Wie sich die Schweizer Armee gegen Cyber-Angriffe wappnet

Der Cyber-Defence Campus (CYD) antizipiert Cyber-Entwicklungen und ist Bindeglied zwischen VBS, der Industrie und der Wissenschaft in allen cyber-relevanten Themen. So entwickelte er beispielsweise ein Verfahren für eine effizientere Abwehr von Cyber-Attacken auf der Basis von maschinellem Lernen. Ziel dieses CYD Campus-Projekts ist es, dass die Armee in Zukunft globale Angriffsversuche zuverlässig und in Echtzeit aufspüren kann.

Alain Mermoud, Vincent Lenders, Patrizia Zwygart

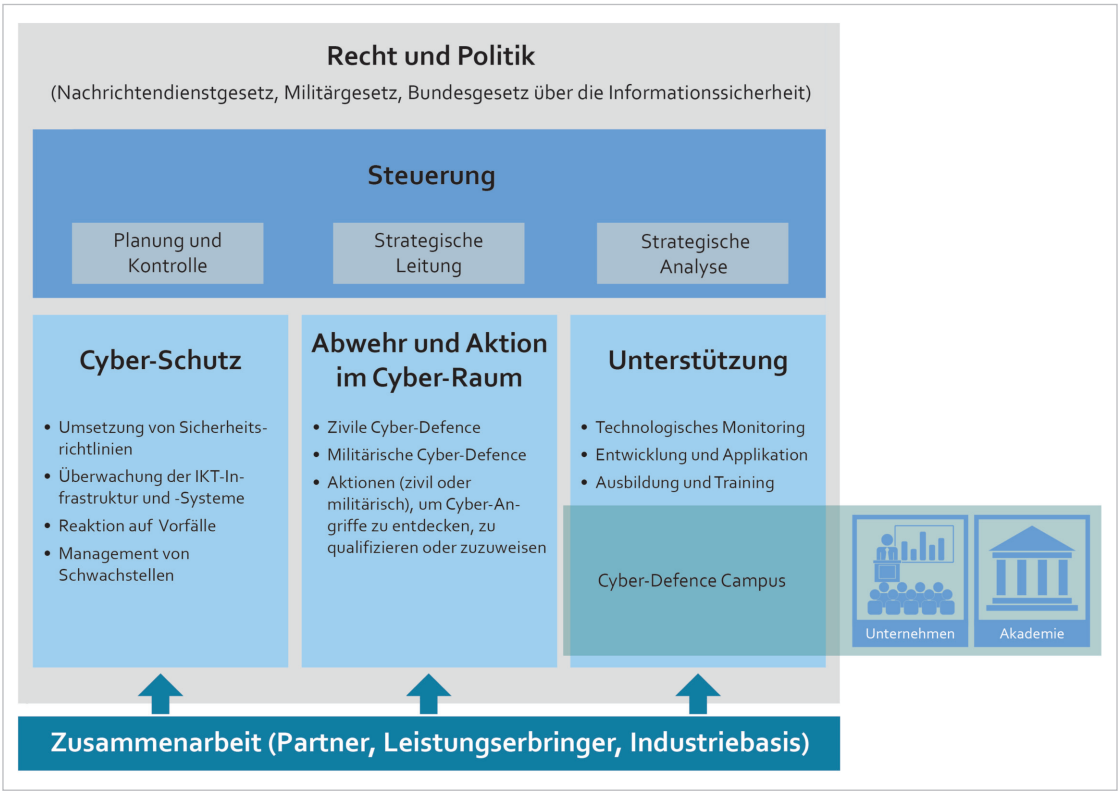
Kommunikation via Social Media, nützliche Assistenten wie Smartphones, Einkaufen mit wenigen Klicks – die Digitalisierung bietet uns viele Erleichterungen. Aber: Sie birgt auch viele Risiken, insbesondere im sicherheitspolitischen Bereich. Immer mehr unserer Daten und Kommunikation sind online. Wichtige Infrastrukturen wie Strom- und Wasserversorgung oder der Zahlungsverkehr sind digital. Schaffen es Hacker, in diese Steuerungen einzudringen oder private Daten zu stehlen, kann für die gesamte Gesellschaft grosser Schaden entstehen. Der Schutz vor Cyber-Angriffen wird deshalb immer wichtiger.

