[redacted]

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

Prüfung der Informatiksicherheit

Führungsunterstützungsbasis

EFK-19364 | inkl. Stellungnahme | 2. März 2020

Inhaltsverzeichnis

Prüfung der Informatiksicherheit
Führungsunterstützungsbasis

Das Wesentliche in Kürze

Die Führungsunterstützungsbasis (FUB) stellt robuste, hochsichere Informations- und Kommunikationstechnologie (IKT)-Leistungen und elektronische Operationen für die Armee in allen Lagen zur Verfügung. Als Leistungserbringer (LE) des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) ist sie für die Bereitstellung und den Betrieb der Büroautomation, Fachanwendungen sowie Informations- und Kommunikationssysteme im Departement zuständig.

Im Juli 2017 konnte ein Cyber-Angriff auf einzelne Server des VBS erkannt und gestoppt werden. Der Angriff wurde nach einem weitgehend bekannten Muster der Malwarefamilie Turla verübt. Im Nachgang zu diesem Vorfall beauftragte die FUB im Winter 2017 und im Frühjahr 2018 eine Drittfirma mit Analysen und Tests zum Führungsnetz Schweiz (Fhr Netz CH)[1]. Die Resultate zeigten, dass das Sicherheitsniveau nicht den Anforderungen eines militärischen Leistungserbringers genügte. Daher wurden elf Massnahmen zur kurzfristigen Verbesserung definiert, welche im Rahmen des Projektes [redacted] bis Ende März 2019 implementiert oder zumindest entscheidend eingeleitet sind.

Ergebnisse aus dem Projekt [redacted] sind vorwiegend konzeptueller Natur

Die angeordneten Massnahmen waren grundsätzlich zielführend. Das Projekt ist seit April 2019 abgeschlossen. Verschiedene Arbeitspakete wurden für die Implementation in Folgeprojekte oder in die betriebliche Organisation überführt. Die vorliegenden Ergebnisse sind vorwiegend konzeptueller Natur und erreichten noch wenige unmittelbare operative Verbesserungen der IKT-Sicherheit. Insbesondere die Verwaltung der IKT-Assets ist zum Prüfzeitpunkt nicht vollständig. [redacted] Mit dem Projekt konnte bei den Mitarbeitenden der FUB primär eine bessere Sensibilisierung für die Aspekte der IKT-Sicherheit geschaffen werden.

Trotz Verbesserungen bei der IT-Security-Governance besteht noch Handlungsbedarf

Die neue Sicherheitsorganisation der FUB ist zielführend definiert, es bestehen aber noch einige Vakanzen, welche für eine operative Umsetzung so schnell wie möglich besetzt werden sollten. Mit der Schaffung der Stelle eines Chief Information Security Officer (CISO) auf Ebene Geschäftsleitung hat die FUB einen wichtigen Schritt gemacht. Das Information Security Management System (ISMS) stellt eine adäquate Basis zur Behandlung der Assets und deren Risiken dar, ist aber noch nicht in der nötigen Tiefe aufgebaut. Der Prozess zur Bearbeitung von Ereignissen ist grundsätzlich zweckmässig aufgebaut und nachvollziehbar. [redacted] Eine detaillierte mittelfristige Planung ist in Arbeit.

[1] [redacted]

IKT-Grundschutzanforderungen sind nicht flächendeckend erfüllt

Am 5. November 2018 informierte das VBS mit einer Informationsnotiz den Bundesrat über den oben erwähnten Sicherheitsvorfall. Das VBS hielt darin fest, das Sicherheitsniveau der FUB habe den Anforderungen an einen militärischen Leistungserbringer nicht genügt, dass aber die Anforderungen des IKT-Grundschutzes eingehalten worden seien. Die EFK kommt in der vorliegenden Prüfung zum Schluss, dass die Vorgaben aus dem IKT-Grundschutz gemäss den Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) Art. 3.2, bei der FUB nicht flächendeckend umgesetzt sind. In unterschiedlichen Bereichen [redacted] werden die Minimalvorgaben des Informatiksteuerungsorgans des Bundes nicht eingehalten. Ausnahmegenehmigungen zu diesen Unterschreitungen liegen nicht vor.

[redacted]

Eine nachhaltige Verbesserung der Situation benötigt Zeit und Ressourcen

[redacted] Mit dem Aufbau des Programms FITANIA (Fhr Netz CH, RZ2020, TK A) soll stattdessen eine neue, von Anfang an sichere und zukunftsgerichtet verwaltete Netzwerkumgebung aufgebaut werden. In der Folge sollten die bestehenden Anwendungen auf dieses neue Netz überführt werden. Das von der FUB beschlossene Vorgehen erscheint grundsätzlich zielführend, aber steht im Widerspruch zum Bundesratsbeschluss vom 23. März 2016. [redacted]

Nach einer sofortigen Orientierung der Departementschefin, hat die EFK am 13. Dezember 2019 den ganzen Bundesrat über diese festgestellten Mängel von grundsätzlicher Bedeutung gemäss Artikel 15 Absatz 3 FKG informiert.

Audit de la sécurité informatique
Base d'aide au commandement

L'essentiel en bref

La Base d'aide au commandement (BAC) fournit à l'armée des prestations solides et hautement sécurisées dans les domaines des technologies de l'information et de la communication et des opérations électroniques en toute situation. En tant que fournisseur de prestations du Département fédéral de la défense, de la protection de la population et des sports (DDPS), elle est responsable de la mise à disposition et de l'exploitation de la bureautique, des applications spécifiques ainsi que des systèmes d'information et de communication du département.

En juin 2017, une cyberattaque visant certains serveurs du DDPS a pu être détectée et stoppée. Elle avait été menée selon un schéma connu utilisé par les maliciels de la famille Turla. À la suite de cet incident, la BAC a chargé une entreprise tierce, en hiver 2017 et au printemps 2018, de procéder à des analyses et à des tests sur le réseau de conduite suisse[1]. Les résultats ont montré que le niveau de sécurité ne répondait pas aux exigences posées à un prestataire militaire. Ainsi, onze mesures d'amélioration à court terme ont été définies qui devaient être mises en œuvre ou, du moins, bien engagées dans le cadre du projet [redacted] avant la fin de mars 2019.

Les résultats du projet [redacted] sont d'ordre principalement conceptuel

Les mesures ordonnées se sont montrées efficaces. Le projet a été achevé en avril 2019. Divers groupes de tâches ont été transférés dans des projets de suivi ou dans l'organisation opérationnelle en vue de leur mise en œuvre. Les résultats obtenus portent surtout sur la conception et n'ont atteint que peu d'améliorations opérationnelles immédiates de la sécurité informatique. En particulier la gestion des actifs informatiques était incomplète au moment de l'audit. [redacted] Le projet a surtout permis de sensibiliser davantage les collaborateurs et collaboratrices de la BAC aux aspects de sécurité informatique.

Malgré des améliorations en matière de gouvernance de la sécurité informatique, des mesures sont encore nécessaires

La nouvelle organisation de sécurité de la BAC est définie de manière judicieuse, mais plusieurs postes vacants devraient être pourvus le plus rapidement possible pour une mise en œuvre opérationnelle. La BAC a franchi une étape importante en créant un poste de Chief Information Security Officer (CISO) au niveau de la direction. Le système de gestion de la sécurité de l'information (Information Security Management System, ISMS) constitue une base adéquate pour le traitement des actifs et de leurs risques, mais il n'est pas encore assez développé. Le processus de traitement des événements est clair et bien structuré. [redacted]

[1] [redacted]

[redacted]

Une planification détaillée à moyen terme est en cours d'élaboration.

