

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]

[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]

[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

werden die Minimalvorgaben des Informatiksteuerungsorgans des Bundes nicht eingehalten. Ausnahmegenehmigungen zu diesen Unterschreitungen liegen nicht vor.

[REDACTED]

[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.