Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cyber-Security aus der Sicht der Politik

Kurzreferat anlässlich Meeting Rotary Club Schwyz, 17.5.2018

Josef Dittli, Ständerat
Präsident der sicherheitspolitischen Kommission

Ausgangslage

- IKT hat Verhalten der Gesellschaft massiv verändert
- Viele Vorteile und Chancen
- Neue Risiken und Gefahren; Missbrauch für kriminelle, wirtschaftliche, nachrichtendienstliche, machtpolitische oder terroristische Zwecke
- Störungen, Manipulationen und gezielte Angriffe, die via elektronische Netzwerke ausgeführt werden, sind Risiken, die mit einer Informationsgesellschaft einhergehen.
- Weitere Zunahme zu erwarten.

Frachtschiff von Moller Maersk: Die weltweit grösste Containerschiffsreederei wurde im Juni 2017 von Hackern angegriffen

Foto: Getty Images; Quelle: KPMG/Zurich/Gartner/Statista

4000 kaputte Server, 300 Millionen Dollar Verlust

Eine Cyber-Attacke richtete bei der Reederei Maersk grosse Schäden an. Schweizer Versicherer hingegen sehen ein neues Geschäftsfeld

Hans-Jürgen Maurus

Zürich Die Zahlen sind alarmierend. Auf rund 500 Milliarden US-Dollar belaufen sich die Schäden durch weltweite Cyber-Attacken jährlich, sagte WEF-Direktor Alois Zwinggi in Davos. Er stellte dort ein neues globales Zentrum für Cybersicherheit vor. Und zählt Hackerangriffe zu den dringlichsten Problemen unserer Zeit.

Pro Firma oder Organisation verursachten Cyberkriminelle 2017 global Kosten von 11,7 Millionen Dollar, schätzt die US-Beratungsgesellschaft Accenture. 2016 lag der Wert noch rund ein Viertel tiefer. Dass der Schaden auch ein Vielfaches höher sein kann, zeigt der Fall Moller Maersk.

Die grösste Containerschiffsreederei der Welt mit Sitz in Dänemark wurde im Juni 2017 von Hackern angegriffen. Man habe ihn nach der Attacke um 4 Uhr früh aus dem Bett geholt, berichtete Verwaltungsratspräsident Jim Snabe in Davos. Mithilfe der Verschlüsselungssoftware Notpetya hatten Unbekannte die gesamte IT des Konzerns lahmgelegt. Maersk musste laut Snabe 4000 Server, 45 000 Computer und 2500 Programme austauschen. «Wir waren zehn Tage komplett offline», so Snabe, «erlitten Umsatzeinbussen von 20 Prozent und mussten die restlichen 80 Prozent unseres Geschäfts von Hand abwickeln.»

Den Schaden beziffert der Konzern mittlerweile auf 250 bis 300 Millionen Dollar. Das sei ein wichtiger Weckruf für ihn gewesen, so das Fazit des Maersk-Topmanagers Snabe, der einen 2017 auch mit dem Erpressertrojaner Wannacry deutlich, der 200 000 Computer in 150 Ländern lahmlegte. Rund 80 Krankenhäuser in Grossbritannien, aber auch die Deutsche Bahn waren betroffen. US-Experten machen Nordkorea für den schweren Angriff verantwortlich. Die Hacker hatten eine Schwachstelle im Betriebssystem Windows XP ausgenutzt, für das Microsoft keine Updates mehr anbot. Der US-Konzern hat das nach der Attacke nachgeholt.

Die meisten Schweizer KMU schützen sich nicht richtig

Auch für Schweizer Unternehmen zählen Cyber-Angriffe zum Alltag. Das ergab eine Studie der Unternehmensberatung KPMG von 2017, bei der 60 einheimische Firmen befragt wurden. 88 Prozent von ihnen gaben an, in den letzten zwölf Monaten Opfer von Attacken geworden zu sein – eine Zunahme im Vergleich zum Vorjahr um satte 34 Prozent.