Les exigences en termes de protection informatique de base ne sont pas pleinement remplies

Le 5 novembre 2018, le DDPS a informé le Conseil fédéral de l'incident de sécurité mentionné plus haut. Dans sa note d'information, il soulignait que le niveau de sécurité de la BAC ne répondait pas aux exigences posées à un prestataire militaire, mais que les exigences en matière de protection informatique de base avaient été respectées. Dans le présent audit, le CDF arrive à la conclusion que la BAC ne remplit pas entièrement les exigences découlant de l'art. 3.2 des directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale. Dans divers domaines [redacted], les directives minimales de l'Unité de pilotage informatique de la Confédération (UPIC) ne sont pas respectées alors qu'aucune dérogation n'a été accordée dans ce sens.

[redacted]

Une amélioration durable nécessite du temps et des ressources

[redacted] Avec le programme « FITANIA » en lieu et place (réseau de conduite suisse, centre de calcul 2020, télécommunications de l'armée), un nouvel environnement de réseau sécurisé doit être créé dès le début avec une gestion tournée vers l'avenir. Les applications existantes devraient ultérieurement être transférées sur ce nouveau réseau. La procédure décidée par la BAC semble en principe efficace, mais va à l'encontre de la décision du Conseil fédéral du 23 mars 2016. [redacted]

Après avoir informé immédiatement la cheffe du DDPS, le CDF a instruit, le 13 décembre 2019, l'ensemble du Conseil fédéral de ces manquements ayant une portée fondamentale, conformément à l'art. 15, al. 3, de la Loi sur le Contrôle des finances.

Texte original en allemand

Generelle Stellungnahme der Geprüften

Stellungnahme VBS:

Wir danken für die Möglichkeit der Stellungnahme und schliessen uns der Stellungnahme der FUB an. Diese Prüfung, die dazugehörenden Dokumente inkl. Schlussbericht sollen vertraulich deklariert und entsprechend behandelt werden.

Stellungnahme FUB:

Gerne nutzen wir die Möglichkeit zur Stellungname zum Thema «Prüfung der Informatiksicherheit» mit dem Prüfungsziel «Beurteilung der Massnahmenumsetzung in den Bereichen Netzwerksicherheit und Firewall», konzentriert auf die Sicherheitsaspekte des Führungsnetzes Schweiz.

Die Schweizer Armee verfügt über eine sehr heterogene, historisch gewachsene IKT-Infrastruktur. Gewisse Technologien, die heute noch im Einsatz sind, lassen sich auf die 1950er Jahre zurückdatieren. Die Menschen, die die Grundsteine legten für die IKT-Systeme der Armee, konnten sich wohl nur schwer vorstellen, wie die technologische Entwicklung bis ins Jahr 2020 aussehen wird. Die Cyber-Bedrohung existierte damals noch nicht in ihrer heutigen Form. Mit dem Ziel, diese Legacy-Systemlandschaft sicher zu machen, hat im April 2016 der damalige Departementschef VBS entschieden, die militärischen und verwaltungstechnischen IKT-Systeme zu entflechten. Verschiedene Massnahmen und breit angelegte Programme zur Erhöhung der IKT-Sicherheit wurden bereits vorher implementiert. So führen zum Beispiel das Programm FITANIA oder die Bildung der Abteilung Cyber Security dazu, dass verschiedene Risiken minimiert werden können und allgemein stetig abnehmen.

Eine sichere IKT-Umgebung für die Schweizer Armee lässt sich aufgrund der Komplexität nicht von heute auf morgen realisieren. Die Prozesse der Beschaffung in der Bundesverwaltung, die zur Verfügung stehenden Ressourcen sowie die laufenden Anforderungen, die an die Führungsunterstützungsbasis gestellt werden, haben zusätzlich grossen Einfluss auf die zeitliche Umsetzung. Spätestens seit der strategischen Ausrichtung [redacted] ist aber die gesamte FUB darauf eingestellt, robuste und hochsichere IKT-Leistungen und elektronische Operationen zugunsten der Armee in allen Lagen anzustreben. Um dieses Ziel im Jahr 2022 zu erreichen, braucht es nun Ausdauer und Stabilität.

Ein essentieller Punkt für eine sichere IKT-Umgebung ist auch die richtige Klassifizierung von sensiblen Informationen. Darum muss dieser Prüfbericht zwingend als VERTRAULICH klassifiziert werden und darf der Öffentlichkeit nicht zugänglich sein. Es geht schlussendlich darum, die Einsatzfähigkeit der Armee sicherzustellen und keine zusätzliche Verwundbarkeit zu verursachen.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Führungsunterstützungsbasis (FUB) sorgt mit Leistungen in den Bereichen der Informations- und Kommunikationstechnologie (IKT) und elektronischen Operationen dafür, dass die Armee ihre Einsätze erfüllen kann. Sie stellt die Führungsfähigkeit der Armee in allen Lagen sicher und erbringt die IKT-Leistungen für das Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). Im April 2016 hat der Departementschef VBS entschieden, die militärischen und verwaltungstechnischen IKT-Systeme zu entflechten. Es geht darum, die Führungsfähigkeit der Armee und der Behörden über alle Lagen zu verbessern, die Sicherheit der militärischen Systeme zu verbessern und die Leistungen der BV-internen IKT Leistungserbringer komplementär auszurichten und abzustimmen. Weiter hat er die FUB beauftragt, ihre Ressourcen auf die Kernleistungen der Armee, der IKT-Systeme und -Services der BV mit erhöhtem Sicherheits- oder Verfügbarkeitsbedarf und des Sicherheitsverbundes Schweiz (SVS) zu konzentrieren. Zusätzlich ist die FUB mit dem Zentrum für elektronische Operationen (ZEO) verantwortlich für die Abwehr von Angriffen aus dem Cyber-Raum, die elektronische Kriegführung und die Kryptologie. Um diesen Auftrag umzusetzen baut die FUB im Auftrag der Armee, eine robuste, hochsichere und autarke IKT-Infrastruktur, bestehend aus einer ortsgebundenen und mobilen Kommunikationsinfrastruktur und einem Rechenzentrumverbund. Als militärischer Arm ergänzt die Führungsunterstützungsbrigade (FU Br 41/SKS) die Berufsorganisation und stellt somit die Durchhaltefähigkeit und Verdichtung der Leistungserbringung der FUB in Krisen, bei Katastrophen und Konflikten sicher.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist die Beurteilung der Massnahmenumsetzung in den Bereichen Netzwerksicherheit und Firewall vor dem Hintergrund des Turla-Cyberangriffs auf einzelne Server des VBS vom Juli 2017.

