Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 12

Artikel: Ist die Schweizer Armee für den Cyberkrieg gerüstet?

Autor: Brechbühl Diaz, Denise

DOI: https://doi.org/10.5169/seals-1052828

Ist die Schweizer Armee für den Cyberkrieg gerüstet?

Am Armeeanlass «Connected» wurde das Zielbild der Schweizer Armee einem grossen Publikum vorgestellt. Cyberrisiken spielen eine grosse Rolle. Eine Umfrage zeigt, dass das Bewusstsein bei Armeeangehörigen gegenüber Cyberrisiken kaum vorhanden ist.

Denise Brechbühl Diaz

Eines Tages könnte die Schweizer Armee Zielscheibe eines Cyberangriffes werden. Falls so ein Fall eintrifft, muss die Armee bereit sein, die Schweiz zu schützen und zu verteidigen. Das ist ein Kernauftrag der Armee, so steht es in der Bundesverfassung. Dieser Fall ist nicht so unwahrscheinlich, wie viele denken mögen. Im Falle des russischen Angriffskrieges auf die Ukraine zeigt sich zwar, dass ein Cyberangriff nicht allein über Sieg oder Niederlage eines Krieges entscheidet. Er kann aber ein Land destabilisieren und einen strategischen Vorteil für den Angreifenden in der Kriegsführung erbringen.

«Durch den Krieg in der Ukraine hat sich gezeigt, dass der Cyberraum die erste Verteidigungslinie einer Nation bildet», sagt Divisionär Alain Vuitel, Projektleiter Kommando Cyber der Schweizer Armee. Und weiter: «Der Krieg in der Ukraine hat uns im Projekt Kommando Cyber viele Erkenntnisse gegeben. Primär will ich hervorheben, wie wichtig der Wissens- und Entscheidungsvorsprung gegenüber einem Gegner ist.»

Die Bedrohungslage im Cyberraum stellt auch einen wichtigen Punkt im Bericht «Die Verteidigungsfähigkeit stärken» von Korpskommandant Thomas Süssli, Chef der Armee, und Divisionär Alain Vuitel dar, der Mitte August im Rahmen des Armeeanlasses «Connected» vorgestellt wurde. «Connected war ein grosser Erfolg», so Divisionär Vuitel. «Zum ersten Mal konnte sich die Schweizer Bevölkerung und auch unsere Angehörigen der Armee ein umfangreiches Bild unserer Mittel im Bereich Cyber machen.»

Wo steht die Schweizer Armee heute?

Der sicherheitspolitische Bericht vom November 2021 gab die Richtung vor und forderte unter anderem die Verstärkung des Schutzes vor Cyberbedrohungen und eine stärkere Ausrichtung der Armee auf das hybride Konfliktbild. Auch politisch wurde die Bedeutung von Risiken im Cyberraum früh erkannt. Eine Motion von FDP-Nationalrat Josef Dittli verlangte 2017, dass ein Cyberdefence-Kommando mit Cybertruppen aufgebaut wird. Der Bericht «Gesamtkonzeption Cyber» vom April 2022 zeigt zudem die Grundlage für die kommenden Jahre.

«Die häufigste Sicherheitslücke stellt der Mensch dar.»

Philipp Leo, Experte für Cybersicherheit

Ab dem 1. Januar 2024 wird das Kommando Cyber durch den vom Bundesrat zum Divisionär ernannten Oberst i Gst Simon Müller operationell funktionieren. Die Führungsunterstützungsbasis wird in ein militärisches Kommando Cyber weiterentwickelt, welches sich auf die einsatzkritischen IKT-Leistungen zugunsten der Armee und ihrer Partner im Sicherheitsverbund fokussiert.

Mängel im Cybersicherheits-Bewusstein

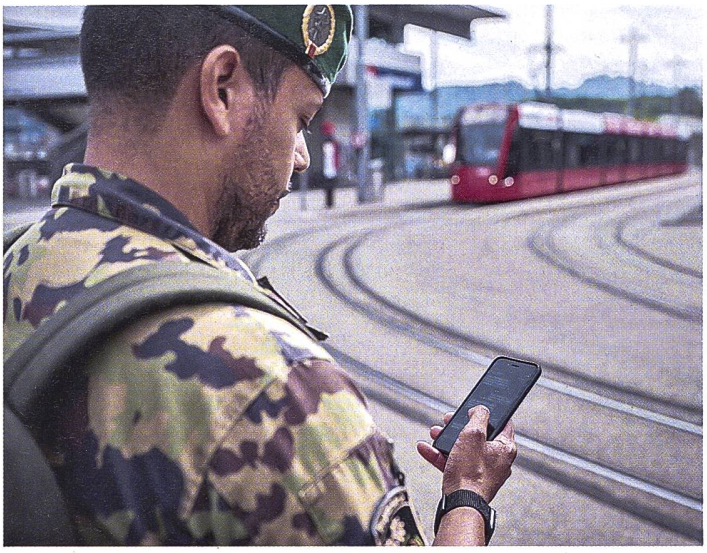
Wie steht es um das Bewusstein von Cyberbedrohungen bei den Angehörigen der Armee, sowohl bei den Soldatinnen und Soldaten als auch beim Kader? Als Grundlage für diesen Artikel wurde eine Umfrage geführt. Zwischen dem 15. August und dem 15. September 2023 wurden über das Schweizer Onlinetool «Findmind» Bataillonskommandanten befragt. In der Schweiz gibt es aktuell 115 Bataillonskommandanten, davon wurden über einen Linkedin-Aufruf und per E-Mail-Anfrage 50 Bataillonskommandanten angeschrieben, 18 Personen haben an der Umfrage teilgenommen. Unter den Befragten sind Bataillonskommandanten aus den deutsch-, französisch- und italienischsprachigen Kantonen vertreten.

