Digital Risk – Political Perspective

Swiss Risk Association

Josef Dittli, Ständerat
Präsident der sicherheitspolitischen Kommission

Ausgangslage

- Informations- und Kommunikationstechnologie haben Wirtschaft, Staat und Gesellschaft grundlegend verändert.
- Die Nutzung des Cyber-Bereichs (z.B. Internet, mobile Netze, Internet of things) hat viele Vorteile und Chancen gebracht.
- Die digitale Vernetzung auch dazu geführt, dass Informations- und Kommunikationsinfrastrukturen für kriminelle, wirtschaftliche, nachrichtendienstliche, machtpolitische oder terroristische Zwecke missbraucht oder ihr Funktionieren beeinträchtigt werden können.
- Störungen, Manipulationen und gezielte Angriffe, die via elektronische Netzwerke ausgeführt werden, sind Risiken, die mit einer Informationsgesellschaft einhergehen.
- Es ist davon auszugehen, dass diese in Zukunft tendenziell zunehmen.

Swiss Risk Association

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

Swiss Risk Association

Kritische Infrastrukturen

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

Swiss Risk Association

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

Swiss Risk
Association

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.

Swiss Risk Association

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

Swiss Risk Association

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.

Swiss Risk Association

10 Handlungsfelder der NCS 2018-22

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

➔ 29 konkrete Massnahmen in diesen zehn Handlungsfeldern

Swiss Risk Association

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.

Swiss Risk Association

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.

Swiss Risk Association

Armee

- NATO und ihre Mitglieder definieren den Cyber Raum zu einem eigenständigen Operationsraum
- In der Armee sind die Mittel immer noch nicht in ausreichendem Masse vorhanden, um im Rahmen der Armeeaufträge den Bedrohungen angemessen begegnen zu können.
- Aktionsplan Cyber-Defence des VBS
- Umsetzung 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.

Swiss Risk Association

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.

Swiss Risk Association

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.

Swiss Risk Association

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.

CHRISTIAN BEUTLER / KEYSTONE

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

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.

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 Nachrichtendienst 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

Swiss Risk Association