Mehr als die Hälfte der betroffenen Firmen musste die Ge-

Bereits 2016 stellte die Zurich Versicherung in einer Umfrage fest, dass Schweizer KMU schlecht für Cyber-Angriffe gerüstet sind. Lediglich 2,5 Prozent der befragten Firmen haben ausreichende Schutzmassnahmen. Aufgerechnet auf alle Schweizer KMU heisst

Allerdings: Gerade für die Versicherungsbranche liegt hier auch ein Geschäftsfeld. Die Zurich Insurance Group bietet seit 2009 Cyberversicherungen in 20 Ländern an. Die Police bietet Deckung gegen eigene Schäden der Kunden sowie Haftpflichtschäden, bei denen Dritte in Mitleidenschaft gezogen wurden. In einigen Ländern wie der Schweiz gibt es zwei Varianten von Cyberpolicen: eine für KMU mit Prämien ab 440 Franken pro Jahr und eine für Konzerne je nach Grösse.

Künstliche Intelligenz erzeugt «selbstmutierende Viren»

Laut Zurich verzeichnet man in der Schweiz ein solides Wachstum bei den Prämieneinnahmen, das Potenzial sei hoch. Maya Bundt, Chefin der Abteilung Cyber und digitale Lösungen bei Swiss Re, schätzt, dass sich der Cyberversicherungsmarkt verdoppeln und bis 2020 ein Volumen von 7,5 Milliarden Dollar erreichen wird.

Aber: Gewisse Risiken mit katastrophalen Auswirkungen sind laut Swiss Re nicht versicherbar.

den potenziellen Schäden», so Swiss Re. Unternehmen müssten zudem «weit mehr tun», um Cyber-Abwehrmassnahmen in ihre Risikomanagementstrategien zu integrieren.

Der Schweizer Unternehmer André Kudelski warnt ebenfalls

«sehr ökonomisch und setzen neue Technologien für ihre Angriffe» ein. Auch künstliche Intelligenz (KI) könne für Attacken auf Infrastruktur verwendet werden, warnt Kudelski. KI sei wie ein «selbstmutierendes Virus», wodurch sich ständig neue Herausforderungen ergeben würden.

«Hacker wissen genau, wo sie nach Schwachstellen suchen müssen», warnt Assistenzprofessorin Jean Yang von der Fakultät für Computer Science der Carnegie-Mellon-Universität in Pittsburgh. Bei etlichen Krankenhäusern seien es veraltete Windows-XP-Betriebssysteme. Sogar die Wahlmaschinen in den USA liefen mit alter Software, wundert sich die Computerexpertin.

Chefjurist Timothy Murphy vom Kreditkartenspezialisten Mastercard beklagt fehlende Fachleute. Spitzenkräfte zu rekrutieren, sei ein «unüberwindbares Hindernis», man brauche in jedem Falle «mehr Cyber-Absolventen».

Dass die Gefahr wächst, die von Hackerattacken ausgeht, zeigt der

ten weltweit auf 3 Billionen Dollar steigen.

Als Hauptursachen für die aggressiven Cyber-Attacken nennt der Bericht das Erstarken des Darknet-Marktes, die zunehmende Nutzung von Cloud-Dienstleistungen und die Hartnäckigkeit der

Attacke auf Kraftwerk schreckt Schweizer Betreiber auf

Die Software Triton sollte ein Kraftwerk in Saudiarabien beschädigen. Der Angriff wirft die Frage auf, wie sicher kritische Industrieanlagen sind

Baden AG Im November 2017 ist eine Schadsoftware namens Triton im Nahen Osten entdeckt worden. Sie hat es auf Sicherheitssysteme in der Industrie abgesehen und alarmiert Cyberexperten und Infrastrukturbetreiber gleichermassen.

Der Angriff galt laut der US-Sicherheitsfirma Fireeye, deren Tochterunternehmen Mandiant den Vorfall entdeckte, einem Kraftwerk in Saudiarabien und wurde offenbar von einem staatlichen Akteur ausgeführt, vermutlich dem Iran. Ziel der Attacke war es, Schäden an der physischen Infrastruktur anzurichten. Dabei listen die Cyberkriminellen versehentlich eine Sicherheitsabschaltung des ganzen Systems aus – nur deshalb

Sicherheitskontrollsystem des französischen Konzerns Schneider Electric, der prompt eine Warnung veröffentlichte, aber sein Produkt als sicher bezeichnet. Nach Angaben des Konzerns sind 13 000 Anlagen mit Triconex ausgerüstet, darunter Energieunternehmen und Chemiefabriken.

