RISK MANAGEMENT

Cyber-Abwehr der Armee wird durch Miliz verstärkt

Lesezeit: 4 Minuten

Divisionär Alain Vuitel, Projektleiter Kommando Cyber Schweizer Armee, will 600 Cyberspezialistinnen und -spezialisten aus der Miliz im Dienst.

Von Sandra Escher Clauss
am 14.06.2021
Quelle: HZ Insurance

Herr Divisionär, wodurch unterscheidet sich das Risk Management in der Armee vom Risk Management in der Wirtschaft?
Die Risiken, welche die Armee sowie die Partner im Sicherheitsverbund Schweiz bewältigen müssen, gehen über diejenigen aus der Wirtschaft hinaus. Als einzige sicherheitspolitische Reserve der Schweiz muss die Armee stärker mit Risiken wie Spionage, Sabotage sowie physischen Angriffen rechnen und muss in der Lage sein, diese Risiken zu antizipieren und ihnen zu begegnen – egal in welcher Lage. Ein weiteres Beispiel sind Waffensysteme, die mit ICT unterstützt werden. Deren Manipulation hätte für den Erfolg des Auftrags und für die Sicherheit der Truppe verheerende Konsequenzen. Das muss bei der Sicherheitskonzeption beachtet werden. Um dieses Risiko zu minimieren, werden entsprechend hohe Aufwände unternommen.

Gilt das Risiko der Spionage, Sabotage und der physischen Angriffe nicht auch für privatwirtschaftliche Unternehmen?
Doch, das ist selbstverständlich auch für zivile und private Organisationen relevant, daher werden über die in der Nationalen Cyber-Strategie NCS definierten Kanäle innerhalb der Bundesverwaltung auch Informationen geteilt. Die Armee als letzte Sicherheitsreserve für die Schweiz muss aber für alle Fälle gewappnet sein.

AUCH INTERESSANT

BERUF
Aktivistin fordert eine Revolution des Milizsystems

POLITIK
EDA erneut von Hackern heimgesucht

SICHERHEIT
Ständerat will Cyber-Rekrutenschule schaffen

Wie muss man sich das Teilen von Informationen vorstellen?
Ein Beispiel wäre das Teilen von Informationen über Manipulationen oder Hintertüren in der Produktelieferkette. Um diese zu verhindern oder zu kontrollieren, werden in der Armee speziell überprüfte Sicherheitskomponenten eingesetzt, die zwar höhere Kosten aufweisen, dank denen die Risiken jedoch vermindert werden können.

Was genau unternimmt die Armee?
Analog zur Wirtschaft werden auch in der Armee die Risiken der Informationssicherheit über ein Information Security Management System gesteuert. Neben der Auftragserfüllung werden dabei Vertraulichkeit, Integrität und Verfügbarkeit behandelt.

Die Armee ist ein zentraler Cyber-Leistungserbringer für die Strategie Cyber des VBS.

Was heisst das?
Die Strategie Cyber wurde im Generalsekretariat des VBS in Zusammenarbeit mit allen Verwaltungseinheiten erarbeitet. Aus dem Projekt Kommando Cyber wurden Inhalte heraus- und in die Strategie hineinintegriert.

«Die Cyber-Kräfte der Armee sind in erster Linie dazu da, die eigene Infrastruktur zu schützen.»

Gab es davor keine Cyber-Strategie?
Die Armee stellte bereits vor der Formulierung der Strategie Cyber des VBS Leistungen im Bereich der hochsicheren ICT zur Verfügung. Einerseits für sich selbst und anderseits für weitere Leistungsbezüger innerhalb des Departements VBS, beispielsweise für den Nachrichtendienst des Bundes oder das Bundesamt für Bevölkerungsschutz.

Damit die Schweizer Armee wie auch ihre Partner in Notlagen und Krisen einsatzfähig bleibt, muss sie jederzeit über Systeme der Informations- und Kommunikationstechnik verfügen können. Autonome Rechenzentren, ein Übertragungsnetz und ein mobiles Kommunikationsnetz bilden die Grundpfeiler für die neue Digitalisierungsplattform. Die Armee und weitere Partner des Sicherheitsverbundes Schweiz, welche als Anforderungen die Sicherheit, den permanenten Betrieb und die Autonomie haben, sollen zukünftig auf dieser Plattform ihre Services wie Daten und Sprache betreiben können.

Welche Bereiche des Cyber-Schutzes übernimmt die Armee und für welche sind die Unternehmen selbst zuständig?
Die Cyber-Kräfte der Armee sind in erster Linie dazu da, die eigene Infrastruktur zu schützen. Das ist die neue Frontline der Landesverteidigung. Das ist also eine Parallele zur Wirtschaft, in der ebenfalls jede Organisation für die eigene Sicherheit zuständig ist.

