Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Autor(en): **Fischer, Peter / Frey, Stefanie / Henauer, Marc**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **179 (2013)**

Heft 5

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-327673

Die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

Mit der Nationalen Strategie will der Bundesrat die Widerstandsfähigkeit der Schweiz gegen Cyber-Angriffe und -Ausfälle stärken und damit die Nutzung der Chancen unterstützen, welche die zunehmende Vernetzung für Gesellschaft und Wirtschaft bietet. Es geht letztlich um die Attraktivität des Wirtschaftsstandortes und die Krisenfestigkeit der Schweiz.

Peter Fischer, Stefanie Frey, Marc Henauer

Der Bundesrat hat die Strategie am 27. Juni 2012 gutgeheissen und die Umsetzungsphase für die 16 Massnahmen in sieben Handlungsfeldern bis 2017 eingeleitet. Sie reiht sich bestens in die Strategie für eine Informationsgesellschaft Schweiz ein. Mit der Koordination der Umsetzung ist das Eidgenössische Finanzdepartement (EFD) bzw. das Informatiksteuerungsorgan Bund (ISB) mit der Melde- und Analysestelle Informationssicherung (MELANI) betraut.

Das Internet ist ein sehr verteiltes und vernetztes System. Der Umgang mit seinen Risiken und die Verantwortung dafür können nicht in eine einzige Einheit ausgelagert werden. Im Vordergrund steht deshalb die Eigenverantwortung des Einzelnen. Risiken schafft der Einsatz von vernetzten IT-Systemen. Sei dies das Versenden von Nachrichten über E-Mail anstelle eines Postbriefes oder die Steuerung hoch komplexer Systeme von Versorgungsbetrieben über den Computer, anstelle einer manuellen Bedienung. Die Identifikation von Cyber-Risiken muss auf einer Einschätzung der tatsächlichen Bedrohung für die einzelnen Prozesse fussen. Die zur Minimierung dieser Risiken erforderlichen Massnahmen dürfen sich nicht auf die IT-Sicherheit beschränken. Sie müssen immer physische, personelle, technisch sowie daraus resultierende organisatorische Möglichkeiten in Betracht ziehen und aufeinander abstimmen.

Bewusst wurde dabei der Begriff des Umgangs mit Cyber-Risiken und nicht derjenige der Cyber Defense gewählt. Cyber Defense unterstellt, dass eine Abwehr von Cyber-Angriffen innerhalb eines bestimmten Raumes möglich ist und stellt technische Schutzkonzepte in den Vordergrund. Wir können auch starke Parallelen zu existierenden Konzepten der klassischen Kriegsführung, wie z. B. Deterrence, Credible Defense Posture, Retaliation beobachten. – Beim Umgang mit Cyber-Risiken geht man hingegen davon aus, dass Risiken nicht bekämpft oder abgewehrt, sondern nur sie oder ihre Auswirkungen minimiert werden können. Das geschieht im Rahmen eines gesamtheitlichen Risikomanagementprozesses.

Risiko- und Verwundbarkeitsanalysen im Zentrum

Die NCS setzt für Risiko- und Verwundbarkeitsanalysen, speziell bei so genannten kritischen Infrastrukturen an. Dabei stützt sie sich u. a. auf die Nationale Strategie zum Schutz Kritischer Infrastrukturen (SKI) des Bundesamtes für Bevölkerungsschutz BABS. Im Rahmen der SKI-Strategie wurde ein Leitfaden entwickelt, mit dem kritische Prozesse auf Risiken analysiert werden sollen. Die NCS sorgt dafür, dass speziell Risiken, die durch den Einsatz von IT-Systemen entstehen, korrekt und vollständig in diese übergreifenden Risiko- und Verwundbarkeitsanalysen einfliessen. Zuständig für allfällige rechtliche Fragen sind in erster Linie die jeweiligen Regulatoren oder Aufsichtsbehörden. Konsequenterweise erteilt die NCS den Regulatoren, den Auftrag zum Aufbau von Fachwissen im Bereich der Cyber-Risiken innerhalb ihrer Zuständigkeiten. Für die Durchführung der Risiko- und Verwundbarkeitsanalysen sind denn auch nicht irgendwelche Cyber-Stellen zuständig, sondern das Bundesamt für Landesversorgung (BWL) und jeweilige Fachbehörden.