BKW leitete «umgehend Abklärungen» ein

Der Angriff schreckte auch Schweizer Kraftwerksbetreiber wie die BKW auf. Nach dem Einsatz von Triton-Schadsoftware habe der Berner Energiekonzern «umgehend Abklärungen» eingeleitet, ob er potenziell von einem solchen An-

griff auf das iranische Nuklearprogramm entwickelt werden und dürfte 2010 bis zu 1000 Zentrifugen in der Atomanlage Natanz schwer beschädigt haben.

Bei der jüngsten Cyberattacke hat Triton die kritischen Sicherheitskontrollsysteme eines Infrastrukturbetreibers infiltriert. Die Angreifer versuchten, einen

Der Triton-Angriff wirft gleichwohl gravierende Fragen auf. Wie sicher sind kritische Infrastruktur- und Industrieanlagen im Zeitalter des sogenannten Internets der Dinge, in dem sogar Gegenstände miteinander vernetzt sind? Wie verwundbar sind ferngesteuerte Kontrollsysteme, wie sie der Industriekonzern ABB vom Forschungszentrum in Baden-Dättwil AG aus bei Bergbauminen in der ganzen Welt betreibt, darunter eine Kupferminе in Nordschweden? Satish Ganesu, Sicherheitsexperte bei ABB, räumt eine «zunehmende Anfälligkeit von Sicherheitslücken» aufgrund der «Weiterentwicklung der Bedrohungsakteure» ein.

WEF launches Global Centre for Cybersecurity (24.1.2018)

Die Aufgaben des Staates

- Sensibilisierung von Bevölkerung, Wirtschaft und Gesellschaft
- Wahrung der Handlungsfähigkeit des Staates
  - durch frühzeitige Erkennung von Gefahren (z.B. BND)
  - durch Schutz der eigenen Systeme
  - durch Vorgaben und Massnahmen bei Betreibern von kritischen Infrastrukturen
- Gesetzliche Rahmenbedingungen schaffen
  - zum Schutz der Bevölkerung
  - zur Regelung des Missbrauchs
  - zur Sanktionierung
- Betrieb einer zentralen Anlaufstelle
- Armee gemäss Art 58 BV

Kritische Infrastrukturen

- Fluglenkungssysteme (Skyguide, Flughäfen)
- Energieproduktionsanlagen (AKW, KW)
- Verkehrslenkungssysteme (Bahn, Autobahn)
- Gesundheitsinformationssysteme (ICT von Spitälern)
- Finanzlenkungssysteme
- Führungsanlagen von Bund und Kantonen
- Systeme der Armee
- …
- ….

Der Staat ist nicht für alles zuständig

- Jeder ist grundsätzlich für sich selber verantwortlich
- Firmen müssen selber für den Schutz ihrer Systeme sowie für die Einhaltung ihrer Vorgaben sorgen
- Der Staat ist «nur» dort zuständig, wo er selber betroffen ist

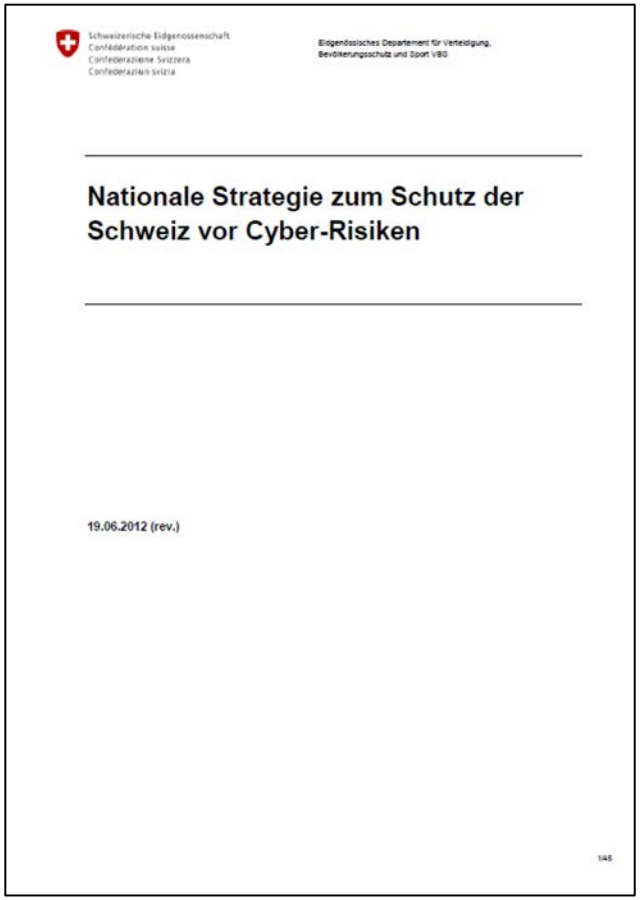
Rahmenbedingungen für Reduktion von Cyber Risiken

- das Handeln in Eigenverantwortung
- die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden
- die Kooperation mit dem Ausland.
- Mit einem permanenten gegenseitigen Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden.
- Der Staat soll nur eingreifen, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt.