Ein Netzwerk für die nationale Sicherheit

Im Januar 2019 hat unter der Federführung von armasuisse Wissenschaft und Technologie der Cyber-Defence Campus in Thun seinen offiziellen Betrieb aufgenommen. Der Auftrag umfasst die Früherkennung der rasanten Entwicklungen im Cyber-Bereich, die Entwicklung von Technologien zur Abwehr und die Ausbildung von Cyber-Fachkräften. Um den Zugang zu den neusten Entwicklungen, Erkenntnissen und Trends im Cyber-Bereich sicherzustellen, arbeitet der CYD Campus eng mit der Eidgenössischen Technischen Hochschule in Zürich (ETHZ) und der École polytechnique fédérale de Lausanne (EPFL) zusammen.

VBS stärkt Cyber-Defence-Partnerschaft mit der ETH Zürich

Der CYD Campus nahm im September 2019 sein «Labor» an der EPFL in Betrieb und im November 2019 eröffneten Verteidigungsministerin Viola Amherd und ETHZ-Präsident Joël Mesot den Standort an der ETHZ. Neben den Studierenden werden an diesen beiden Standorten auch die Industrie und internationale Partner in die Arbeit mit eingebunden. Die Schwerpunkte der Partnerschaft liegen auf der Förderung des Technologie- und Innovationstransfers mit Priorität auf Cyber-Sicherheits-Technologien, Informationssicherheit, Datenwissenschaft und künstlicher Intelligenz. Am Eröffnungsanlass in Zürich betonte Bundesrätin Amherd, der CYD Campus diene als Antizipationsplattform für Cyber-Entwicklungen und sei da-



Der Aktionsplan Cyber-Defence (APCD) des VBS umfasst drei Säulen, eine davon ist der Cyber-Defence Campus von armasuisse Wissenschaft und Technologie. Der Aktionsplan soll bis 2020 umgesetzt werden. Grafik: VBS

Bundesrätin Viola Amherd weihte den Cyber-Defence Campus an der ETH ein, gemeinsam mit dem Direktor des ZISC Srdjan Capkun, dem Leiter des Cyber-Defence Campus Vincent Lenders, dem ETH Präsidenten Joël Mesot sowie Andreas Häberli von Dormakaba (v. l. n. r). Bild: Autoren

rüber hinaus «Plattform und Bindeglied zwischen VBS, der Industrie und der Wissenschaft in allen cyber-relevanten Themen».

Das VBS stellt sich den Cyber-Herausforderungen

Der CYD Campus ist eine von verschiedenen Massnahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), die gestartet wurde, um den aktuellen Herausforderungen in der «Cyber-Welt» effektiver begegnen zu können. Der Aktionsplan für Cyber-Defence des VBS definiert zwei weitere Handlungsfelder:

- Die Führungsunterstützungsbasis (FUB) stellt den sicheren Betrieb der informations- und kommunikationstechnischen (IKT) Systeme und Infrastrukturen der Verteidigung sicher;
- Der Nachrichtendienst und die Verteidigung entdecken und qualifizieren Cyber-Attacken militärischer und ziviler Art und finden deren Ursprung.

Ist die Schweizer Armee gegen Cyber-Angriffe gewappnet?

An der weltweit grössten internationalen *Cyber-Defence*-Übung «Locked Shields» nehmen jährlich über 1000 Cyber-Experten teil. Hier zeigt sich, wie gut die Schweizer Armee gegen Cyber-Angriffe gerüstet ist. Diese Übung wird einmal jährlich vom *NATO Cooperative Cyber Defence Center of Excellence* von Tallinn (Estland) organisiert. Ein Team von versierten Angreifern, das sogenannte *Red Team,* stellt während mehreren Tagen die Abwehrkräfte verschiedener Nationen auf die Probe. Nationale Teams von IT-Spezialisten, die als *Blue Teams* fungieren, helfen jeweils einem fiktiven Land, sich gegen die breit angelegten Cyber-Angriffe des *Red Teams* zu verteidigen. Mit von der Partie ist auch das von der Führungsunterstützungsbasis (FUB) geführte *Blue Team* der Schweiz. Das zu schützende Netzwerk besteht aus traditionellen Computern und Servern, aber auch aus Geräten mit Software-Applikationen für kritische Infrastrukturen sowie Routern und Geräten für die drahtlose Mobilfunkkommunikation. Während der gesamten Übung greift das *Red Team* die Systeme der *Blue Teams* an. Dabei werden die Aktivitäten in dem von den *Blue Teams* geschützten Netzwerk aufgezeichnet. Nach der Übung werden die *Blue Teams* bewertet und das *Red Team* berichtet über die verwendeten Angriffsmethoden sowie Taktiken, damit die *Blue Teams* ihre Verteidigungsstrategien verbessern können.