Die Prüffragen lauten:

1. Ist das Führungsnetz und die dazu gehörenden Netzwerkkomponenten so konzipiert, dass eine angemessene Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und Resilienz sichergestellt ist?
2. Sind die im Projekt [redacted] definierten Massnahmen zur Verbesserung der IKT-Sicherheit in den Bereichen Führungsnetz und Firewall zielführend und wirksam umgesetzt?
3. Ist eine permanente und lückenlose Überwachung der Infrastruktur am Perimeter und im Inneren des Netzes sichergestellt und werden Auffälligkeiten zeitnah detektiert und abgeklärt?
4. Ist die IT-Security-Governance in der FUB angemessen und wirksam?
5. Sind die Informationsprozesse im Rahmen der Sicherheitsvorfallbewältigung definiert und adressieren diese die richtigen Stellen?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf die Sicherheitsaspekte des Fhr Netz CH. Sie erfolgte anhand des International Organization for Standardization (ISO) Standards 2700x sowie des Minimalstandards zur Verbesserung der IKT-Resilienz des Bundesamtes für wirtschaftliche Landesversorgung (BWL). Weiter kamen die Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IKT-Grundschutz zur Anwendung.

Die Prüfung wurde von Roland Gafner (Revisionsleiter), Cornelia Simmen und Christian Brunner vom 21. November bis 13. Dezember 2019 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. [redacted] Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

Nach einer sofortigen Orientierung der Departementschefin, hat die EFK am 13. Dezember 2019 den ganzen Bundesrat über die festgestellten Mängel von grundsätzlicher Bedeutung gemäss Artikel 15 Absatz 3 FKG informiert.

1.4 Unterlagen und Auskunftserteilung

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

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 7. Februar 2020 statt. Teilgenommen haben seitens der Geprüften der Chef der Armee, der Chef FUB, der Chef Betrieb und der Chef Cyber Security. Das Generalsekretariat VBS (GS-VBS) wurde durch den Generalsekretär vertreten. Seitens der EFK haben der Direktor, der Federführende und der Revisionsleiter mit einem Teammitglied teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Das Projekt [redacted] schaffte vor allem Awareness

2.1 Die Resultate sind vorwiegend konzeptueller Natur

Das Projekt [redacted] wurde im 2018 mit hoher Aufmerksamkeit der FUB-Leitung gestartet. Es ist mit Schlussberichten zu den 11 Arbeitspaketen (AP) und einem Gesamt-Schlussbericht vom 24. April 2019 offiziell abgeschlossen worden. Der Projektausschuss wurde nicht aufgelöst. [redacted] Aus den Berichten und Statusmeldungen geht hervor, dass zahlreiche Dokumente erstellt worden sind. Zur operativen Umsetzung sind Arbeitspakete in die entsprechend verantwortliche Linie überführt worden. Der Stand der operativen Umsetzung soll gemäss den Abschlussberichten teilweise weiterhin an den Projektausschuss [redacted] rapportiert werden.

Die EFK stellt zu den einzelnen AP fest:

- Das AP01 «Asset Management» wurde noch nicht vollständig abgeschlossen und in das Projekt «Integrale IKT Management Plattform» (IIMP) überführt (siehe Kapitel 2.2).
- Das AP02 «Tech Assets zurückgewinnen» wurde am 31.03.2019 abgeschlossen (siehe Kapitel 4.4). Die Verantwortung wurde in die Linie übergeben und die Ergebnisse werden künftig im Information Security Management System der FUB (ISMS.FUB) bewirtschaftet.
- Das AP03 «Risikobeurteilung» wurde am 30.06.2019 abgeschlossen und in die Linie überführt. Die nicht umgesetzten Massnahmen werden durch den Riskmanager weiterbehandelt.
- Das AP04 «Sicherheitsvorgaben pro Technologie-Asset» wurde abgeschlossen. Das Referenzdesign nach Nato C3 Taxonomie[2] wurde erstellt, [redacted]. In der Folge erarbeitet die FUB die Grundlagen für eine Lösungsarchitektur. Die Weiterentwicklung der Architektur wurde als steter Prozess in die Linie übergeben.
- Das AP05 «Umsetzung Sicherheitsvorgaben» wurde noch nicht vollständig abgeschlossen und in das «ISMS.FUB» überführt. Das AP ist abhängig von den Resultaten aus dem noch nicht abgeschlossenen AP01.
- Das AP06 «Ausbau Cyber Defence» wurde abgeschlossen und die Lieferobjekte sollen im Projekt [redacted] weiterentwickelt werden.
- Das AP07 «Security Incident Response Plan (SIRP)» wurde abgeschlossen. Die Lieferobjekte werden in der Linie weiterentwickelt.
- Das AP08 «Schnittstellen» konnte nicht abgeschlossen werden. [redacted] Die Standardisierung der Schnittstellen erfolgt nach dem Abbruch des Projektes «Selz» neu mit Unterstützung des Projektes «SIEG». Die Rapportierung erfolgt an den Chief Information Security Officer (CISO FUB).

[2] Consultation, Command and Control (C3)

- Das AP09 «Awareness» ist abgeschlossen. Die Mitarbeitenden wurden in Workshops und über Kampagnen sensibilisiert. Die Sensibilisierung wird eine fortlaufende Tätigkeit bleiben.
- Das AP10 «Security Testing» wurde noch nicht vollständig abgeschlossen.
- Das AP11 «Krisenmanagement@FUB» wurde noch nicht vollständig abgeschlossen. Es fehlt noch die Durchführung der Krisenmanagementübung «FLEX» (ehemals «POTTER»). Die weitere Erarbeitung der Lieferobjekte wurden der Linie übertragen (siehe Kapitel 3.6).

Projekt [redacted]

Das Projekt verfolgt die operative Verbesserung der IKT-Sicherheit in den Netzen der FUB. Diverse AP aus dem Projekt [redacted] sollen mit diesem technisch umgesetzt werden. Es besteht aus verschiedenen Einzelvorhaben [redacted], welche beim Armeestab (A Stab) eingesteuert oder an bereits existierende Vorhaben geknüpft wurden. Auf einen konsolidierten Projektauftrag wurde aus diesem Grund verzichtet.

Teilprojekt [redacted]

Der Auftrag zum Teilprojekt [redacted] ist die Grundlage für den Aufbau des Cyber Fusion Center. [redacted] Das Security Operations Center kann auch als Service anderen Stellen der Bundesverwaltung zur Verfügung gestellt werden. Die notwendigen Massnahmen zur Erreichung des Endzustands sollen mittels geplanter Aktionen [redacted] umgesetzt werden.

Beurteilung

Die im Rahmen des Projekts [redacted] geplanten AP zur Erhöhung der IKT-Sicherheit, erachtet die EFK als zielführend. [redacted] Die vorliegenden Ergebnisse sind mehrheitlich konzeptueller Natur und haben daher noch nicht überall die benötigte Wirkung auf die IKT-Sicherheit. Das Projekt schaffte Grundlagen und bei den Mitarbeitenden der FUB immerhin eine gewisse Sensibilisierung für die Aspekte der IKT-Sicherheit.

[redacted] Mit dem Aufbau des neuen Fhr N CH (NPV) soll stattdessen eine sichere und konsequent verwaltete Netzwerkumgebung aufgebaut werden. In der Folge sollten die bestehenden Anwendungen in dieses neue Netz überführt werden.

