyguide hat sich entschlossen, ihr Sicherheitsniveau hinsichtlich Erkennung von Vorfällen und Reaktion bei Eintreten durch ein CDC deutlich zu erhöhen. Das CDC stellt dabei eigentliche SOC-Leistungen zur Verfügung. Das bedeutet, dass Logs zentral gesammelt, Use Cases und Monitoring Rulesets ausgewertet und allenfalls eine Alarmierung sichergestellt wird. Ausserdem wurde durch das CDC auch die Reaktionsfähigkeit gesteigert, indem für bestimmte Vorfälle «Playbooks» erstellt wurden. Durch Letztere sind Handlungsabläufe (z. B. Eingrenzung) vorgegeben, können geübt und somit bei einem Vorfall effizient eingesetzt werden. Zum Zeitpunkt der Prüfung waren jedoch einige Vorhaben noch nicht abgeschlossen:

- Die Agenten zum Sammeln der Logs sind noch nicht vollständig ausgerollt (z. B. in der Air-Navigation-Services-Welt);
- Das Incident-Reporting geschieht noch auf zwei unterschiedlichen Systemen. Deren Integration steht noch aus;
- Wichtige Informationen werden im Incident-Reporting nicht festgehalten (z. B. der Inhalt von Telefongesprächen). Damit ist nicht nachvollziehbar, welche Entscheidungen getroffen wurden;
- Daten aus dem Schwachstellen-Management werden nicht verwendet;
- Es besteht erst eine beschränkte Anzahl an Playbooks (z. B. kein Unternehmensweites Szenario einer Ransomware-Attacke);
- TP Operational Bridge wird nicht in die Erarbeitung der Playbooks einbezogen (dadurch potenziell fehlende Expertise betreffend Business Impact oder unvollständige Liste der betroffenen Systeme);
- Die geplante Data Loss / Leakage Prevention (DLP) Plattform ist noch nicht aktiv;
- Die Use Cases und das Monitoring Ruleset werden noch nicht systematisch überprüft.

Beurteilung

Das CDC der Skyguide ist ein neues Element, welches das Sicherheitsniveau weiter anheben wird. Grundsätzlich gehen die Arbeiten in die richtige Richtung, jedoch befindet sich das CDC, gemäss der Roadmap, noch im Aufbau und einige Elemente wurden noch nicht umgesetzt. Die aufgeführten Punkte sind entweder in der Roadmap des CDC oder in zusätzlichen Projekten (z. B. Evaluation der DLP-Plattform) adressiert.

Aufgrund des geplanten Vorgehens der Skyguide verzichtet die EFK auf eine Empfehlung.

2.13 Schnittstellen zu externen Partnern sind bekannt und werden kontrolliert betrieben

Die Schnittstellen zu externen Partnern sind bekannt und die relevanten Datenströme im Architektur- sowie Incidentmanagement-Tool erfasst. Externe Verbindungen werden systematisch adressiert und via einheitlicher Architektur aufgeschaltet. Die Verbindungen werden jeweils auf einem Firewall-Cluster terminiert.

Zugriffe von extern werden immer auf einem Sicherheitsgateway (Jumphost, Firewall…) terminiert. Sämtliche Zugriffe von externen Partnern werden mittels «Session Recording» aufgezeichnet. Zudem findet der externe Zugriff immer mittels Zwei-Faktor-Authentisierung statt.

Beurteilung

Die Verbindungen zu externen Netzwerken sind bekannt, dokumentiert und werden systematisch behandelt. Zugriffe werden via Zwei-Faktor-Authentisierung auf spezialisierte Systeme gemacht, auf welchen sie terminiert werden, und sind entsprechend gut abgesichert. Zudem kann mittels dem «Session Recording» nachvollzogen werden, was für Änderungen durchgeführt wurden.

3 Vorgaben des Bundesamts für Zivilluftfahrt

Die Vorgaben des BAZL sind geprägt durch internationale und europäische Bestimmungen:

International

Der ICAO Annex 17 Security beinhaltet seit November 2018 einen Standard 4.9.1 und eine Recommendation 4.9.2 betreffend Cyber Security. Diese sind in der Schweiz anwendbar und bilden die Grundlage für Kapitel 19 des NASP.

Der «Global Aviation Safety Plan» (GASP) der Internationalen Zivilluftfahrtorganisation, International Civil Aviation Organisation (ICAO), legt globale Sicherheitsziele sowie Vorgaben zu deren Umsetzung fest (siehe Kapitel 2.1).