Die Chefin VBS im Gespräch mit dem Leiter des Cyber-Defence Campus. In ihren sicherheitspolitischen Überlegungen nehmen Cyber-Themen einen hohen Stellenwert ein. Bild: Autoren

Cyber-Angriffe in Echtzeit aufspüren

Bereits im Vorfeld der Übung evaluierte der CYD Campus, gemeinsam mit Studenten der von Prof. Laurent Vanbever geführten Gruppe der ETH Zürich, mehr als 300 GB Aufzeichnungen von vergangenen *Locked Shield*-Übungen. Sie analysierten das Verhalten sowie die verwendeten Mittel der Angreifenden mittels maschinellen Lernens und entwickelten daraus eigene Erkennungs- und Interventionstechniken.

Erfolgreicher Einsatz maschinellen Lernens in der Armee

Um die Armee mit dieser neuen Methode zu befähigen, arbeitete der CYD

Maschinelles Lernen

Maschinelles Lernen ist eine Disziplin der künstlichen Intelligenz. IT-Systeme werden dadurch in die Lage versetzt, aufgrund von Daten und Algorithmen, Muster und Gesetzmässigkeiten zu erkennen und Modelle zu entwickeln.
Anhand eines solchen Modells lassen sich anschliessend Aufgaben lösen, wie zum Beispiel die Klassifikation von Objekten oder die Detektion von Anomalien. Maschinelles Lernen gewinnt für die Armee zunehmend an Bedeutung. Nämlich überall dort, wo Daten digital vorliegen und somit vom Computer schneller und effizienter analysiert werden können als von einem Menschen.

Campus eng mit der Führungsunterstützungsbasis der Armee (FUB) zusammen. Die neuen Verfahren wurden von Cyber-Wachmeistern in bestehende Systeme der FUB integriert und so erweitert, dass die Detektion der Angriffe mit den vorhandenen Netzwerkaufzeichnungssystemen der FUB in Echtzeit funktionieren. Im April 2019 setzte das Schweizer *Blue Team* das Verfahren erstmals an der *Locked Shields*-Übung ein. Die Übung bestätigte, dass die Methodik sehr effizient ist, um Angriffe eines *Red Teams* in Echtzeit aufzuspüren. Die Methodik erreichte eine Identifikationsgenauigkeit von 99% und eine Rückrufquote von mehr als 90%. Die Ergebnisse des Projekts stellte der CYD Campus an der NATO-Konferenz über Cyber-Konflikte (CyCon 2019) im Mai 2019 in Tallinn vor. Dadurch profitieren andere Nationen, aber auch zivile Organisationen, von den gewonnenen Erkenntnissen für ihre eigene Verteidigung.

Ebenso bedeutsam wie der Erfolg des Verfahrens ist jedoch die Art und Weise, wie ein solches Projekt in weniger als einem Jahr von der Idee bis zur erfolgreichen Umsetzung durchgeführt werden konnte. Dank der engen Verbindung zwischen der Grundlagenforschung an der ETH Zürich und den operativen Cyber-Organisationseinheiten der Armee konnte der CYD Campus gewonnene Erkenntnisse und neues Wissen sehr rasch und agil in die Armee transferieren und umsetzen. Im Gegenzug hat die Armee neue Praxiserfahrungen und Fragestellungen gewonnen, welche wiederum als neue Projekte im CYD Campus aufgenommen und dieses Jahr zusammen mit den Hochschulen weitergeführt werden.

Die Digitalisierung bringt uns viel. Der CYD Campus hilft mit, dass es vor allem Chancen und nicht Risiken sind. ■


Capitaine
Alain Mermoud
armasuisse W+T
Leiter Tech. Monitoring
Cyber-Defence Campus
1015 Lausanne


Vincent Lenders
armasuisse W+T
Direktor
Cyber-Defence Campus
3602 Thun


Patrizia Zwygart
armasuisse W+T
Projektleiterin
Unternehmensentwicklung
3602 Thun