Dieses Vorgehen erscheint grundsätzlich zielführend, steht aber im Widerspruch zum Bundesratsbeschluss (BRB) vom 23. März 2016. [redacted]

Die FUB muss sicherstellen, dass die offenen Massnahmen, welche in andere Projekte oder in die Line verschoben wurden, auch wirklich konsequent umgesetzt werden. Hierfür müssen nicht nur die technischen, sondern auch die personellen und finanziellen Ressourcen sichergestellt werden. Die weitere Verfolgung der Arbeitspakete und insbesondere deren technische Umsetzung ist durch die FUB adressiert. Aus diesem Grund verzichtet die EFK auf eine Empfehlung.

2.2 Erst anhand eines vollständigen Assetinventars kann die Sicherheit verlässlich umgesetzt werden

[redacted] Mit dem Projekt IIMP verfolgt die FUB das Ziel, die Datenbanken mit Angaben zu den Assets zusammenzuführen, um ein vollständiges zentrales Inventar zu erhalten. [redacted] Zum Zeitpunkt der Revision liefen Tests mit dem Tool [redacted]. Damit sollen zukünftig die Assets zentral verwaltet werden können. [redacted] Daher hat sich das Projektteam mit dem Cyber Fusion Center (CFC) kurzgeschlossen, welches ebenfalls ein Tool [redacted] zur Überwachung der Assets beschafft hat. [redacted] Das Projekt IIMP wird die Informationen aus den Auswertungen des CFC erhalten und mit den vorhandenen Angaben aus den verschiedenen Quellen vergleichen sowie konsolidieren.

[redacted]

Beurteilung

[redacted] Ein solches Inventar der IKT-Assets stellt die wichtigste Grundlage für die Umsetzung der IKT-Sicherheit dar. Es ermöglicht erst die Verwaltung der Netzwerkressourcen. Zahlreiche wichtige Elemente der IKT-Sicherheit, insbesondere Change- und Configuration Management, das Business Continuity Management (BCM) sowie das IT Service Continuity Management (ITSCM) können nur funktionieren, wenn auf ein lückenloses Inventar zurückgegriffen werden kann.

[redacted]

Die Vorgehensweise im Projekt IIMP erachtet die EFK als zielführend. Dem Projekt muss grosse Beachtung geschenkt werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der FUB, dem Projekt IIMP höchste Priorität und Unterstützung zu geben. Schwachstellen können nur dann erkannt und eliminiert werden, wenn ein vollständiges und aktuell gehaltenes Inventar aller IKT-Assets vorhanden ist.

Stellungnahme FUB

Erfassung Netzübergänge:
Bei der Schnittstellensanierung [redacted] sind [redacted] Massnahmen noch offen. [redacted]

IKT-Asset-Management:
Der IKT-Grundschutz Bund, Punkt 13.1.1 wird durch die Führung der IKT-Mittel in zwei Datenbanken in der FUB abgedeckt. Die zentrale Führung und Steuerung der IKT-Mittel und eine vollständige, einheitliche Erfassung aller IKT-Assets ist Ziel des Projekts IIMP. Die Erfassung wird umgesetzt und hat höchste Priorität nach Empfehlung EFK. [redacted]

3 Vorgaben aus dem Grundschutz sind nicht vollumfänglich umgesetzt

3.1 Die Sicherheitsorganisation ist zielführend

Die Sicherheitsorganisation der FUB ist im Aufbau. Die Stelle des CISO wurde am 1. August 2018 besetzt. Als Mitglied der Geschäftsleitung kann der CISO auf hoher Ebene wirken. Mit der Reorganisation wurde auch die Abteilung Cyber Security neu geschaffen, bzw. bestehende Bereiche zusammengeschlossen. Diese betreut für die ganze FUB die Informatik- und Cybersicherheit. Das neugeschaffene CFC beinhaltet das Military Computer Emergency Response Team (milCERT), das Security Operations Center (SOC) und einen Bereich für die Infrastruktur und Weiterentwicklung (I + W) der Detektions- und Auswerteplattform. Die Organisation des CFC soll [redacted] ausgebaut werden. [redacted]

I + W betreibt das eigene Rechenzentrum (RZ) für die Detektions- und Auswerteplattform. Das Monitoring erfolgt im Security Information and Event Management (SIEM), die vertieften Analysen erfolgen in dedizierten Systemen bei milCERT. Die Sensordaten werden auch anderen Bereichen wie dem Betrieb und dem ZEO zur Verfügung gestellt.

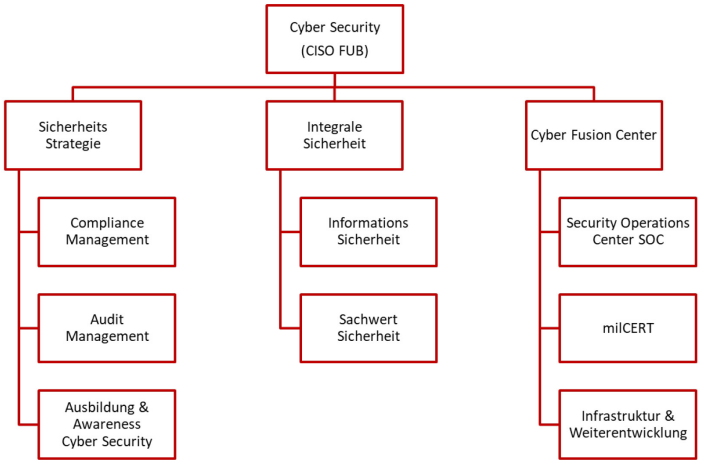

Abbildung 1: Organigramm Cyber Security, Stand 16.1.2020

Der Bereich Integrale Sicherheit beinhaltet die Teilbereiche Objekt- und Sachwertsicherheit sowie die Informationssicherheit. Letzterem sind die Bereiche Datenschutz, das Risikomanagement und das ISMS untergeordnet.

Beurteilung

Die EFK begrüsst die Schaffung der Position eines CISO und dessen Einbindung in die Geschäftsleitung. Mit dieser Massnahme fliessen die Anliegen zur Sicherheit bei einer zentralen Stelle zusammen und erhalten die bestmögliche Unterstützung durch das Top-Management. Der Zusammenzug der Ressourcen im Sicherheitsbereich zu einem Fachbereich kann längerfristig zu einem verbesserten Austausch zwischen den Akteuren beitragen. Dieser begünstigt nachhaltig die konsolidierte Erfassung von Bedrohungen und Vorfällen und dient einer verbesserten Erstellung des Lagebildes. Es ist wichtig, dass die vakanten Positionen so rasch als möglich besetzt werden können, damit der Bereich seine volle Wirkung erzielen kann.

3.2 Das Information Security Management System schafft eine Grundlage zur Erhöhung der IKT-Sicherheit

Das von der FUB implementierte ISMS dient der Geschäftsleitung der FUB zur aktiven Steuerung und Überwachung der Informationssicherheit. Dabei berücksichtigt das System die Auswirkungen von Sicherheitsrisiken auf die Geschäftstätigkeit bzw. Aufgabenerfüllung. Die Risiken werden quartalsweise dem Chef der FUB summarisch rapportiert und durch diesen beurteilt. Festgelegte Massnahmen werden durch den ISMS-Verantwortlichen periodisch bei den verantwortlichen Stellen überprüft. Dies erfolgt mittels einer Selbstdeklaration. Als erledigt gemeldete Aufträge werden stichprobeweise mit internen Audits überprüft.