Wo steht die Schweiz in Sachen Cyber-Security

- Nationale Strategie zum Schutz der Schweiz vor Cyber Risiken (NCS)
- Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)
- Sonderstab Informationssicherung (SONIA)
- Melde- und Analysestelle Informationssicherung (MELANI)
- Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
- Nachrichtendienst des Bundes: neue Kompetenzen mit dem revidierten NDG
- Bundesratsbeschluss zur 2. NCS
- Neues Informationssicherheitsgesetz
- Armee: am aufholen mit Aktionsplan Cyber-Defence

NCS 2012-2017


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

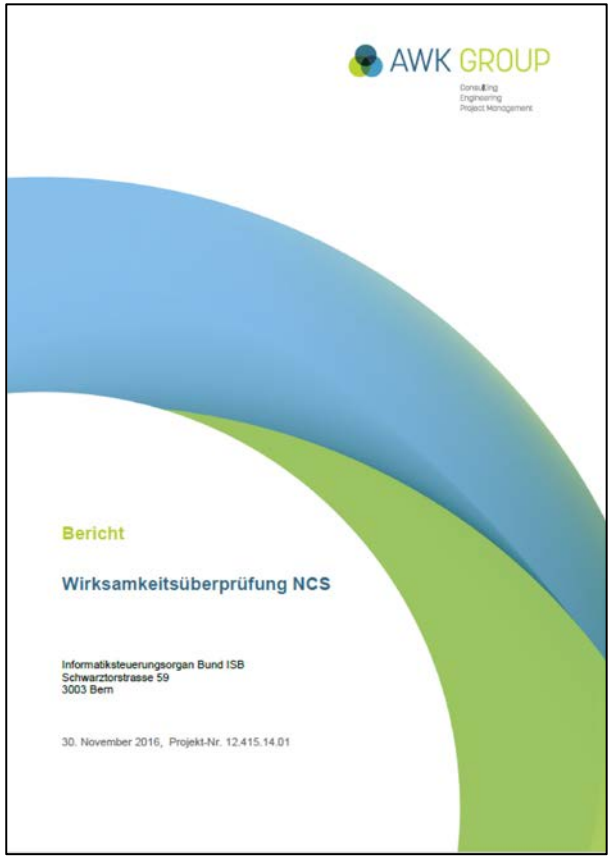
19.06.2012 (rev.)

Strategische Ziele

1. Frühzeitige Erkennung der Bedrohungen & Gefahren
2. Erhöhung Widerstandsfähigkeit der kritischen Infrastrukturen
3. Wirksame Reduktion von Cyber-Risiken

➔ **Umsetzung von 16 Massnahmen bis 2017 in den Bereichen Prävention, Reaktion, Kontinuität und unterstützende Massnahmen**

Wirksamkeitsüberprüfung NCS



- **Stärken**
  - **Umsetzung:** die Massnahmen wurden plangemäss umgesetzt (Wirkung bleibt aber noch schwierig messbar).
  - **Inhalt:** die Ziele waren grundsätzlich richtig gesetzt.
  - **Struktur:** die dezentrale Umsetzung der Massnahmen hat funktioniert.
- **Schwächen:**
  - **Unklare Zuteilung der Verantwortung:** es bleiben offene Fragen bezüglich der Zuständigkeiten (z.B. Krisenmanagement, Rolle Armee).
  - **Fehlende Sichtbarkeit:** in Politik, Wirtschaft und Öffentlichkeit wird die NCS wenig wahrgenommen.
  - **Fokus auf kritische Infrastrukturen:** Cyber-Risiken sind relevant für die gesamte Wirtschaft und Gesellschaft.
  - **Knappe Ressourcen**

Beschluss zur Überarbeitung der NCS (BRB vom 26.4.2017)

