Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 98 (2023)
Heft: 12

Artikel: Ist die Schweizer Armee für den Cyber-Krieg gerüstet?
Autor: Brechbühl Diaz, Denise
DOI: https://doi.org/10.5169/seals-1053084

Ist die Schweizer Armee für den Cyber-Krieg gerüstet?

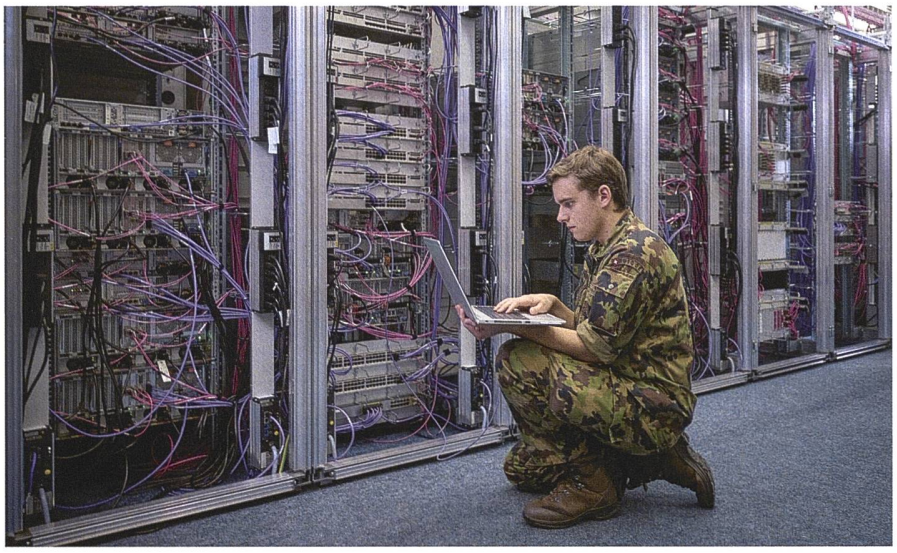
Am Armeeanlass «Connected» wurde das Zielbild der Schweizer Armee einem grossen Publikum vorgestellt. Die Verteidigung hat dabei einen hohen Stellenwert eingenommen. Cyber-Risiken spielen in diesem Szenario weiterhin eine grosse Rolle. Wie eine Umfrage zeigt, ist das Bewusstsein bei Armeeangehörigen gegenüber Cyber-Risiken kaum vorhanden.

Text und Analyse von Denise Brechbühl Diaz

Eines Tages könnte die Schweizer Armee Zielscheibe eines umfassenden und grossflächigen Cyber-Angriffes werden. Tritt ein solcher Fall ein, 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 vielleicht jetzt denken. Im Falle des russischen Angriffskrieges auf die Ukraine zeigt sich zwar, dass ein Cyber-Angriff nicht allein über Sieg oder Niederlage eines Krieges entscheidet, es kann aber ein Land destabilisieren und einen strategischen Vorteil für den Angreifenden in der Kriegsführung erbringen.

«Es hat sich durch den Krieg in der Ukraine 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».

Um sich auf die neue Bedrohungslage im Cyberraum einzustellen, möchte sich die Schweizer Armee wieder mehr auf die Verteidigung ausrichten. Dafür hat die Führung der Armee ein Zielbild ab 2023 ausgearbeitet und dazu den Bericht «Die Verteidigungsfähigkeit stärken» durch Korpskommandant Thomas Süssli, Chef der Armee, und Divisionär Alain Vuitel den Medien Mitte August an «Connected» vorgestellt. «Connected» war der grösste Armeeanlass seit Jahren und fand vom 16. bis zum 20. August 2023 auf dem Waffenplatz Kloten-Bülach statt, mit dem Fokus auf die Themen Digitalisierung und Cyber. «Connected war ein grosser Erfolg», so Divisionär Alain Vuitel. «Zum ersten Mal konnten sich die Schweizer Bevölkerung und auch unsere Angehörigen der Armee ein umfangreiches Bild unserer Mittel im Bereich Cyber machen».



