Fighting hackers : Cyber-Lehrgang der Schweizer Armee gestartet

Autor(en): **Lanz, Lina / Flück, Robert**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **184 (2018)**

Heft 8

PDF erstellt am: **03.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-813206

Fighting hackers – Cyber-Lehrgang der Schweizer Armee gestartet

Am 6. August 2018 beginnt der Cyber-Lehrgang: 25 handverlesene Rekruten und Kader starten in eine intensive und anspruchsvolle Ausbildungsphase mit hoch gesteckten Zielen. Mit dem Cyber-Lehrgang baut die Schweizer Armee ihre Cyber-Fähigkeiten aus und verstärkt die personelle Durchhaltefähigkeit.

Lina Lanz, Robert Flück

Kann ein Cyber-Lehrgang im Rahmen der Grundausbildungslehrgänge der Schweizer Armee mit mindestens 20 Teilnehmern durchgeführt werden? Und genügen die Teilnehmer dann nach dem Abschluss des Lehrgangs den hohen Einsatzanforderungen im Bereich Cyber? Zur Klärung dieser Fragen bildeten die FUB und das Kdo Ausb Ende 2017 ein Projektteam aus Berufsmilitärs und Cyber-Spezialisten der Berufsorganisation FUB. Um die Arbeiten breit abzustützen, wurden Vertreter des GS-VBS und SBFI, Miliz-Offiziere des Stabs FUB sowie auch der Branchenverband ICT-Switzerland miteinbezogen. Das Projektteam erarbeitete in den letzten sechs Monaten ein Lehrgangskonzept, welches nun mit dem Pilot-Lehrgang umgesetzt und überprüft wird.

Entstehung und Konzeption

Mit der WEA erfolgt der Ausbau im Bereich Cyber auf eine Kompanie mit einem Bestand von rund 100 Cyber-Spezialisten. Um den daraus entstehenden Nachwuchsbedarf sicherzustellen, wird die seit 2010 bestehende Cyber-Ausbildung in der Elektronischen Kriegführung Schule 64 (EKF S 64) angepasst. Bis anhin wurden pro RS zwei bis vier Rekruten auf den Einsatzsystemen der FUB direkt durch die Berufsorganisation ausgebildet. Aufgrund der zukünftig höheren Teilnehmerzahl kann dieser Ansatz nicht mehr weiterverfolgt werden und die Ausbildung wurde in Teilbereichen neu konzipiert. Daraus entstand der Cyber-Lehrgang, der mit dem Start der RS 2/2018 als Pilot-Lehrgang das erste Mal in der EKF RS 64 durchgeführt wird.

Selektion und Ausbildung

Aufgrund des grossen Stoffumfangs reicht die Dauer einer RS nicht aus. Die Ausbildung dauert – vergleichbar mit der Ausbildung zum Fallschirmaufklärer – darum 40 Wochen und jeder Rekrut absolviert die Weiterausbildung zum Wachtmeister. Bis die Rekrutierung über den normalen Prozess läuft (geplant ist per

Die Kandidaten beim Assessment in Jassbach. Bild: VBS

RS 1/20), werden interessierte und geeignete Kandidaten aus den RS schweizweit ausgewählt. Die Armee will insbesondere auch Frauen für den Cyber-Lehrgang gewinnen.

Auf die Selektion wird viel Wert gelegt: Es werden sowohl online und schriftliche Tests als auch persönliche Interviews durchgeführt. Einerseits, weil der Lehrgang mit viel und anspruchsvollem Stoff eine überdurchschnittliche Motivation

«Der Schlüssel zum Erfolg ist die sorgfältige Selektion.»

und Durchhaltewillen erfordert. Andererseits ist es essentiell, die Rekruten im persönlichen Gespräch kennenzulernen, weil der vermittelte Stoff nicht mutwillig falsch angewendet werden darf. Die ausgewählten Rekruten werden anschliessend an die allgemeine militärische Grundausbildung den Cyber-Lehrgang absolvieren.

Die 800 Stunden Ausbildung umfassen von Ethik und Recht, über Kenntnisse der Informatik- und Kommunikationstechnologie (IKT) bis hin zu der klassifizierten Ausbildung in ihrem eigentlichen Fachbereich. Letztere abhängig davon, in welche der drei Funktionen die Einteilung erfolgt (vgl. Kasten). Daneben wird die einsatzbezogene Ausbildung auch *on the Job* in Kleindetachementen auf den Einsatzsystemen bei der Berufsorganisation FUB durchgeführt.

Weil sich Bedrohung, Verfahren und Mittel im Cyber-Raum ungewöhnlich schnell weiterentwickeln, wird die Fachverantwortung des Lehrgangs bei der FUB bleiben. Damit ist sichergestellt, dass die Einsatzerfahrung wieder in den Lehrgang einfliesst. Die Verantwortung für die Durchführung des Lehrgangs liegt beim Kdo Ausb. Teilnehmer mit ungenügender Leistungen oder problematischem persönlichem Verhalten werden in das Provisorium versetzt. Falls keine Verbesserung eintritt, erfolgt die Umteilung in eine andere Funktion innerhalb der EKF.