15 der 18 Befragten hatten den Eindruck, dass Cyberangriffe die Auftragserfüllung der Armee gefährden können. In einer Skala von 1 bis 5 (5 = sehr gut, 1 = gar nicht gut) fühlten sich zehn Kommandanten bei einer Zahl von 3 (mittel) durch die Armee und Vorgesetzte in Bezug auf Cybersicherheit ausreichend unterstützt. Aus der Sicht von zehn Kommandanten stellt ebenfalls die Nutzung von sozialen Medien im Dienst ein Sicherheitsrisiko dar. Und 13 Kommandanten waren der Meinung, dass es nicht genügend Sensibilisierung bei den Soldatinnen und Soldaten gibt, damit sie während des Dienstes keine operativen Informationen preisgeben, die einem Angreifer von Nutzen sein könnten.

Instagram, Linkedin und Tiktok sind beliebte Social-Media-Plattformen. Bei einer Aufrufaktion wurden letzten Frühling Bilder vom Militärdienst auf dem Business-Netzwerk Linkedin geteilt. Informationen wie diese eignen sich dafür, gezielt Informationen zur Schweizer Landesverteidigung zu sammeln. Es ist erlaubt, Beiträge aus dem Militärdienst auf den sozialen Netzwerken zu veröffentlichen. Voraussetzung ist aber, dass die Geheimhaltungsvorschriften eingehalten werden müssen. Die Armee appelliert an die Eigenverantwortung. «Die häufigste Sicherheitslücke stellt der Mensch dar», erklärt Philipp Leo. Er ist Experte für Cybersicherheit und unterrichtet unter anderem im Cyberlehrgang der Armee. Je nach Studie beinhalten 70 bis 90 Prozent aller Cyberangriffe ein menschliches Fehlverhalten*.

Die Zusammenarbeit soll gestärkt werden

Bei der Umfrage gaben 13 von 18 Befragten an, dass Cybersicherheit bei allen Truppengattungen und Funktionen zur Ausbildung dazu gehören sollte. Und 12 gaben an, dass sie als Bataillonskommandanten nicht genug Know-how und Ressourcen haben, um sich vor einem Cyberangriff zu schützen. Denn derzeit sind die Fähigkeiten und die Expertise in den Operationssphären Cyber und Elektromagnetischer Raum überwiegend im Kommando Cyber konzentriert. Eine funktions- und truppengattungsübergreifende Zusammenarbeit scheint es derzeit auf Stufe Bataillon nicht zu geben. «Wir sind bestrebt, den Kommandanten al-



◀ Die Sensibilität der Armeeangehörigen bei der Benutzung von Social Media soll gesteigert werden.
Bild: Clemens Laub, VBS

ler Stufen und unseren Soldaten und Kader den Wissens- und Entscheidvorsprung zu garantieren. Bereits heute bilden wir mit dem Cyberlehrgang Cyberspezialisten der Armee aus und im Technischen Lehrgang Cyber Stabsoffiziere und Kommandanten. Wir dürfen keineswegs zulassen, dass es ein Silo-Denken gibt, bei dem jede Organisationseinheit der Armee primär für sich selbst schaut», so Divisionär Alain Vuitel. Er betont: «Nur als Gesamtsystem Armee können wir im Ernstfall bestehen und dabei spielt per se der Informationsaustausch eine zentrale Rolle.»

Das Kommando Cyber ist bestrebt, den Armeeangehörigen aller Stufen den Wissens- und Entscheidungsvorsprung zu garantieren. Seit 2018 können Rekrutinnen und Rekruten auch einen Cyberlehrgang absolvieren und in Zusammenarbeit mit der Höheren Kaderausbildung der Armee (HKA) werden spezifische Ausbildungen zu diesem Thema durchgeführt. Seit diesem Jahr hat die Armee die kostenlose Sparc-Vorausbildung lanciert, um Jugendliche und junge Erwachsene für die Cybersicherheit zu begeistern. Mitmachen können Schweizer Staatsbürgerinnen und -bürger über 16 Jahre, welche die Rekrutenschule noch nicht begonnen haben.