Es versteht sich von selbst, dass eine korrekte Identifizierung von Cyber-Risiken nur dann erfolgreich sein kann, wenn man die Bedrohungs- und Gefährdungslage im Cyber-Bereich für kritische Prozesse möglichst vollständig kennt. Um dies zu ermöglichen, stärkt die NCS die Mel-

Der virtuelle Raum birgt neben vertrauten ganz neue Risiken. Grafik: AvePoint

de- und Analysestelle Informationssicherung MELANI. Sie soll im Austausch mit der Wirtschaft und den Behörden Bedrohungen erkennen, auswerten, eine Einschätzung vornehmen und den Betreibern der kritischen Infrastrukturen Bedarfs- und zeitgerecht zur Verfügung stehen. Dazu verfügt sie über ein technisches Kompetenzzentrum im EFD und eine operative Auswertungszelle im Nachrichtendienst des Bundes (NDB). Zur Anbindung der Strafverfolgungsbehörden arbeitet sie eng mit der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) zusammen. MELANI ist die zentrale Informationsdrehscheibe für Cyber-Bedrohung und Cyber-Risiken, ähnlich dem 2011 in Deutschland geschaffenen Cyber-Abwehrzentrum. Allerdings verfügt MELANI anders als das Cyber-Abwehrzentrum über technische und nicht technische Ressourcen. MELANI hat ihre Produkte zur Unterstützung der Betreiber kritischer Infrastrukturen verfügbar zu machen, deren Informationen mit den eigenen zu vernetzen und subsidiär Unterstützung zu leisten.

Kontinuitäts- und Krisenmanagement für den Fall der Fälle

Selbst die genausten Risikoanalysen und das beste Risikomanagement können Störungen und Vorfälle nicht verhindern. Darum sieht die NCS Vorbereitungen für den Krisenfall und die Schaffung eines Kontinuitätsmanagement vor. Auch hier entstehen keine neuen Cyber-Organe ab, bleibt verantwortlich, wer für Kontinuitäts- und Krisenmanagement zuständig zeichnet. Namentlich sind dies das BWL, die Fachbehörden und das BABS. MELANI, zuständig für die Unterstützung bei Vorfällen, welche sich aus IT-Systemen bei Betreibern kritischer Infrastrukturen ergeben, stellt sicher, dass genügend Ressourcen zur Verfügung stehen. Gleichzeitig obliegt, unabhängig von der Art eines Vorfalles, das Kontinuitäts- und Krisenmanagement den immer gleichen Stellen.

Sicherheitspolitik und kohärente Internationale Position

Standards, die sich mit der Minimierung von Cyber-Risiken befassen, werden in internationalen Gremien definiert. Das Völkerrecht, welches sich damit auseinanderzusetzen hat, wann Cyber-Angriffe ein kriegerischer Akt sind und wie darauf reagiert werden darf, ist im internationalen Kontext anzupassen. Gemeinsame Code-of-Conducts im Umgang mit Cyber-Aktivitäten lassen sich nur multilateral erarbeiten. Auch die Governance des Internets basiert auf einem Einbezug aller relevanten Akteure und Staaten. Obwohl heute die Interessen der Staaten aufgrund ihrer offensiven Fähigkeiten noch sehr unterschiedlich sind, beauftragt NCS die zuständigen Schweizer Behörden damit, sich im internationalen Umfeld dafür einzusetzen, dass den Risiken kollektive Grenzen gesetzt werden. Gerade ein kleines Land wie die Schweiz hat ein eminentes Interesse an einem multilateralen Ansatz, der die Kräfteverhältnisse etwas neutralisiert. Weiter soll auch die Wirtschaft in diesen Prozess eingegliedert werden, denn es sind am Ende internationale Standards, die für lokale Betreiber kritischer Infrastrukturen und Unternehmen gelten.