Kooperation mit Privatwirtschaft

Dem Lehrkörper wurde besondere Beachtung geschenkt, damit eine Vernetzung mit der Berufswelt oder dem Studium garantiert ist. Das Konzept des Cyber-Lehrgangs wurde dem Verband ICT-Berufsbildung Schweiz vorgestellt, welcher die Zusammenarbeit von Anfang an sehr begrüsste. Nach eingehender Prüfung des Lehrgangstoffes, können die Absolventen des Cyber-Lehrgangs ab Herbst 2019 den «Cyber Security Specialist mit eidgenössischem Fachausweis» erlangen. Durch die enge Zusammenarbeit mit der Privatwirtschaft und den Bildungsinstituten bietet der Lehrgang den Teilnehmenden mit dem eidgenössischen Fachausweis einen grossen Vorteil für ihr Berufsleben. Unterrichtet wird der Inhalt durch ausgewiesene Spezialisten ihres Gebiets. Die Armee konnte erfahrene Dozenten als Unterstützung für den Cyber-Lehrgang gewinnen. Momentan noch in Prüfung ist, ob man den Cyber-Lehrgang auch mittels ECTS-Punkten im Studium anrechnen lassen kann.

Vorteil Miliz

Die Armee kann, dank unserem Milizsystem, auf gut ausgebildete Rekruten zählen. Im Gegensatz zu ausländischen Berufsarmeen wird im Cyber-Lehrgang nicht mit dem Einmaleins der IKT begonnen. Aufgrund der Lehre, Matura, Studium oder autodidaktisch angeeigneten Kenntnissen kann man auf fundiertem Wissen aufbauen. Dieses wird während den 40 Wochen intensiv erweitert, vertieft, angewendet und den militärischen Bedürfnissen angepasst. «Wir sind in der Schweiz in der hervorragenden Lage, dass wir dank unserem Bildungssystem mit gut ausgebildeten jungen Menschen in den Lehrgang starten können», betont auch der Chef Führungsunterstützungsbasis, Divisionär Thomas Süssli.

Die Armee verfolgt nebst dem Lehrgang noch einen weiteren Weg, um die Cyber-Kompanie so rasch als möglich vollständig zu alimentieren. Militärdienstpflichtige Cyber-Spezialisten, die ihre Berufsausbildung abgeschlossen haben, können sich auch nach der militärischen Grund- bzw. Weiterausbildung in die Cyber-Kompanie umteilen lassen. Nach dem Abschluss des Cyber-Lehrgangs bietet sich auch die Möglichkeit, eine militärische Karriere via Offizierslaufbahn einzuschlagen; einem Absolventen stehen alle Türen offen. Der Nachwuchsbedarf verlangt, dass pro Lehrgang mindestens ein Wachtmeister die (zusätzliche) Selektion besteht und den Vorschlag für die Offiziersschule des Lehrverbands Führungsunterstützung erhält.

Abhängig von Stärken und Kenntnissen werden die AdA in eine der drei Funktionen eingeteilt:

Spezialist CNO

Computer Network Operations (CNO) mit Aufgaben unter anderem als Entwickler von Softwarewerkzeugen, Analyst von Cyber-Ereignissen und -Attacken sowie Analyst von Schwachstellen.

Spezialist milCERT

Spezialist militärisches Computer Emergency Response Team (milCERT) mit Aufgaben unter anderem als Analyst in einem Security Operation Center (SOC) mit Analysen von Cyber-Bedrohungen auf die Informatik- und Kommunikationstechnik-Systeme der Armee, Incidentmanagement sowie technische und forensische Untersuchungen.

Spezialist Cyber Defence

Spezialist im Rahmen Cyber Defence (CYD) mit nachrichtendienstlichen Aufgaben unter anderem in der Lage-Analyse und -Darstellung für die Abwehr von Cyber-Angriffen, sowie Unterstützung (auch technisch/forensisch), Beratung und Ausbildung von Truppen im Feld.

Für eine sichere Schweiz

Die Miliz unterstützt die Berufsorganisationen im Eigenschutz der militärischen Informationssysteme und Informatiknetzwerke, stellt die personelle Durchhaltefähigkeit sicher und ergänzt fachspezifische Fähigkeiten. Mit dem neu konzipierten Cyber-Lehrgang und damit ausgebildeten Fachkräften hat die Schweizer Armee den Bereich Cyber gestärkt, um für eine sichere Schweiz in allen Lagen und allen Operationsräumen einzustehen. Für die Schweizer Armee gilt das Motto: Kämpfen, schützen, helfen – gerade auch im Cyber-Raum. ■

Lina Lanz
Master of Arts, hist.
Wissenschaftliche Mitarbeiterin Cyber Defence
FUB
3003 Bern

Oberst i Gst
Robert Flück
Stabschef
FUB
3003 Bern