1. Kenntnisnahme des Jahresberichts NCS 2016, des strategischen Controllings der NCS per 31.12.2016 und des Berichts „Wirksamkeitsüberprüfung NCS"
2. Das ISB (Informatiksteuerungsorgan des Bundes) wird beauftragt, bis Ende 2017 eine Nachfolgestrategie auszuarbeiten
3. 30 Stellen zur Umsetzung der NCS werden weitergeführt
4. Das ISB prüft die Schaffung eines Ressourcenpools in der Bundesverwaltung zu Cyber-Risiken

Teilnehmende an den Workshops und eingegangene Stellungnahmen

- **Beteiligung an den Workshops zur Erstellung der Strategie:**
  - **Bundesstellen:** EDA (ASP), EDI (GS, BAG, BSV, MeteoSchweiz), EJPD (GS, fedpol), UVEK (BAKOM, BAV, BAZL, BFE), VBS (GS, BABS, FUB, NDB, armasuisse), WBF (BWL, SBFI), EFD (Expertengruppe Datensicherheit, BIT, ISB, FINMA), BK.
  - **Privatwirtschaft / Verbände:** economiesuisse, ICT-Switzerland, Schweizerischer Versicherungsverband (SVV), Swissmem, RUAG, Switch, Swisscom, UBS, SATW
  - **Kantone:** Vertretung durch Sicherheitsverbund Schweiz (SVS)

- **Stellungnahmen durch:**
  - ASUT, BKW, ElCom, ENSI, ETHZ, KKJPD, IBM, Post, PostCom, SECO, SWICO, Swiss Cyber Experts, Swissgrid, ZAS

Strategische Ziele NCS 2018-22

1) Die Schweiz verfügt über **Kompetenzen, Wissen und Fähigkeiten** zur Erkennung und Einschätzung der Risiken.
2) Die Schweiz entwickelt wirksame **Präventionsmassnahmen**.
3) Die Schweiz kann auch lang anhaltende und sektorübergreifende **Vorfälle bewältigen.**
4) Die kritischen Infrastrukturen sind gegenüber Cyber-Risiken **resilient.**
5) Der Schutz der Schweiz vor Cyber-Risiken wird als **gemeinsame Aufgabe** von Gesellschaft, Wirtschaft und Staat wahrgenommen.
6) Die Schweiz engagiert sich für die **internationale Kooperation** zur Erhöhung der Cyber-Sicherheit.
7) Die Schweiz **lernt aus Cyber-Vorfällen** im In- und Ausland.

10 Handlungsfelder der NCS 2018-22

- Kompetenzen- und Wissensaufbau
- Bedrohungslage
- Resilienzmanagement
- Standardisierung / Regulierung
- Vorfallbewältigung
- Krisenmanagement
- Strafverfolgung
- Cyber-Defence
- Internationale Cyber-Sicherheitspolitik
- Aussenwirkung und Sensibilisierung

➔ 28 konkrete Massnahmen in diesen zehn Handlungsfeldern

Wichtigste inhaltliche Neuerungen

- **Erweiterte Zielgruppen:** KMUs und Bevölkerung sollen auch adressiert werden. MELANI entwickelt Produkte für diese Zielgruppen.
- **Standardisierung:** Minimalstandards für IT-Sicherheit sollen in den verschiedenen kritischen Sektoren eingeführt werden.
- **Prüfung Meldepflicht:** eine Meldepflicht für Cyber-Vorfälle wird in Zusammenarbeit mit den zuständigen Behörden geprüft.
- **Cyber-Defence ist Teil der NCS:** die Arbeiten des VBS im Bereich Cyber-Defence sind integraler Bestandteil der NCS.

Organisation und Umsetzungsplan (in Bearbeitung)

- Die Strategie wird durch einen Umsetzungsplan ergänzt, welcher folgende Elemente enthält:
  - **Organisationsstruktur der NCS**: wer trägt die strategische Verantwortung, wer übernimmt die Koordinationsaufgaben, wer führt das Controlling durch?
  - **Zuständigkeiten für die Massnahmen**: welche Organisationseinheit setzt welche Massnahme um?
  - **Leistungsziele:** welche Leistungen müssen bis wann erbracht werden?
- Das Parlament fordert eine **Zentralisierung** der Aktivitäten zum Schutz vor Cyber-Risiken (**Motion Eder 17.3508** wurde im Stände- und Nationalrat angenommen).