Für die Abwehr von Cyber-Angriffen und allfällige Gegenmassnahmen soll die Armee eine Auslegeordnung vornehmen. Sie wird klären, welche defensiven Fähigkeiten sie selber in Friedens- und Kriegszeiten benötigt. Sie wird auch ihre offensiven Fähigkeiten prüfen und sich grundsätzlich Gedanken zum Einsatz von Computer Network Attacks im Kriegsfall machen. Entsprechende Konzeptarbeiten wurden eingeleitet.

Im Bereich aktiver Massnahmen unterhalb der Kriegsschwelle tun sich alle Strategien im Ausland schwer. Entweder wird dieser Themenbereich ausgeklammert oder aber es wird auf die heikle rechtliche Situation verwiesen. Auch in der Schweiz steht ein politischer Grundsatzentscheid in dieser Frage noch aus. Die NCS strebt deren Behandlung in den politischen Prozessen an.

Eine Strategie für die ganze Schweiz

Mit Risikoanalyse, Kontinuitätsmanagement und einem Informationsaustausch zwischen Behörden und Wirtschaft ist es freilich nicht getan. Am Ende sollen nachhaltig das Verständnis und der Umgang mit Cyber-Risiken in der ganzen Schweiz verbessert werden. Aus diesem Grund verlangt die NCS eine höhere Priorität im Bereich Forschung und Ausbildung.

Die Cyber-Problematik ist ein komplexes Querschnittthema, dass nur durch die Wahrnehmung der Verantwortung eines jeden einzelnen in den Griff zu kriegen ist. Der Bund soll dort wirken, wo er unabhängig von marktwirtschaftlichen Prämissen aktiv werden kann, so bei der Erstellung einer gesamtheitlichen Bedrohungslage. Bund und Kantone sollen agieren, wo ihre Regulierungs- und Versorgungsaufträge liegen. Namentlich seien hier beispielsweise die Wahrung der inneren Sicherheit, die Strafverfolgung und das Einbringen der Schweizer Position im internationalen Kontext erwähnt.

Die Armee muss ihre Aufgaben in allen Einsatzformen erfüllen. Sie trifft deshalb Massnahmen zum Schutz der eigenen Infrastrukturen und stellt ihre Handlungsfähigkeit sicher. Im Sinne der subsidiären Unterstützung kann sie auf Gesuch hin Behörden und Betreibern Erkenntnisse und ausfallresistente Infrastrukturen zur Verfügung stellen. Gerade im virtuellen Raum sind die Übergänge zwischen militärisch und zivil fliessend.

Es geht letztlich um einen permanenten Prozess, um eine Kultur. Eine zu starke Fokussierung auf IT-Sicherheit zur Minimierung von Cyber-Risiken liesse zwar schnelle und teils zentralisierte Strukturen zu. Allerdings lassen diese das Gesamtbild ausser Betracht und erwiesen sich schon in der Vergangenheit nur kurzfristig als alltagstauglich. Mit einer zu starken Fokussierung auf die Abwehr von Angriffen knapp unterhalb der Kriegsschwelle ist ebenfalls nicht gedient. Ein solcher Ansatz liesse die Alltagsrealität gänzlich ausser Acht. Statt dessen sollten diese Risiken identifiziert, in das Risikomanagement eingegliedert und in Geschäftsleitungen und Chefetagen angegangen werden. Die Verantwortung ist verteilt, liegt bei allen. Der Bund unterstützt die Fähigkeiten, die Verantwortung wahrzunehmen, und stärkt das Gesamtsystem. ■


Peter Fischer
lic.iur., Fürsprecher
Delegierter des Bundesrates
EFD
3003 Bern


Marc Henauer
MA NSS
Chef Op & Info Center
MELANI
VBS
3003 Bern


Stefanie Frey
Phd, King's College London
Expertin Cyber Risks
Ik Steuerungsorgan Bund
im EFD
3003 Bern