Die ICAO hat im Oktober 2019 zudem eine «Aviation Cybersecurity Stategy» publiziert, welche von einem Action Plan begleitet wird.

Auch anlässlich der ICAO Assembly, welche alle drei Jahre stattfindet, wird das Thema Cyber Security in den Resolutions thematisiert.

Europa

Auf europäischer Ebene sind die Ziele des GASP im European Aviation Safety Programm (EASP) sowie im dazugehörigen European Plan for Aviation Safety (EPAS) berücksichtigt. Auch auf europäischer Ebene wurde im September 2019 eine «Strategy for Cybersecurity in Aviation» erstellt.

National

Das BAZL erstellt das Nationale Sicherheitsprogramm Luftfahrt, «National Aviation Security Programme (NASP)», mittels welchem Schutzmassnahmen gegen äussere Bedrohungen wie Flugzeugentführungen, Sabotageakte oder Terrorangriffe erlassen werden. Das NASP ist vertraulich klassifiziert und wird nicht veröffentlicht. Es wird gemäss dem «need-to-know»-Prinzip den relevanten Akteuren zugestellt. Die Vorgaben betreffend Cyber Security Massnahmen, inkl. Koordination zwischen Safety und Security sind im Kapitel 19 «Cyber Threats to Civil Aviation» ausgeführt.

Parallel zum NASP beschreibt das State Safety Programm (SSP) auf nationaler Ebene die Strategie des Sicherheitsmanagementsystems der Schweizer Zivilluftfahrt. Es enthält die Sicherheitspolitik sowie auf höchster Ebene eine Beschreibung des gesetzlichen Hintergrundes, Prozesse und Massnahmen. Die Umsetzung dieser nationalen Strategie ist im Swiss Aviation Safety Plan (SASP) definiert.

In der Schweiz müssen diverse Akteure im Flugverkehr, inkl. Skyguide, das Kapitel 19 des NASP erfüllen. Dieses wird laufend angepasst. Zum Beispiel wurde die Meldepflicht verschärft. Die Organisationen müssen bei einem Cyberangriff mit potentiellem Effekt auf die Sicherheit der Luftfahrt seit dem 1. September 2021 das BAZL sofort informieren, und ihm innerhalb von 72 Stunden einen Rapport zustellen. Zudem hat das BAZL ein Hilfsdokument «NASP Kapitel 19 - IT Security Guidance» erstellt in welchem die Beurteilungskriterien zum Erfüllen des Standards beschrieben sind.

Beurteilung

Der ICAO-Annex 17, Security Standard (siehe Kapitel 2.1) ist sehr generisch gehalten und gibt keine konkreten Vorgaben, wie die IT-Sicherheit umgesetzt werden soll.

Das BAZL spezifiziert deshalb im NASP-Kapitel 19 konkrete Vorgaben was erwartet wird und bietet insbesondere im Zusatzdokument «IT-Security-Guidance» konkrete Anhaltspunkte, wie diese umgesetzt werden können. Die Vorgaben werden regelmässig angepasst und aktualisiert (letzte Anpassung im Frühjahr 2021, für IKT 1.9.2021) und sind zielführend.

Das BAZL ist eine treibende Kraft im Bereich der Cyber Security im Flugverkehr, dies insbesondere auf ICAO-Ebene, wo es Inputs geben und die Umsetzung beeinflussen kann.

Im Falle von Skyguide konnte die IT-Sicherheit durch die Vorgaben und die durchgeführten Audits des BAZL deutlich erhöht werden.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2021), SR 614.0
Verordnung über den Flugdienst beim Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation vom 4. Oktober 1999 (Stand am 1. Juli 2008), SR 172.217.2
Verordnung vom 17. Dezember 2014 über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV) (Stand: 1. Februar 2015), SR 742.161
Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG) vom 17. Juni 2016 (Stand am 1. Januar 2020), SR 531
Luftrecht Schweiz
Bundesgesetz über die Luftfahrt vom 21. Dezember 1948 (Stand am 1. Januar 2021), SR 748.0
Verordnungen 748.x: https://www.fedlex.admin.ch/de/cc/internal-law/74
Staatsverträge (SR 0.748)
Circa 180 bilaterale und multilaterale Staatsverträge: https://www.fedlex.admin.ch/de/cc/international-law/0.74#0.748
Bilaterales Luftverkehrsabkommen Schweiz-EG
Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr, abgeschlossen am 21. Juni 1999 (Stand am 1. Juli 2020), SR 0.748.127.192.68
International Civil Aviation Organisation (ICAO[7])
Übereinkommen über die internationale Zivilluftfahrt (Chicago Convention) in Kraft getreten für die Schweiz am 4. April 1947 (Stand am 18. Juni 2019), SR 0.748.0
ICAO Annex 17, Security (PDF, 4 MB, 30.12.2020)[8]