➔ Die Entscheide des Parlaments werden im Umsetzungsplan NCS berücksichtigt.

Armee

- NATO und ihre Mitglieder definieren den Cyber Raum zu einem eigenständigen Operationsraum
- In der Armee sind die Mittel nicht in ausreichendem Masse vorhanden, um im Rahmen der Armeeaufträge den Bedrohungen angemessen begegnen zu können.
- Aktionsplan Cyber-Defence des VBS
- Motion Dittli
  - Der Bundesrat wird beauftragt, zur Erfüllung der Armeeaufträge (gemäss Art. 58 der Bundesverfassung) bei der Schweizer Armee Cybertruppen aufzubauen.
  - Die Cyberorganisation soll professionalisiert aus 100 bis 150 IT-/Cyberspezialisten bestehen, und milizmässig aus 400 -600 Angehörige der Armee umfassen.

Armee (2)

Motion Dittli

Leistungsprofil der Armee: Die Armee soll

- permanent und in allen Lagen seine eigenen Systeme und Infrastrukturen vor Cyberangriffen schützen;
- für den Verteidigungsfall befähigt sein, als Truppenkörper oder mit Teilen davon eigenständige Cyberoperationen durchzuführen (Cyberaufklärung, Cyberverteidigung, Cyberangriff);
- im Rahmen des Nachrichtendienstgesetzes (NDG) den Nachrichtendienst des Bundes (NDB) subsidiär unterstützen und dessen Systeme schützen;
- die Betreiber kritischer Infrastrukturen subsidiär unterstützen;
- die zivilen Behörden des Bundes und der Kantone bei Cyberangelegenheiten subsidiär unterstützen.

Armee (3)

Motion Dittli

Zu diesem Zweck soll die Schweizer Armee:

- eine enge Kooperation mit den Hochschulen (z. B. ETHZ, EPFL), der IT-Wirtschaft und Vertretern der potenziell gefährdeten Infrastrukturen (Energie, Verkehr, Banken usw.) eingehen;
- die notwendigen organisatorischen Konzeptionen wie Gliederung und Aufbau des Kommandos, Einsatzdoktrin, Anwerbung von IT-/Cyberspezialisten, Rekrutierung von IT-/Cybersoldaten, Ausbildung, Ressourcenbeschaffung usw. rasch vorantreiben.

Armee (4)

Antreten zur Cyber-Ausbildung

Berufsmilitärs müssen sich ab nächstem Herbst in IT-Sicherheit schulen lassen

Andreas Schmid

Spätestens seit dem Hackerangriff auf den Rüstungskonzern Ruag vor drei Jahren, von dem auch der Bund gravierend betroffen war, gibt der Schutz vor solchen Attacken zu reden. Mit einer Ausbildungsoffensive will das Verteidigungsdepartement (VBS) von Bundesrat Guy Parmelin die Armee nun für Cyberattacken wappnen. Ab Herbst müssen alle Berufsoffiziere, die an der ETH Zürich Militärwissenschaften oder Staatswissenschaften studieren, Vorlesungen und Übungen in Cyber-Sicherheitspolitik besuchen. Zudem wird dieser Bereich auch an der Militärakademie in Birmensdorf (ZH) in den Lehrplan integriert.

Mit einer Studienreform reagiert das Center for Security Studies an der ETH – dort werden angehende Berufsoffiziere ausgebildet – auf die wachsende Bedeutung der Cybersicherheit. «Die Armeekader müssen eine Vorstellung erhalten, wie der Cyberraum militärisch genutzt wird», sagt der Studiendirektor Andreas Wenger. Zudem habe die neue Kriegsform der Cyberangriffe eine weit grössere Dimension als die militärische.

Alle Soldaten schulen

Das VBS will über die Berufsoffiziere, die ihr Wissen weitergeben, künftig die ganze Truppe erreichen. «Es geht darum, sicherzustellen, dass die Armeeangehörigen wissen, was Cyberabwehr bedeutet, und dass sie für mögliche Gefahren im Umgang mit elektronischen Mitteln sensibilisiert sind», sagt VBS-Sprecher Renato Kalbermatten. Ein Grundwissen in Cybersicherheit gehöre zu einer modernen Ausbildung.

