Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Band: 96 (2021)
Heft: 7-8

Artikel: "Der Mensch bildet im Bereich Cybersicherheit die Frontlinie"
Autor: Besse, Frederik / Amsler, Hans-Ulrich
DOI: https://doi.org/10.5169/seals-977163

«Der Mensch bildet im Bereich Cybersicherheit die Frontlinie»

Kennen Sie die sieben Regeln der Cybersicherheit? Das ist wichtig, denn als Angehöriger der Armee gehört man zur Frontline der Cybersicherheit. Hans-Ulrich Amsler, Chef Cyber Fusions Center ad interim und zusätzlich Chief Information Security Officer der FUB, gibt einen Überblick.

Hptm Frederik Besse

Allgemein: Können Sie unseren Lesern und Leserinnen Ihre Funktion beschreiben?

Hans-Ulrich Amsler: Seit etwas mehr als zwei Jahren verantworte ich das Cyber Fusion Center, welches aus dem Security Operation Center (SOC), dem militärischen Computer Emergency Response Team (milCERT), einem Team zur Betreuung der Überwachungslösungen (INWE) und einem Team für die Lagedarstellung besteht (CyOC).

Derzeit darf ich zudem ad interim die Rolle des Chief Information Security Officers (CISO) der FUB übernehmen. In dieser Rolle bin ich unter anderem für die Informationssicherheit und das Risikomanagement zuständig. Die Beratung der Geschäftsleitung in allen Sicherheitsfragen, bei Bedrohungen und wenn es um die Einhaltung der Compliance-Vorgaben geht, gehört auch zu meinen Aufgaben. Konkret schützen wir in dieser Abteilung die IKT-Infrastruktur vor Angriffen im Cyberraum

Können Sie uns einen Einblick in die Massnahmen zum Schutz der Cyber-Infrastruktur des VBS geben?

Amsler: Die Armee schützt in erster Linie ihre eigene Informatik-Infrastruktur. Zum einen wird der Schutz der bestehenden Infrastruktur laufend auf Schwachstellen geprüft und wo nötig angepasst. Zum anderen werden Unregelmässigkeiten durch unseren Sensorverbund erkannt und deren Ursache untersucht. Zudem wird mit dem Kommando Cyber die neue Digitalisierungsinfrastruktur gebaut. Diese Plattform wird uns einen grossen Sprung nach vorne in der Digitalisierung, aber auch im Bereich Sicherheit verschaffen.

Was sind aktuelle Projekte?

Amsler: Eines der Themen im Bereich Sicherheit, das uns im Moment beschäftigt, ist die Initiative «Sicherheit, Abbau und Werterhalt», kurz SAW.

Damit wird bei der bestehenden Informatik-Infrastruktur der Schutz den aktuellen Bedrohungen angepasst und, wo dies nicht möglich ist, die Systeme isoliert.

Das ist ein aufwendiges Unterfangen, da die bestehende Informatik-Infrastruktur historisch gewachsen ist und aus ganz verschiedenen Technologien der vergangenen Jahrzehnte besteht.

Weiter ist die Sensibilisierung der Mitarbeitenden und der Miliz ein ständiges Thema. Der Mensch bildet im Bereich Cybersicherheit die Frontlinie und muss genau wissen, wie er oder sie sich in gewissen Situationen zu verhalten hat.

Bild: VBS

Hans-Ulrich Amsler verantwortet die Informationssicherheit der FUB. In seiner Milizfunktion war er bisher Kp Kdt einer Spitalbat Stabskp, S3 eines Spitalbat sowie Of zVf des Kommandanten der Log Brigade 1.

Innerhalb der Berufsorganisation der Führungsunterstützungsbasis gibt es zu diesem Zweck zum Beispiel einen eigens dafür erstellten Adventure-Room, in dem das Thema Cyber- und Informationssicherheit trainiert werden kann.

Die Mitarbeitenden der Gruppe Verteidigung und auch von anderen Verwaltungseinheiten werden regelmässig im Rahmen einer Phishing-Kampagne geprüft und falls nötig auf das richtige Verhalten hingewiesen.

Welche Vorsichtsmassnahmen kann jeder WK-Soldat im Dienst einhalten, um zur Cybersicherheit des Verbandes beitragen?

Amsler: Das sind die sieben Regeln der Cybersicherheit:

1. Äusserungen in sozialen Medien sind immer als öffentlich anzusehen.
2. Niemals fremde oder private USB-Geräte an Systeme der Armee oder der Verwaltung anschliessen.
3. Öffentliche Hotspots können schädlich sein. Ein Hotspot des eigenen Handys ist sicherer.
4. WLAN, Bluetooth, GPS, NFC, etc. sind deaktiviert, ausser sie werden bewusst benötigt.
5. Handys, Uhren und Notebooks sind potenzielle Wanzen. Vor vertraulichen oder geheimen Gesprächen diese Geräte wegschliessen.
6. Keine Mitteilungen/Anhänge/Links unerwarteter Herkunft öffnen. Bei Verdacht den Absender telefonisch kontaktieren.
7. Bei Verdacht auf Malware-Infektion schnellstmöglich die Netzverbindung trennen, das Gerät laufen lassen und den Verdacht der Hotline oder dem Vorgesetzten melden.

Die Regeln sind auch unter diesem QR-Code auffindbar