[7] https://www.icao.int/Pages/default.aspx, abgefragt am 30.08.2021

[8] https://www.bazl.admin.ch/bazl/de/home/fachleute/regulation-und-grundlagen/rechtliche-grundlagen-und-richtlinien/anhaenge-zur-konvention-der-internationalen-zivilluftfahrtorgani.html, abgefragt am 30.08.2021

Weitere Dokumente
NATIONAL CIVIL AVIATION SECURITY PROGRAMME (NASP) 11th Electronic Edition (CONFIDENTIAL): Kapitel 19 - Cyber Threats to Civil Aviation.pdf
NASP Kapitel 19 – IT Security Guidance

Anhang 2: Abkürzungen

ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
ATSEP	Air Traffic Safety Electronics Personnel
BAZL	Bundesamt für Zivilluftfahrt
BCP	Business Continuity Plan
BR	Bundesrat
BWL	Bundesamt für wirtschaftliche Landesversorgung
CDC	Cyber Defense Center
CSIRT	Computer Security Incident Response Team
DLP	Data Loss / Leakage Prevention
DRP	Disaster Recovery Plan
EASP	European Aviation Safety Programm
EFK	Eidgenössische Finanzkontrolle
EPAS	European Plan for Aviation Safety
GASP	Global Aviation Safety Plan
ICAO	International Civil Aviation Organisation
IKT	Informations- und Kommunikationstechnik
ISMS	Information Security Management System
IT	Informationstechnologie
KI	Kritische Infrastruktur
NASP	National Civil Aviation Security Programme
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
SASP	Swiss Aviation Safety Plan
SKI	Schutz der kritischen Infrastrukturen

SMC	System Monitoring & Control
SOC	Security Operation Center
SPOF	Single Point of Failure
SSP	State Safety Programm
VC	Virtual Centre[9]

[9] https://www.skyguide.ch/company/innovation/virtual-centre, abgefragt am 30.08.2021

Anhang 3: Glossar

HERMES	eCH-0054: HERMES Projektmanagement-Methode HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung.
Air Traffic Management (ATM)	Flugverkehrsmanagement dient der Sicherstellung einer sicheren und effizienten Bewegung von Luftfahrzeugen während allen Phasen ihres Betriebes (Start, Flug, Landung).
BCP	Der Business Continuity Plan umfasst eine detaillierte Strategie und alle relevanten Systemen, mit welchen ein Unternehmen Unterbrechungen des Betriebs verhindern oder notfalls eine schnelle Wiederherstellung durchführen kann. Der Plan ist im Wesentlichen ein Leitfaden dafür, wie Organisationen ihr Tagesgeschäft während des Ereignisses und unmittelbar danach weiterführen können.
Confluence	Confluence ist eine kommerzielle Wiki-Software, die vom australischen Unternehmen Atlassian entwickelt und als Enterprise Wiki hauptsächlich für die Dokumentation und Kommunikation von Wissen und den Wissensaustausch in Unternehmen und Organisationen verwendet wird.
CSIRT	Im Computer Security Incident Response Team arbeiten qualifizierte Spezialisten aus verschiedenen Fachgebieten, mit dem Ziel, IT-Sicherheitsvorfälle zu identifizieren, einzudämmen und den Normalbetrieb wiederherzustellen.
DLP	Data Loss / Leakage Prevention hat das Ziel, den unerwünschten Abfluss von sensiblen Daten zu entdecken oder zu verhindern.
DRP	Der Disaster Recovery Plan geht von der Unterbrechung des normalen Geschäftsbetriebs durch Ereignisse wie Stromausfälle, Naturkatastrophen oder schlicht menschliches Versagen aus. Bei der Wiederherstellung im Katastrophenfall geht es darum, wie man nach dem Ereignis reagiert und wieder in den normalen Betrieb zurückkehrt.
Firewall	Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten externen Netzwerkzugriffen schützt.