CHRISTIAN BEUTLER/KEYSTONE

Soldaten studieren an Computern mögliche Bedrohungslagen. (Kriens, 13. November 2013)

Studenten, die sich in einem ETH-Studium zum diplomierten Berufsoffizier ausbilden lassen, oder Akademiker, die nach abgeschlossenem Studium einen 18-monatigen Diplomlehrgang für Berufsoffiziere absolvieren, sind künftig verpflichtet, ein Semester lang Vorlesungen über Cyberabwehr, Abschreckungsstrategien oder Gegenmassnahmen zu elektronischen Attacken zu belegen.

Neben den neuen Lehrveranstaltungen für die Offiziere wird das VBS im Bereich Cyberabwehr auch an der Basis tätig. Im Sommer sollen erste Armeeangehörige, die beruflich mit IT vertraut sind, militärspezifisch geschult werden. «Ein erster Lehrgang ist als Pilotprojekt vorgesehen», sagt Kalbermatten. Sofern sich dies bewähre, werde diese Ausbildung künftig zweimal pro Jahr durchgeführt. So sollen nach Planung des VBS jedes Jahr 50 Cyberexperten rekrutiert und geschult werden. 400 bis 600 IT-Spezialisten möchte die Armee dereinst zur Verfügung haben, um Einheiten zu verstärken. Eine eigenständige Cybertruppe will das VBS nicht aufstellen.

Innerhalb des Departements sieht das VBS ausserdem vor, 100 zusätzliche Fachleute – heute sind 50 IT-Spezialisten im Cyber-Bereich tätig – zu rekrutieren. Bis Ende 2020 soll dieser Plan umgesetzt sein. Sprecher Kalbermatten hält fest, das Ziel sei ambitioniert: Das VBS müsse 300 Stellen einsparen und dürfe für die Cyberabwehr keine neuen Arbeitsplätze schaffen. Entsprechend muss das Departement in anderen Bereichen Stellen streichen. «Das Projekt Weiterentwicklung der Armee und andere Aufgaben dürfen dabei nicht gefährdet werden», sagt Kalbermatten.

Neue Studiengänge

Zumindest der Mangel an Fachkräften für Cybersicherheit sollte in den nächsten Jahren reduziert werden. Ausser der ETH und der Militärakademie bieten auch Fachhochschulen neue Ausbildungen an, wie die NZZ berichtete. Zum Beispiel jene in Luzern, die im Herbst einen Bachelor in Informations- und Cybersicherheit ins Programm aufnimmt. Der Hackerangriff auf die Ruag habe einen Ruck ausgelöst, stellt ETH-Professor Andreas Wenger mit Blick auf die Aktivitäten von Hochschulen und Behörden fest.

Vize von Geheimdienst entlastet

Der deutsche Generalbundesanwalt wolle das Verfahren gegen Paul Zinniker, den stellvertretenden Direktor des Nachrichtendiensts des Bundes (NDB), einstellen. Dies schreibt das deutsche Nachrichtenmagazin «Der Spiegel». Ein weiterer NDB-Mitarbeiter, gegen den ermittelt wurde, bleibt laut dem Bericht ebenfalls unbehelligt. Im Laufe der Untersuchung hätten sich keine weiteren Verdachtsmomente gegen die beiden Schweizer ergeben, die Einstellung des Verfahrens stehe bevor, berichtet «Der Spiegel» ohne Bezug auf eine Quelle.

Die beiden NDB-Mitarbeiter waren im Zusammenhang mit dem Fall des Schweizer Spions Daniel M. ins Visier der deutschen Ermittlungsbehörden geraten. Dieser sollte für den NDB in Deutschland Informationen über Steuerfahnder beschaffen und wurde verhaftet. Zinniker und ein weiterer NDB-Angestellter sollen Daniel M. beauftragt und instruiert haben, so der Vorwurf der deutschen Behörden.

Der Schweizer Geheimdienst habe sich vor einiger Zeit bei der Bundesanwaltschaft in Karlsruhe erkundigt, ob Zinniker eine Verhaftung drohe, wenn er nach Deutschland reise, heisst es im «Spiegel»-Bericht. Der stellvertretende NDB-Direktor plane, Hans-Georg Maassen, den Verantwortlichen für die deutsche Spionageabwehr, zu treffen. *(asc.)*

Cyber-Security aus der Sicht der Politik

Danke für
Ihre
Aufmerksamkeit