Das ISMS der FUB wurde am 2. November 2018 durch die Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS) nach ISO/IEC 27001:2013 zertifiziert. Die Anwendbarkeitserklärung (SOA) vom 16. September 2019 zeigt auf, dass sämtliche Controls anwendbar sind. Die Prüfstelle bescheinigte der FUB, dass das Managementsystem den Anforderungen der aufgeführten normativen Grundlage entspricht. [redacted]

«ISMS.VBS»

Im Rahmen der Prüfungshandlungen hat die EFK auch die Bereiche der FUB im übergeordneten «ISMS.VBS» geprüft. Es sollte geklärt werden, welche Informationen zur Steuerung auf dieser Ebene einfliessen. Das vom VBS aufgesetzte ISMS beinhaltet über [redacted] Schutzobjekte, diese sind in verschiedene Gruppen aufgeteilt. Die Schutzobjekte weisen nur das Datum der Schutzbedarfsanalyse (Schuban) und der Informationssicherheits- und Datenschutzkonzept (ISDS) aus. Das «ISMS.VBS» wird zum heutigen Zeitpunkt primär dazu verwendet, quartalsweise gegenüber dem Generalsekretariat (GS) und Ende Jahr gegenüber dem Informatiksteuerungsorgan des Bundes (ISB) den Stand der Sicherheitsdokumente zu rapportieren. [redacted]

Mit Prüfbericht «ISMS.VBS – Konformitätsaudit 2019» IKT-Prüfung I 2019-06, konnte die interne Revision des GS-VBS die Wirksamkeit des «ISMS.VBS» nicht bestätigen.

Beurteilung

Aufbau und Funktionsweise des ISMS der FUB erachtet die EFK als geeignet zur Behandlung der Sicherheitsanforderungen. Die Behandlung von Risiken und den daraus abgeleiteten Massnahmen inkl. dem Controlling der Umsetzung, ist ein zielführender Ansatz. Eine stichprobenweise Überprüfung der Umsetzung findet mittels interner Audits statt und sichert die Qualität des Reportings.

[redacted]

3.3 Die Information Security Policy ist konsequent weiter zu entwickeln und die Massnahmen sind gezielter zu priorisieren

Mit dem [redacted] ist im Oktober 2019 die strategische Ausrichtung der FUB bis 2022 festgelegt worden. Darin wird die konsequente Weiterentwicklung der FUB zum Serviceprovider in allen Lagen beschrieben. Dem Aspekt der Sicherheit wird in der strategischen Stossrichtung ein hoher Stellenwert beigemessen. Die FUB visiert darin den höchsten Maturitätslevel an.

Die Information Security Policy der FUB vom 11. Oktober 2019 strebt eine «Kultur von Sicherheit» an. Diese soll mit sieben generisch gehaltenen Massnahmen erreicht werden. Ein Ziel ist insbesondere die Sicherstellung des IKT-Grundschutzes. [redacted]

Beurteilung

Mit dem [redacted] hat die FUB die strategische Stossrichtung mit Zielen und fünf auf hohem Niveau definierten Massnahmen vorgegeben. Verschiedene Dokumente verfeinern die Ziele, welche künftig erreicht werden sollen. [redacted] Aufgrund der verfügbaren Ressourcen, sollte die FUB den Fokus auf rasch umsetzbare Massnahmen setzen, damit erkannte Schwachstellen systematisch vermindert werden können.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt der FUB, mittels einer detaillierten Umsetzungsplanung die mittel- bis langfristigen Massnahmen zur Verbesserung der IKT-Sicherheit zu definieren und zu terminieren. Insbesondere der Priorisierung der Massnahmen muss besondere Beachtung geschenkt werden.

Stellungnahme FUB

Die strategische Ausrichtung der FUB [redacted] ist die Grundlage für die Transformation hin zu robusten und hochsichere IKT-Leistungen und elektronische Operationen zugunsten der Armee in allen Lagen. Die mittel- und langfristigen Planungen darüber hinaus werden in Anlehnung an das Zielbild 2030+ der Armee erarbeitet. Darin enthalten sind auch die mittel- bis langfristigen Massnahmen zur Verbesserung der IKT-Sicherheit. Für die detaillierte Umsetzung wird eine vertiefte Sicherheitsstrategie entwickelt. Sie definiert die Zwischenziele und Priorisierung, die erforderlichen Massnahmen, die notwendigen Mittel zur Realisierung und zeigt die Überprüfungsmethoden auf. Die Umsetzungsplanung der Sicherheitsstrategie wird iterativ und fortlaufend aktualisiert.

3.4 Die Vorschriften zum Umgang mit klassifizierten Informationen werden nicht konsequent eingehalten

Im Rahmen der Prüfung konnte festgestellt werden, dass Dokumente mit dem Klassifizierungsvermerk VERTRAULICH unverschlüsselt auf Netzablagen gespeichert sind. Bei mehreren ISDS Konzepten wurde dies durch die Mitarbeitenden der FUB in der Folge korrigiert. Eine gezielte Suche auf diesen Laufwerken zu einem späteren Zeitpunkt hat dies bestätigt. [redacted]

Beurteilung

Die Verordnung über den Schutz von Informationen des Bundes (ISchV) regelt die Handhabung von klassifizierten Informationen detailliert und schreibt die Verschlüsselung für die Klassifizierungsstufe VERTRAULICH in vernetzten Umgebungen vor. Unverschlüsselte und klassifizierte Informationen können, wenn sie in falsche Hände geraten, den Landesinteressen Schaden zufügen. [redacted]

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt der FUB, sämtliche Datenablagen auf unsachgemäss behandelte Informationen zu prüfen und entsprechende Schutzmassnahmen umzusetzen. Die Mitarbeitenden auf allen Stufen müssen gezielt in der Umsetzung der ISchV geschult werden.

Stellungnahme FUB

Die Awarenesskampagne der FUB zur Erhöhung der Informationssicherheit enthält eine detaillierte Umsetzungsplanung mit Schulungsmassnahmen und wird laufend an die aktuellen Cyber-Bedrohungen angepasst. Dabei ist die konsequente Durchführung der bestehenden LMS-Lektionen, welche unter anderem auch die Schulung der ISchV enthalten, ein wesentlicher, integraler Bestandteil. Schon heute erfolgt die regelmässige Beauftragung der Datenowner zur Bereinigung der Datenablagen und die Kontrolle der korrekten Klassifizierung sowie die Einhaltung der Sicherheitsvorschriften. Mittels periodischer Überprüfung mit Stichproben wird die Einhaltung der ISchV sichergestellt. Die FUB wird 2020 eine ausserordentliche Überprüfung mit Stichproben durchführen.

3.5 Konten [redacted] im Fhr Netz CH sind ungenügend geschützt

Mit Beschluss vom 14. Dezember 2009 hat der Bundesrat verfügt, dass Mitarbeitende und Administratoren nur mittels 2-Faktor-Authentifizierung (etwas haben und etwas wissen) auf Systeme der Bundesverwaltung zugreifen dürfen. [redacted]

Beurteilung

Die 2-Faktor-Authentifizierung ist eine wichtige Massnahme, um die Systeme vor unerlaubtem Zugriff zu schützen, [redacted]

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt der FUB, die 2-Faktor-Authentifizierung für alle [redacted] zeitnah zu implementieren. Wo dies technisch nicht umsetzbar ist, sind mitigierende Massnahmen zu treffen und wo erforderlich die entsprechenden Ausnahmegenehmigungen beim ISBD des VBS oder dem ISB zu beantragen.