Zukunft Pilotprojekt

Für mehr Bewusstein im Bereich Cybersicherheit wurde im Wiederholungskurs der Pz Stabskp 12 in Zusammenarbeit mit dem Cyber Bataillon 42 ein Pilotprojekt initiiert. «Mit dem Pilotprojekt wollen wir die Cybersicherheit bei konventionellen Truppen genauer untersuchen», sagt Elena Lanfranconi, Initiantin des Pilotprojekts und Kompaniekommandant der Pz Stabskp12. Das Projekt zeigte, dass es unter den Soldatinnen und Soldanten ein mangelndes Bewusstein gegenüber Cyberrisiken gibt und es für Laien schwierig ist, die Risiken richtig einzuschätzen. Bei jeder Übung müssen bei der Wahl von Standort, Aufbau und Betrieb die Cybergefahren berücksichtig werden. Diese erkannten Schwächen stellen eine Bedrohung dar und können sich negativ auf die Einsatzfähigkeit der Kompanie auswirken. Ziel des Pilotprojekts war es, dass sich ein Cyberspezialist des Cyber Bataillon 42 während drei Tagen einen Überblick verschaffen konnte.

Zu Beginn bestanden gegenseitige Kenntnislücken im Bereich Cyber und im Bereich Panzertruppe. Eine vertiefte Ausbildung in der Cybersicherheit erhalten ausser den Cybersoldaten im Cyber Bataillon 42 keine andere Truppengattung oder Funktion. Während den 18 Wochen in der Rekrutenschule erlernen die Rekrutinnen und Rekruten den Umgang mit Waffen und Ausrüstung, die Ausbildung in der erwählten Funktion (zum Beispiel Panzer) und auch Grundkenntnisse im Sanitätswesen. Während des Besuchs wurde eine Bestandesaufnahme innerhalb der Truppe zur Selbsteinschätzung zu Cybersicherheit geführt.

Es hat sich gezeigt, dass auch bei den Soldatinnen und Soldaten ein Bedürfnis nach einer Ausbildung im Bereich Cyber besteht. Viele Cyberrisiken, auf die der Cyberexperte während der Übung hingewiesen hat, waren weder Kader noch Soldaten bewusst gewesen. Daher soll im Dienst eine Checkliste durchgearbeitet werden, auf welcher alle möglichen Cybergefahren aufgelistet werden. Zum Beispiel soll bei der Standortwahl darauf geachtet werden, dass zivile Überwachungskameras abgedeckt werden. Bei zivilen Überwachungskameras und Webcams besteht die Gefahr, dass sich ein Gegner in das System hacken und die Truppen ausspionieren könnte.

Seit letztem Jahr sollen Armeeangehörige die kostenpflichtige Messaging-App Threema für die dienstliche Kommunikation nutzen. Threema hat ihren Sitz in der Schweiz und laut Unternehmen befinden sich alle Server in der Schweiz. Anders als bei amerikanischen Messaging-Dienste wie Whatsapp unterliegt Threema nicht dem sogenannten Cloud Act. Nach diesem Gesetz verpflichtet es Unternehmen mit Sitz in den USA, den US-Behörden Zugriff auf gespeicherte Daten zu gewähren. Beim Pilotprojekt zeigte sich, dass zwar unter den Kadern einheitlich mittels Threema kommuniziert wird, aber dass Whatsapp unter den Soldaten weiterhin sehr verbreitet ist. Es gibt keine Sanktionen, wenn Armeeangehörige trotzt Verbot andere Messaging-Dienste als Threema verwenden. Auch werden Apps wie zum Beispiel Google Maps für die Navigation benutzt oder um den militärischen Standort zu teilen. Um diese Sicherheitslücken zu schliessen, braucht es laut dem Cyberspezialisten eine konsequente Nutzung von Kommunikationsmitteln, die von der Armee bewilligt werden.

Das Projekt ist nicht abgeschlossen. Nächstes Jahr werden die Handlungsfelder vertieft, damit bedarfsgerechte Ausbildungsinhalte erstellt werden können. «Um eine Standardausbildung im Bereich Cyber für alle Truppengattungen zu entwickeln, müssen aus meiner Sicht WK-Formationen und Schulen einbezogen werden», sagt Hauptmann Lanfranconi. Sie hat die Auswertungen ihrem Bataillonskommandanten und dem Cyber Bataillon 42 vorgelegt. ■

Dieser Text wurde durch Unterstützung der Akademien der Wissenschaften Schweiz ermöglicht und am 3. November in Bern gewürdigt.

* Zum Beispiel: https://www.hslu.ch/de-ch/hochschule-luzern/ueber-uns/medien/medienmitteilungen/2022/05/06/cyber-risk-management/, https://www.proofpoint.com/de/resources/threat-reports/human-factor

Denise Brechbühl Diaz
Freie Journalistin
8008 Zürich