Im Cyber Lehrgang bildet die Schweizer Armee Cyber Spezialistinnen und Spezialisten aus.

Wo steht die Schweizer Armee?

Eine kurze Vorgeschichte: Der sicherheitspolitische Bericht vom November 2021 gab die Richtung der Armee 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 des FDP-Nationalrates Josef Dittli verlangte 2017, dass ein Cyberdefence-Kommando mit Cybertruppen aufgebaut wird. Der Bericht «Gesamtkonzeption Cyber» vom April 2022 zeigt weiter die Grundlage für die kommenden Jahre. Diese Konzeption dient als Grundlage für den neuen vorgestellten Bericht «Die Verteidigungsfähigkeit stärken», welcher an «Connected» präsentiert wurde.

Der Bericht ist ein Beweis dafür, dass die Verteidigung im Cyberraum gestärkt werden muss. Ab dem 1. Januar 2024 wird das Kommando Cyber durch den vom Bundesrat zum Divisionär ernannten Oberst i Gst Simon Müller operationell funktionieren. Die derzeit existierende Führungsunterstützungsbasis (FUB) wird in ein militärisches Kommando Cyber weiterentwickelt, welches sich auf die einsatzkritischen IKT (Informations- und Kom-

munikationstechnik)-Leistungen zugunsten der Armee und ihrer Partner im SVS (Sicherheitsverbund Schweiz) fokussiert.

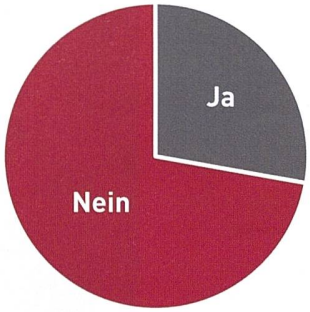
Analyse der Awareness

Wie steht es um die Awareness von Cyber-Bedrohungen 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» Kommandanten auf Stufe Truppenkörper, befragt. Ein Bataillon ist die kleinste taktische Formation der Schweizer Armee, welche eigenständig einen Kampf führen kann. Aus diesem Grund wurden auch Bataillonskommandanten für die Umfrage ausgewählt. In der Schweiz gibt es 115 Bataillonskommandanten, davon wurden über einen LinkedIn-Aufruf und per E-Mail-Anfrage 50 Bataillonskommandanten angeschrieben und 18 Personen haben an der Umfrage teilgenommen. Unter den Befragten sind Bataillonskommandanten aus den deutsch-, französisch- und italienischsprechenden Kantonen vertreten.

15 von 18 der Befragten hatten den Eindruck, dass Cyber-Angriffe die Auftragserfüllung der Armee gefährden können. In einer Skala von 1 bis 5 (5 = sehr gut, 1 = gar nicht gut) fühlten sich 10 Kommandanten bei einer Zahl von 3 (mittel) durch die Armee und Vorgesetzte in Bezug auf Cybersicherheit ausreichend unterstützt. Aus der Sicht von 10 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.

Gibt es genügend Awareness bei den Soldat:innen, damit sie im Dienst keine operativen Informationen preisgeben?



Ja	5
Nein	13
Anzahl Teilnehmer an der Umfrage	**18**

Grafik: SCHWEIZER SOLDAT

Instagram, LinkedIn und Tiktok sind beliebte Social-Media-Plattformen. Bei einer Aufruf-Aktion wurde letzten Frühling ein Bild 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 Cyber-Lehrgang der Armee. Je nach Studie nutzen 70 bis 90 Prozent aller Cyber-Angriffe ein menschliches Fehlverhalten.