Stellungnahme FUB

[redacted] Für die Abweichungen vom Grundschutz Bund bestehen im Fhr Netz CH bereits heute die entsprechenden ISDS-Konzepte. Diese werden spezifisch auf Abweichungen zum IKT-Grundschutz in der Bundesverwaltung überprüft und wo nötig ein P035-Antrag an den ISBD oder das ISB gestellt.

3.6 Sicherstellung des Geschäftsbetriebs und Notfallmanagement ist aufgesetzt [redacted]

Die FUB verfügt über eine umfangreiche Krisenorganisation. Im Bedarfsfall kann der Krisenstab auf die Unterstützung einer Task-Force mit Teilnehmenden aus allen Fachbereichen zurückgreifen. Unterstützend wirkt ein Response Team und ein Spezialisten-Pool mit. Die Vorgaben und Konzepte für den Krisenstab sind umfangreich und stehen in einer logischen Gliederung auf einem SharePoint zur Verfügung. Im Bedarfsfall sind für die wichtigsten Szenarien Checklisten vorhanden. Die Zusammenarbeit im Krisenstab wird mehrmals jährlich geübt und die Erkenntnisse daraus fliessen in die Weiterentwicklung der Organisation ein.

Auch in den Bereichen BCM und ITSCM sind verschiede Vorgehen und Prozesse beschrieben. [redacted]

Beurteilung

Die FUB verfügt über eine breit abgestützte Krisenorganisation. Die EFK erachtet die Organisation als zielführend aufgebaut. Kontinuitäts- und Notfallpläne sind eine wichtige Grundlage für ein systematisches Vorgehen im Störungsfall. Die FUB hat die Massnahmen und Prozesse angemessen, jedoch nicht lückenlos dokumentiert. Fehlende Dokumente und Prozesse müssen zeitnah erarbeitet werden. Regelmässige Überprüfungen und Aktualisierungen dieser Dokumentation sind für einen reibungslosen Betrieb im Störfall eine elementare Grundvoraussetzung. [redacted]

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt der FUB, «end-to-end»-Tests im Rahmen der Wiederherstellungsverfahren und des betrieblichen Kontinuitätsmanagements zu planen und regelmässig durchzuführen.

Stellungnahme FUB

[redacted] In den anderen Bereichen werden die BCM-Planung überarbeitet und entsprechende Recovery/Restore-Tests durchgeführt. Bei der zeitlichen Umsetzung gilt es die Meilensteine (Maturitätsstufen) des Befehls «ULFA» (Umfassende Leistungsfähigkeit der Armee) zu beachten.

3.7 Die BInfV Vorgaben zur IKT-Sicherheit werden nicht konsequent eingehalten

Unterschreitet eine Verwaltungseinheit (VE) die Vorgaben des IKT-Grundschutzes, liegt eine bewilligungspflichtige Ausnahme vor (BinfV, Art. 17 Abs. 1 Bst. e und f). Die VE ist verpflichtet, die daraus resultierenden Risiken zu identifizieren, quantifizieren und durch das ISB oder den ISBD genehmigen zu lassen. Letzterer kann diese Genehmigung nur unter definierten Rahmenbedingungen erteilen, andernfalls muss die VE einen Antrag an das ISB stellen (P035 – Prozess).

Dem ISBD des VBS liegen keine Anträge für Grundschutzunterschreitungen vor und es sind zum Prüfzeitpunkt auch keine Ausnahmen genehmigt worden. Ebenfalls sind beim ISB keine Ausnahmen der FUB verzeichnet. Dies lässt fälschlicherweise den Schluss zu, dass die FUB den Grundschutz lückenlos umsetzt. Mit einer Informationsnotiz vom 5. November 2018 informierte der Departementschef VBS den Gesamtbundesrat über die Einhaltung des IKT-Grundschutzes bei der FUB.

Eine Meldung an das ISB im Rahmen der Berichterstattung über den Stand der Umsetzung von Sicherheitsmassnahmen gemäss Art. 11 BInfV, erfolgte weder 2017 noch 2018. Damit war die Orientierung des Bundesrats über den Stand der IKT-Sicherheit Ende 2018 durch das ISB unvollständig.

Beurteilung

Die FUB kann im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen vom IKT-Grundschutz abweichen. Jede Abweichung muss jedoch im entsprechenden ISDS-Konzept beschrieben und die Risiken ausgewiesen werden. Der Leiter oder die Leiterin der VE entscheidet, ob diese Risiken in Kauf genommen werden können. Zudem müssen solche Grundschutzunterschreitungen vom ISBD oder vom ISB genehmigt werden. Bei Nichteinhalten dieser Vorgaben besteht die Gefahr, dass eine VE Risiken nicht erkennt und diese auch nicht entsprechend behandelt, oder dass sich solche Risiken unerkannt kumulieren.

Der heutige Zustand der Umsetzung des Grundschutzes lässt den Schluss zu, dass bereits zum Zeitpunkt der Informationsnotiz vom 5. November 2018 an den Gesamtbundesrat, die Anforderungen nicht konsequent eingehalten wurden.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt der FUB, sämtliche Ausnahmen zu den IKT-Grundschutzanforderungen zu erfassen und zu prüfen. Primär sollen Grundschutzunterschreitungen vermieden werden. Wo dies nicht umsetzbar ist, müssen diese entsprechend dem IKT-Grundschutz Kapitel 1.2 formalisiert werden.

Stellungnahme FUB

Sämtliche Abweichungen zum IKT-Grundschutz in der Bundesverwaltung werden überprüft, die ISDS-Konzepte wo nötig ergänzt und wo gefordert ein P035-Antrag an den ISBD oder das ISB gestellt.

4 Das Führungsnetz Schweiz [redacted]

4.1 Das Fhr Netz CH [redacted]

Für das heutige Fhr Netz CH besteht eine generische Übersicht inklusive dem Netzwerkperimeter Verteidigung (NPV). Dabei handelt es sich um ein logisches Modell, welches die IKT-Sicherheitsarchitektur V beschreibt. Mit dem NPV wurde in den letzten Jahren eine neue, besser kontrollierte Netzwerkzone mit klar definierten Übergängen geschaffen. [redacted]

Mit dem Projekt NPV 2016 wurde die bis dahin fehlende Georedundanz der Verwaltungssysteme des NPV behoben. Im Rahmen des Projekts wurde auch die Systemarchitektur angepasst, die Prinzipien festgelegt und die Firewall-Regeln bereinigt. [redacted] Das Engineering hat Kommunikationsvorgaben für die Freischaltung von Firewall-Ports erstellt. Die FUB richtet sich hierbei nach den Vorgaben des ISB. Für Portöffnungen besteht ein Prozess [redacted]. Dieser gibt Anforderungen vor und stellt die Nachvollziehbarkeit sicher. [redacted]

Im Oktober 2019 wurde die Referenzarchitektur für den Swiss Information Exchange Gateway (SIEG) genehmigt. Der SIEG ist ein Sicherheits-Konzept, welches mittels bedarfsgerecht parametrisierbaren Schutzmechanismen den gesteuerten und überwachten Datenaustausch zwischen zwei Hoheitsgebieten ermöglicht. Der SIEG setzt sich aus dedizierten Bausteinen zusammen, welche definierte Funktionalität zur Verfügung stellen. Dieser befindet sich aber erst im Aufbau und wird [redacted] vollständig operativ in den NPV integriert sein.