Die Armee kann über die Kantone auch für subsidiäre Unterstützung im Cyber-Bereich angefragt werden, sollten die zivilen Mittel für die Bewältigung eines Vorfalls nicht ausreichen. Also gleich wie bei der Corona-Pandemie – nur dass dann keine Sanitätssoldaten ausrücken, sondern Cyber-Soldaten. Die Armee kann den Kantonen, dem Sicherheitsverbund oder der Wirtschaft subsidiär nur Unterstützung bieten, wenn die folgenden Bedingungen erfüllt sind: die zivilen Mittel sind erschöpft, geeignete militärische Mittel sind vorhanden und die Bewilligung der Politik liegt vor.

«Die Armee beschafft Informationen über Mittel und Methoden von verschiedenen besonders gefährlichen Cyber-Akteuren und wertet

diese aus.»

Woher holt sich die Armee das Wissen im Bereich Cyber-Risiken?
Die Armee nimmt regelmässig an nationalen und auch internationalen Cyber-Übungen teil. An diesen findet ein wichtiger Wissensaustausch statt und die Erfahrungswerte, die dabei gesammelt werden, fliessen wieder zurück in die eigene Planung und Organisation.

Darüber hinaus ist es einer der zentralen Pfeiler in der Cyber-Sicherheit, sich mit Partnerorganisationen auszutauschen. Sei dies über aktuelle Angriffsmuster, aber auch über Erfahrungen und bewährtes Vorgehen. Die Armee beschafft ausserdem – zum Zweck des Eigenschutzes – Informationen über Mittel und Methoden von verschiedenen besonders gefährlichen Cyber-Akteuren und wertet diese aus. Weiter findet natürlich auch zwischen Profi und Miliz ein wertvoller Erfahrungsaustausch statt. Die Angehörigen der Miliz kommen in den Dienst und bringen ihre Erfahrungen aus der Privatwirtschaft mit – die Erfahrungen aus dem Dienst nehmen sie wiederum zurück in die Arbeit in der Privatwirtschaft. Diesen Mehrwert generiert das Milizsystem allgemein, nicht nur im Cyber-Bereich.

Apropos Milizsystem, wie ist die «Cyber-Truppe» organisiert?
Innerhalb der Armee ist die Führungsunterstützungsbasis der Armee beziehungsweise das zukünftige Kommando Cyber für die Leistungen im Bereich ICT und Cyber verantwortlich. Die Leistung wird durch Berufspersonal und Milizpersonal erbracht. Der Einsatz des Milizpersonals erhöht die Durchhaltefähigkeit, welche für die Leistungserbringung in allen Lagen von zentraler Bedeutung ist. Das heisst, dass das Berufspersonal und das Milizpersonal bereits heute eng zusammenarbeiten.

«Die Armee bietet im Bereich Cyber einzigartige Aufgabenfelder und auch die Sinnhaftigkeit ist einzigartig.»

Im Rahmen der Revision der Armeeorganisation werden per 1.1.2022 zwei Cyber-Formationen (ein Cyber-Bataillon und ein Fachstab Cyber) gebildet. Dies ermöglicht der Armee, zukünftig bis zu 600 Armeeangehörige in diesem Bereich einzusetzen. Die Alimentierung dieser Formationen dürfte vier bis sechs Jahre dauern.

Was ist in Sachen Cyber das Worst-Case-Szenario für die Armee?
Eines der Worst-Case-Szenarien, das leider kein Szenario mehr ist, ist der Fachkräftemangel und der Brain Drain zu Positionen in der Privatwirtschaft, die besser bezahlt werden. Die Armee bietet im Bereich Cyber einzigartige Aufgabenfelder und auch die Sinnhaftigkeit ist einzigartig.

Nebst dem wäre es für uns am schlimmsten, wenn unsere Infrastrukturen dahingehend manipuliert würden, dass die Erfüllung unseres Auftrags erschwert oder verunmöglicht wird. Zum Beispiel, indem die Logistik beeinträchtigt, die Führungsprozesse gestört oder ausgespäht oder Waffensysteme wirkungslos gemacht werden. Die Verhinderung dieser Szenarien erfordert Massnahmen, welche oft über die klassischen Sicherheitsmassnahmen in der Privatwirtschaft hinausgehen. Aus diesem Grund prüfen wir laufend unsere Lieferketten sowie die Vertrauenswürdigkeit unserer Partner.

Die **Market Opinion: Cyberrisiken managen** wird in Zusammenarbeit mit **Aon Schweiz** realisiert.

Hier geht es zum Dossier. Bisher erschienen:

Cyber-Risiken zu managen, erfordert eine zirkulierende Strategie

Cyberrisiken: Der Stromwirtschaft drohen Milliardenschäden

Cybersecurity als Herausforderung für die Logistikindustrie

Divisionär Alain Vuitel, Projektleiter Kommando Cyber der Schweizer Armee, im Interview

THEMEN PER E-MAIL FOLGEN

#Armee Folgen

#Cyber Security Folgen

#Cyberabwehr Folgen

#Risk Management Folgen

HZ Insurance: Das Neuste aus der Branche

Erhalten Sie wöchentlich unseren Newsletter mit den aktuellsten News aus der Versicherungsbranche. Wir laden Sie herzlich ein, diesen für den Moment kostenfrei zu testen.

Ihre E-Mail-Adresse

Anmelden