Stärkere Zusammenarbeit

Bei der Umfrage gaben 13 von 18 Befragten an, dass Cybersicherheit bei allen Truppengattungen und Funktionen zur Ausbildung gehören sollte. Und zwölf gaben an, dass sie als Bataillonskommandanten nicht genug Knowhow und Ressourcen haben, um sich vor einem Cyber-Angriff zu schützen. Aktuell sind die Fähigkeiten und die Expertise in den Operationssphären Cyber und elektromagnetischem 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 aller Stufen und unseren Soldaten und Kadern den Wissens- und Entscheidvorsprung zu garantieren. Bereits heute bilden wir mit dem Cyber Lehrgang Cyber Spezialisten der Armee aus und bilden im Technischen Lehrgang Cyber Stabsoffiziere und Kommandanten weiter. 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». →

Bei der Umfrage gaben 13 von 18 Kommandanten an, dass nicht genügend Kenntnisse über Cybergefahren bei den Soldatinnen und Soldaten vorherrschen.

Das Kommando Cyber ist bestrebt, den Armeeangehörigen aller Stufen den Wissens- und Entscheidungsvorsprung zu garantieren. Seit 2018 können Rekrutinnen und Rekruten einen Cyber-Lehrgang absolvieren, und in Zusammenarbeit mit der Höheren Kaderausbildung der Armee HKA werden spezifische Ausbildungen zu diesem Thema durchgeführt. Seit diesem Jahr 2023 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 Awareness im Bereich Cybersicherheit wurde im Wiederholungskurs (WK) der Panzer Stabskompanie 12 in Zusammenarbeit mit dem Cyber Bataillon 42 ein Pilotprojekt initiiert. «Mit dem Pilotprojekt wollen wir die Cybersicherheit bei konventionellen Truppen genauer untersuchen», sagt Hauptmann Elena Lanfranconi, Initiantin des Pilotprojekts und Kompaniekommandant der Panzerstabskompanie 12. Das Projekt zeigte, dass es unter den Soldatinnen und Soldanten eine mangelnde Awareness gegenüber Cyber-Risiken gibt und es für Laien schwierig ist, die Risiken richtig einzuschätzen. Bei jeder Übung müssen bei der Wahl von Standort, Aufbau und Betrieb die Cyber-Gefahren 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 Cyber-Spezialist 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 ausschliesslich die Cybersoldaten des Cyber Bataillons 42. Während den 18 Wochen in der Rekrutenschule erlernen die Rekrutinnen und Rekruten den Umgang mit Waffen und Ausrüstung, die Ausbildung in der erwählten Funktion und auch Grundkenntnisse im Sanitätswesen. Während des Besuchs wurde eine Bestandesaufnahme innerhalb der Truppe zur Selbsteinschätzung bezüglich Cybersicherheit geführt. Es hat sich gezeigt, dass auch bei den Soldatinnen und Soldaten ein Bedürfnis nach einer Ausbildung im Bereich Cyber besteht.

Bilder: VBS

Das Kommando Cyber wird ab dem 1. Januar 2024 operationell.

Viele Cyberrisiken, auf die der Cyberexperte während der Übung hingewiesen hat, waren weder Vorgesetzten noch Soldaten bewusst gewesen. Daher soll im Dienst eine Checkliste durchgearbeitet werden, auf welcher alle möglichen Cybergefahren aufgelistet werden. Zum Beispiel soll bei der Wahl vom Standort darauf geachtet werden, dass zivile Überwachungskameras verdeckt werden. Bei zivilen Überwachungskameras und Webcams besteht die Gefahr, dass sich ein Gegner in das System hacken und die Truppen ausspionieren könnte.

Threema als sichere Alternative

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-Diensten wie «WhatsApp» unterliegt Threema nicht dem sogenannten «Cloud Act». Dieses Gesetz berechtigt 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 oder um den militärischen Standort zu teilen, benutzt. Um diese Sicherheitslücken zu schliessen, braucht es laut dem Cyberspezialisten eine konsequente Nutzung von Kommunikationsmitteln, die von der Armee bewilligt wurden.

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.

Dieser Text wurde durch Unterstützung der Akademien der Wissenschaften Schweiz ermöglicht und am 3. November 2023 in Bern gewürdigt.

Der Text erschien als erstes in der Dezember-Ausgabe der Allgemeinen Schweizerischen Militärzeitschrift ASMZ.