[redacted]

Beurteilung

[redacted] Die Vorgaben und Prozesse im Netzbereich sind grundsätzlich vorhanden [redacted]

[3] Sämtliche Verbindungen in beide Richtungen sind zugelassen.

[redacted]

Ein fehlendes ITSCM birgt das Risiko in sich, dass das Fhr Netz CH im Ereignisfall nicht oder nur beschränkt zur Verfügung steht (siehe Kapitel 3.6).

Eine vollständige Erhebung der gesamten Systemlandschaft ist eine Forderung aus dem Grundschutz und ist mit der Empfehlung 6 abgedeckt. Die Behandlung des fehlenden ITSCM ist in der Beurteilung des Kapitel 3.6 beschrieben. Aus diesen Gründen verzichtet die EFK hier auf weitere Empfehlungen.

Die in der Referenzarchitektur beschriebenen Anforderungen und Prinzipien sind detailliert und zielführend. Um die Sicherheit zu erhöhen, muss sichergestellt werden, dass den Vorgaben entsprechend implementiert wird und möglichst keine Ausnahmen stattfinden, bzw. solche immer wieder überprüft werden müssen.

Stellungnahme FUB

Die im Bericht Kapitel 4.1 erwähnten [redacted] Verbindungen betreffen die Domotik im CAMPUS-Lan. Diese wurden mit erteilter Bewilligung für den Aufbau und die Integration der Domotik-Komponenten zugelassen. In der derzeit laufenden Inbetriebnahme werden diese Verbindungen bis 31.12.2020 sukzessive zurückgebaut.

4.2 [redacted] Wiederherstellungsverfahren [redacted]

Im Konzept zu Backup und Restore der Kommunikationsinfrastruktur sind die gerätespezifischen Anforderungen beschrieben. Die Datensicherung erfolgt regelmässig. [redacted]

Beurteilung

Die FUB ist sich der Wichtigkeit von Backups bewusst und hat solche konzeptionell auch angemessen umgesetzt. [redacted]

Empfehlung 7 (Priorität 2)

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

Stellungnahme FUB

Im Rahmen des Projektes Fhr Netz CH wurde bereits ein Teilprojekt (IKT NMS) initiiert und gestartet. In diesem Zusammenhang werden die Wiederherstellungsverfahren des Netzwerkmanagements neu beschrieben und die regelmässige Überprüfung definiert. [redacted]

4.3 Veraltete Systeme [redacted]

Der IKT-Grundschutz fordert im Kapitel 12.1.6 die Ablösung von Systemen innert 2 Jahren, wenn aufgrund des Alters von Komponenten keine Fehlerkorrekturen mehr gemacht werden können.

Beurteilung

Aktuelle System- und Softwarestände sind aus Sicht der IKT-Sicherheit essentiell. Wenn die Systeme nicht auf dem neuesten Stand sind, wird die Möglichkeit eines Angriffs oder eines Ausfalls deutlich erhöht. Es ist zu vermeiden, dass vom Hersteller nicht mehr unterstützte Systeme betrieben werden. Ausserdem stellt der Weiterbetrieb veralteter Systeme einen Verstoss gegen verschiedene Kapitel des IKT-Grundschutzes dar.

Empfehlung 8 (Priorität 1)

Die EFK empfiehlt der FUB, bei der Erneuerung ein einheitliches Life-Cycle-Management zu etablieren, um veraltete Systeme gestützt auf eine langfristige Planung zeitnah ablösen zu können. Dies würde nicht nur die Steuerung der finanziellen Mittel, sondern auch der benötigten Ressourcen erleichtern.

Stellungnahme FUB

Im Rahmen der Transformation [redacted] ist das Life-Cycle-Management integraler Bestandteil der IKT Gesamtplanung V. Aktuell werden die Firewalls im Rahmen des Projektes Firewallautomatisierung auf einen einheitlichen Firmware-Stand gebracht. Bei den Servern sind im Bereich der Windows Operatingsystems aktuell noch Versionen im Einsatz, welche einen extended Support benötigen.

4.4 Der Betrieb der Active Directory muss zentral erfolgen

Die EFK hat festgestellt, dass Active Directory Installationen (AD) vorhanden sind, welche nicht durch den Betrieb AD verwaltet werden. Ein Grund hierfür ist das historische Wachstum der Umgebung. [redacted]

[redacted] Im Disaster Recovery Handbuch sind die Wiederherstellungsverfahren der vom Betrieb AD bewirtschafteten Directories detailliert und nachvollziehbar beschrieben. [redacted]

Beurteilung

Die ADs verwalten die verschiedenen Objekte in einem Netzwerk. Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften werden durch die AD organisiert, bereitgestellt und überwacht. Unbekannte oder fremdbetreute ADs stellen daher ein Risiko bezüglich der IKT-Sicherheit dar. Nur durch [redacted] einer zentralen Steuerung durch die FUB können allfällige Sicherheitslücken erkannt sowie entsprechende Massnahmen getroffen werden. Im Falle eines notwendigen Disaster Recovery müssen alle Informationen zentral verfügbar sein.

Empfehlung 9 (Priorität 1)

Die EFK empfiehlt der FUB, zeitnah eine Übersicht aller im Netz der FUB operativen Active Directories zu erstellen und deren Betrieb zu zentralisieren.

Stellungnahme FUB

Die FUB hat bereits eine Übersicht aller zentral betriebener AD. [redacted] Eine Zentralisierung sämtlicher operativen AD ist bei den heutigen Fachanwendungen (Legacy-Systemen) nicht realisierbar. Dies wird erst mit der Migration der Fachanwendungen auf die RZ 2020 Infrastruktur möglich werden.

4.5 [redacted] User Access Management [redacted]

Im Bereich des Netzwerkbetriebs fehlt ein User Access Management für Administrations-Zugriffe. [redacted]

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. [redacted] Um die Sicherheit zu erhöhen und die Umsetzung der im IKT-Grundschutz geforderten Passwortvorgaben umzusetzen, ist der Einsatz eines entsprechenden Passwort-Management-Systems erforderlich. Damit wird auch das Ändern der diversen Passwörter erheblich erleichtert, da es in einem zentralen System erfolgt. Zudem kann die Umsetzung der Vorgaben automatisiert sichergestellt und überprüft werden.

Empfehlung 10 (Priorität 1)

Die EFK empfiehlt der FUB, die Implementierung eines User-Access-Managements [redacted] umzusetzen. Dabei müssen auch die Aspekte des Passwortmanagements berücksichtigt werden.

Stellungnahme FUB

Im Rahmen des Projektes Fhr Netz CH wurde bereits ein Teilprojekt initiiert und gestartet, welches [redacted] die Management Plattform neu definiert und aufbaut. In dessen Umfang werden [redacted] das Passwortmanagement neu festgelegt.

