Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Schweizer Armee
Führungsunterstützungsbasis FUB

IKT-Sicherheit ist ein Prozess und kein Zustand: Informationsupdate der FUB zum EFK-Bericht zur Prüfung der Informatiksicherheit

Im Umgang mit Sicherheitslücken und der entsprechenden Berichterstattung gegenüber der vorgesetzten Stelle hat seit 2018 in der Führungsunterstützungsbasis ein Paradigmenwechsel stattgefunden. Erkannte Sicherheitslücken werden seit da systematischer erfasst, wo möglich behoben oder isoliert und wo nötig gemeldet. Auch mit Unterstützung der EFK konnte seit 2018 die IKT-Sicherheit massgebend verbessert werden. Eine Ausführung mit weiteren Hintergrundinformationen ist auf www.armee.ch/ikt-sicherheit verfügbar.

IKT-Asset-Inventar wird vervollständigt

Vor dem Paradigmenwechsel bestand kein umfassendes IKT-Asset-Inventar (Verzeichnis der IKT-Komponenten inkl. Konfiguration). Diesem Umstand wurde höchste Priorität gegeben und umfassende Massnahmen eingeleitet. Für die bestehende Systemlandschaft werden die bereits vorhandenen IKT-Asset-Inventare zusammengeführt, wo nötig ergänzt und vereinheitlicht. So wird bis zum 31.12.2021 ein lückenloses IKT-Asset-Inventar vorhanden sein. In der neu entstehenden IKT-Landschaft wird bereits heute ein moderner Sicherheitsansatz durchgesetzt, der es möglich macht, alle IKT-Assets kontinuierlich im Überblick zu behalten und das IT-Service-Continuity-Management zu gewährleisten.

Abweichungen zum IKT-Grundschutz Bund und zur Bundesinformatik Verordnung

Die Gruppe Verteidigung kann im Einzelfall aus organisatorischen, technischen oder wirtschaftlichen Gründen vom IKT-Grundschutz abweichen. Zum Beispiel ist dies der Fall, wenn eine Mehrfaktor-Authentifizierung technisch nicht auf allen Komponenten implementiert werden kann. Jede Abweichung muss jedoch im entsprechenden Informationssicherheits- und Datenschutzkonzept ISDS beschrieben und die Risiken ausgewiesen werden. Dort, wo die Anforderungen nicht erfüllt sind, werden kompensierende Massnahmen umgesetzt. Wo solche technisch nicht möglich sind, werden sogenannte P035-Anträge für die Abweichung zum IKT-Grundschutz Bund an die Sicherheitsverantwortlichen im Departement und Nationalen Zentrum für Cybersicherheit NCSC (ehemals Informatiksteuerungsorgan des Bundes ISB) eingereicht.
In Einzelfällen wurde nach der Feststellung einer Abweichung zum IKT-Grundschutz Bund nicht auch noch ein Antrag P035 eingereicht. Diese Unterlassungen wurden in der FUB erkannt und es werden neu seit April 2020 sämtliche Abweichungen zum IKT-Grundschutz systematisch gemeldet.
Aus Sicht FUB ist ein Ausbau des IKT-Schutzes bei veralteten Systemen aus verschiedenen Gründen nicht flächendeckend sinnvoll. Eine der Konsequenzen aus diesem Vorgehen ist, dass die Restrisiken bei veralteten und isolierten Systemen durch die Risikoeigner getragen werden. Somit wurden bei diesen Systemen die Abweichungen zum IKT-Grundschutz Bund, falls dadurch die IKT der Bundesverwaltung nicht gefährdet wird, auch nicht an das ISB gemeldet.

Verbesserungen im Umgang mit klassifizierten Informationen

Speziell für die Schulung der internen und externen Mitarbeitenden der FUB im Umgang mit klassifizierten Informationen wurde 2019 das Team Ausbildung und Awareness Cyber Security aufgebaut, in welchem laufend aktuelle E-Learnings und physische Schulungen zur Erhöhung der IKT-Sicherheit durchgeführt werden. Im Jahr 2020 finden zudem ausserordentliche Stichproben bei der Ablage von klassifizierten Informationen statt. Weiter verfügt die FUB seit Beginn 2020 über die ICT Warrior Academy, wo Fachspezialisten auf die neuen Anforderungen der Armee vorbereitet und mit neuen Kompetenzen ausgestattet werden.