Georedundanz	Einsatz von zwei oder mehreren vollständig funktionsfähigen Rechenzentren an geografisch unterschiedlichen Standorten.
Hash	Hashing bezeichnet die Umwandlung einer Zeichenfolge in einen normalerweise kürzeren, numerischen Wert oder Schlüssel mit fester Länge. Der numerische Wert ist der Hashwert und eine andere Darstellung der ursprünglichen Zeichenfolge. Hashing wird in vielen Verschlüsselungsalgorithmen verwendet. Ein Passwort wird beispielsweise ebenfalls als Hashwert anstelle des Klarwertes in der Datenbank abgespeichert.
ISMS	Verfahren und Vorgaben innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.
Jira	Jira ist eine Webanwendung zur Fehlerverwaltung, Problembehandlung und zum operativen Projektmanagement, die von Atlassian entwickelt wurde. Typische Anwendungsfälle sind dabei Aufgabenmanagement, Anforderungsmanagement und Workflow-Management.
Jumphost	Ein Jumphost ist ein System in einem Netzwerk, das für den Zugriff und die Verwaltung von Geräten in einer separaten Sicherheitszone verwendet wird. Es ist ein gehärtetes und überwachtes System, das zwei unterschiedliche Sicherheitszonen überspannt, und einen kontrollierten Zugang zwischen ihnen ermöglicht.
Kritische Infrastruktur	Als KI werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.
ISO 2700x	Die ISO/IEC 27000-Reihe ist eine Sammlung von Standards zur Informationssicherheit. Herausgegeben werden die über 20 Normen von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).
Logging	Automatische Erstellung eines Protokolls von Softwareprozessen
Patchmanagement	Prozess zur Verteilung und Durchführung von Updates für Software. Solche Patches sind oftmals notwendig, um Fehler in der Software (auch als «Schwachstellen» oder «Bugs» bezeichnet) zu beheben.
Playbook	Leitfaden um Rollen und Verantwortlichkeiten für das Verhindern von und die Reaktion auf sicherheitsrelevante Vorfälle festzulegen.

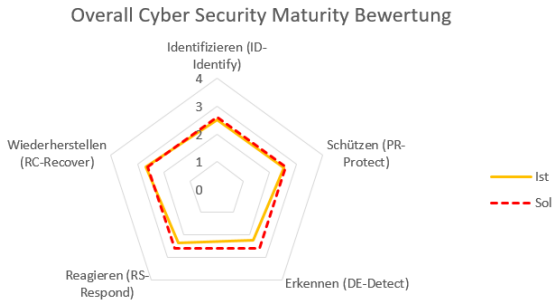
Principle of least privilege	Der Benutzer soll nur über die Zugriffsrechte verfügen, die er zur Ausübung seiner Funktion oder Rolle unbedingt braucht.
Privilege escalation	Beschreibt eine Angriffsmethode, bei der sich ein Angreifer, nachdem er auf dem Rechner oder Server eines Opfers eingebrochen ist, umfassendere Rechte beschafft. Das Ziel ist es durch Privilege-Escalation Administrator- bzw. Root-Rechte zu erlangen um den Angriff auf weiteren Systemen fortzusetzen.
Ransomware	Erpressungssoftware oder Verschlüsselungstrojaner sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff auf die Daten eines Computers verunmöglicht.
Safety / Security	Unter Aviation-Security versteht man in der zivilen Luftfahrt alle Schutzmassnahmen zur Abwehr von äusseren Gefahren wie Flugzeugentführungen, Sabotageakte und Terrorangriffe. Unter Aviation-Safety versteht man alle Massnahmen zur Gewährleistung der technischen und operationellen Verlässlichkeit aller Beteiligten der Zivilluftfahrt.
SOC	Das Security Operations Center überwacht die IT-Infrastruktur rund um die Uhr gegen Cyberbedrohungen. Durch die permanente Überwachung sowie präventive Massnahmen gegen Cyberbedrohungen garantiert das SOC die Verfügbarkeit und Sicherheit des Firmennetzwerkes, inklusive der geschäftskritischen Applikationen.

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).

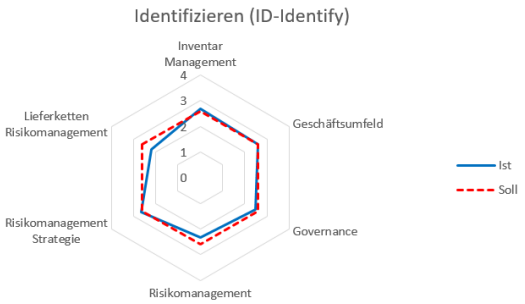
Anhang 4: Auswertung Skyguide

Übersicht:

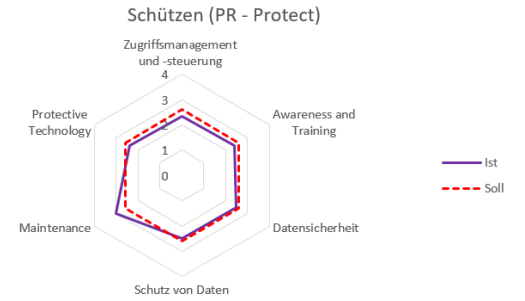


Overall Cyber Security Maturity	Ist	Soll
Identifizieren (ID-Identify)	2.5	2.6
Schützen (PR-Protect)	2.5	2.6
Detektieren (DE-Detect)	2.2	2.6
Reagieren (RS-Respond)	2.4	2.6
Wiederherstellen (RC-Recover)	2.7	2.6

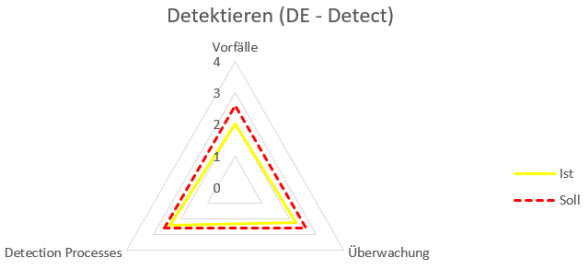
Die fünf Prüffelder im Detail:



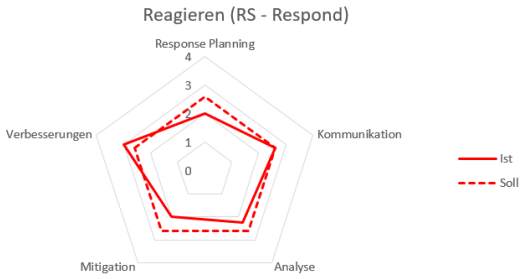
Empfehlung 6,7,8,9



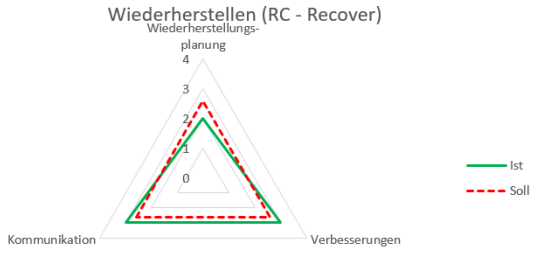
Empfehlung 1,2,5,10,11



Empfehlung 3,4



Empfehlung 5,12



Empfehlung 7

Anhang 5: Follow-up ausgewählter Empfehlungen PA 19120 Skyguide Virtual-Center

Nr.	Empfehlung	Feststellungen	Status
001	Die EFK empfiehlt Skyguide, die Funktion des Programm-Risikomanagers einer anderen Person als dem Leiter des VCT2 zu übertragen. Diese Person sollte direkt an den Programmverantwortlichen berichten. Die Funktion kann auch von einem Fachmann von außerhalb des Unternehmens übernommen werden.	Der Program Owner von VCT ist der Chief Technology Officer, und entsprechend Vorgesetzter vom Program Manager für VCT. Der Vertreter des Enterprise Risk Managements ist dem Chief Safety Officer, unterstellt. Entsprechend ist eine unabhängige Erfassung und Bearbeitung der Risiken gewährleistet.	Umgesetzt
003	Die EFK empfiehlt Skyguide, wirksamere Instrumente zur Einbindung der Informationssicherheitsaspekte von VCT2 einzusetzen. Die Informationssicherheitsrisiken des Programms sollten neu bewertet werden. Es sollte ein Informationsschutzkonzept und ein Umsetzungsplan definiert werden.	Die IT-Sicherheit ist mittlerweile fester Bestandteil bei den Steering Comitee Meetings, welche regelmässig stattfinden. Die Informationssicherheitsrisiken werden laufend beurteilt. Bei der Serviceorientierten Architektur wird die Sicherheit bereits in der Designphase angeschaut. Neue Systeme müssen entsprechend vorgegebener Informationssicherheitsprinzipien implementiert und dokumentiert werden. Es ist ein jährliches Budget für IT-Sicherheit fest eingeplant und es werden entsprechende Priorisierungen vorgenommen. Die geplanten und umgesetzten Massnahmen sind in Jira oder Confluence erfasst und werden überwacht. Es wurden in fünf von acht agilen Teams Mitarbeitende zu «Security Champions» ausgebildet, welche die Einhaltung von IT-Sicherheitsvorschriften in ihrem Bereich durchsetzen und kontrollieren. Ziel ist es, in jedem Bereich «Security Champions» zu etablieren.	Umgesetzt