5 Die Überwachung der Netzwerkaktivitäten muss verstärkt werden

5.1 [redacted]

5.2 Die Handhabung von Sicherheitsvorfällen wird überarbeitet

Der Prozess «Security Incident Management sicherstellen» wurde im Jahr 2017 beschrieben und durch den damaligen Leiter milCERT freigegeben. Grundsätzlich adressiert dieser die üblichen Aktivitäten, Ziele und Verantwortungen. Der Prozess berücksichtigt die Klassifizierung der Ereignisse und beschreibt die entsprechenden Vorgänge. Massnahmen werden bezüglich ihrer Wirkung und auf der Basis von weiterführenden Analyseresultaten überprüft. Folgemassnahmen werden im Rahmen des mit der operativen Stufe definierten

Aktionsplans ausgelöst. [redacted] Auch können diese zur Erstellung eines Lagebilds einen erheblichen Mehrwert bringen.

[redacted]

Inzwischen ist eine Neufassung des Prozesses durch das CFC in Bearbeitung.

Beurteilung

Der Prozess zur Bearbeitung von Ereignissen ist grundsätzlich zweckmässig aufgebaut und nachvollziehbar. [redacted] Aufgrund der laufenden Überarbeitung des Prozesses verzichtet die EFK auf eine diesbezügliche Empfehlung.

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 die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 9. Dezember 2011 (Stand am 1. November 2016), SR 172.010.58
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. Januar 2018), SR 510.411
Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. Januar 2014) SR 235.1
Weisungen des EFD zur Umsetzung der Bundesinformatikverordnung (WUBinfV) vom 19. Februar 2013 (Stand 10. August 2018), W001
Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung(WIsB) vom 16. Januar 2019, W002
Bundesratsbeschlüsse
Bundesratsbeschluss vom 14. Dezember 2009 «Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung»
Vorgaben
IKT-Grundschutz in der Bundesverwaltung (Si001)

Anhang 2: Abkürzungen

AD	Active Directory
AP	Arbeitspaket(e)
APT	Advanced Persistent Threat (siehe auch Glossar)
A Stab	Armeestab
BCM	Business Continuity Management
BRB	Bundesratsbeschluss
BWL	Bundesamte für wirtschaftliche Landesversorgung
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutsch-land)
CISO	Chief Information Security Officer
CFC	Cyber Fusion Center
DC	Datacenter
DMZ(1)	Demilitarisierte Zone (siehe auch Glossar)
EFK	Eidgenössische Finanzkontrolle
EFD	Eidgenössisches Finanzdepartement
FIS HE	Führungsinformationssystem Heer
FIS LW	Führungsinformationssystem Luftwaffe
Fhr Netz CH	Führungsnetz Schweiz
FUB	Führungsunterstützungsbasis
FU Br 41/SKS	Führungsunterstützungsbrigade 41/ Systeme – Kurse – Support (siehe auch Glossar)
GS-VBS	Generalsekretariat VBS
IIMP	Integrale IKT Management Plattform
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes

ISBD	Informatiksicherheitsbeauftragte/r des Departements
ISchV	Verordnung über den Schutz von Informationen des Bundes
ISDS	Informationssicherheits- und Datenschutzkonzept
ISMS	Information Security Management System (siehe auch Glossar)
ISO	International Organization for Standardization
ITSCM	IT Service Continuity Management
I + W	Infrastruktur und Weiterentwicklung
LCM	Life-Cycle-Management
LE	Leistungserbringer
MilCERT	Military Computer Emergency Response Team
NOC	Network Operations Center
NPV	Netzwerkperimeter Verteidigung
PED	Planned Execution Day (siehe auch Glossar)
RZ	Rechenzentrum
Schuban	Schutzbedarfsanalyse
SDR	Software Defined Radio (siehe auch Glossar)
SIEG	Swiss Information Exchange Gateway
SIEM	Security Information and Event Management (siehe auch Glossar)
SIRP	Security Incident Response Plan
SOA	Statement of Applicability (Anwendbarkeitserklärung)
SOC	Security Operations Center
SQS	Schweizerische Vereinigung für Qualitäts- und Management-Systeme
SVS	Sicherheitsverbund Schweiz
V	Gruppe Verteidigung

VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit
ZEO	Zentrum für elektronische Operationen

Anhang 3: Glossar

Advanced Persistent Threat	Komplexer, zielgerichteter und effektiver Angriff auf kritische IKT-Infrastrukturen und vertrauliche Daten.
IKT-Assets	IKT-Assets sind sowohl die Hardware und alle peripheren Geräte als auch die gesamte Software und deren zugehörige Lizenzen. IKT-Assets sind integrale Bestandteile der Systeme und der Netzwerkinfrastruktur eines Unternehmens.
DIN ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 «Information technology – Security techniques – Information security management systems – Requirements» definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
Disaster Recovery	Disaster Recovery bezeichnet die Maßnahmen, welche nach einem Ausfall von Komponenten in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur.
Demilitarisierte Zone	Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.
Domotik	Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung von Gebäuden und technischen Steuerungen.
End of Life	Systeme oder Software, welche vom Hersteller nicht mehr produziert oder unterstützt werden und daher nicht mehr lieferbar sind.
End of Service	Produkte, für die der Hersteller keinen Service bzw. keinen Support mehr anbietet.
FU Br 41/SKS	Die Führungsunterstützungsbrigade 41/SKS (FU Br 41/SKS) ist die Brigade für die Informations- und Kommunikationstechnologie der Schweizer Armee. Sie betreibt die Kommunikationsnetze der Armee, die Führungsanlagen der Landesregierung und der Armee sowie mobile Systeme für die elektronische Kriegsführung.
IKT-Assets	Software oder Hardware innerhalb einer informationstechnischen Umgebung. IT-Assets sind integrale Bestandteile der Systeme und der Netzwerkinfrastruktur des Unternehmens.

ISMS	Verfahren und Vorgaben innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.
Kerberos-Key	Verteilter Authentifizierungsdienst (Netzwerkprotokoll) für offene und unsichere Computernetze (z. B. Internet), welcher auf dem Needham-Schroeder-Protokoll zur Authentifizierung basiert.
Nato C3	Die NATO-Konsultations-, Kommando- und Kontrollorganisation (NC3O) wurde 1996 gegründet. Ihr Hauptziel ist die Bereitstellung einer kohärenten, sicheren und interoperablen C3-Fähigkeit für die NATO.
[redacted]	[redacted]
P035 – Prozess	Die IKT-Vorgabe regelt den Umgang mit Anforderungen und Vorgaben zur Bundesinformatik gemäss Ziffer 4 der Weisungen des EFD vom 19. Februar 2013 zur Umsetzung der Bundesinformatikverordnung (WUBinfV) sowie gemäss P000 - Informatikprozesse in der Bundesverwaltung.
Planned Execution Day	Begriff der FUB, welcher die Zusammenarbeit mit der Industrie zur Rückgewinnung der Assets beschreibt.
[redacted]	[redacted]
Security Information and Event Management	Security Information and Event Management kombiniert «Security Information Management» und «Security Event Management» für die Echtzeitanalyse von Sicherheitsalarmen aus Anwendungen und Netzwerkkomponenten.
[redacted]	[redacted]
Software Defined Radio	Konzepte für Hochfrequenz-Sender und -Empfänger, bei denen kleinere oder größere Anteile der Signalverarbeitung mit Software verwirklicht werden.
[redacted]	[redacted]
Turla-Cyberangriff	Turla, auch Snake oder Uroburos genannt, ist ein 2008 als Malware erkanntes Computerprogramm, aber auch die Bezeichnung für eine (russische) Spionage-Gruppe.

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).