Für ein starkes Cybersecurity-Kompetenzzentrum

Offener Brief an die Schweizer National- und Ständeräte

Zürich, den 24. Juli 2018

Die Motion Eder, die ein starkes Cybersecurity-Kompetenzzentrum fordert, wurde Ende letzten Jahres fast einstimmig überwiesen – gegen den Widerstand des Bundesrates. Das Internet sowie online angebotene Dienstleistungen haben auch in der Schweiz längst eine kritische Grösse erreicht. Schäden an dieser Infrastruktur betreffen nicht mehr lediglich grosse Player. Ein Ausfall der hiesigen ICT-Infrastruktur würde nachhaltig negative Folgen für den Wirtschaftsstandort Schweiz nach sich ziehen. Aber bereits kleinere ICT-Probleme, insbesondere bei KMUs, schwächen die Schweiz langfristig. Die meisten westlichen, aber auch viele asiatische Staaten, haben dies längst verstanden.

Nun reagierte der Bundesrat am 4. Juli 2018 widerwillig auf die Motion Eder: Ein hochrangiger Mr resp. eine Mrs Cyber soll es richten. Diese Person soll jedoch keine Weisungsbefugnis haben – ungeachtet der Forderung der Motion Eder. Hinzu kommt, dass sich die betroffenen Departemente offenbar nicht auf ein gemeinsames Vorgehen einigen können. Das überrascht in der Schweizer Politlandschaft nicht, stellt aber einmal mehr sicher, dass letztlich einfach alle unzufrieden sind und keine Lösung der anstehenden Probleme in Sicht ist. Die Schweiz gerät beim Thema Cybersecurity zunehmend in Rückstand. Die Umsetzung der Motion Eder bietet die Möglichkeit, nun aktiv zu werden und zu verhindern, dass die aktuelle Schlussposition weiter zementiert wird.

Das Parlament muss also unbedingt auf die Umsetzung der Motion Eder bestehen und den Bundesrat auffordern, diesem Auftrag nach zu kommen und sich nicht um den Willen des Parlaments zu foutieren. Bundesrat und Verwaltung vermitteln mit ihrem Vorgehen den Eindruck, Partikularinteressen vor die Sicherheit des Wirtschaftsstandortes Schweiz zu stellen.

Nun muss dringend eine Strategie ausgearbeitet werden, die diesen Namen auch verdient. Im Idealfall wird sie von Bund und Privatwirtschaft gemeinsam, unter Einbezug von nationalen und internationalen Experten, erarbeitet. Die Strategie muss unbedingt die folgenden Fragen beantworten. Eine detaillierte Betrachtung sowie Hintergründe zu den einzelnen Punkten werden in der Folge aufgeführt.

1. Wie werden die existierenden Stakeholder im Bereich Cybersecurity konkret koordiniert? Insbesondere die kantonalen Behörden, die Strafverfolgungsbehörden, die Armee und das EDA.
2. Wie wird sichergestellt, dass der gesamte Wirtschaftsstandort Schweiz umfassend geschützt wird? Und nicht nur ausgewählte Betreiber kritischer Infrastrukturen, sondern auch KMUs?
3. Welche Weisungsbefugnis hat das Cybersecurity-Kompetenzzentrum?
4. Wie können bestehende Cybersecurity-Initiativen der verschiedenen Stakeholder gestärkt und in das Zentrum eingebunden werden?
5. Wie werden die Massnahmen der nationalen Cybersecurity-Strategie konkret umgesetzt und woran werden sie gemessen? Wie kann das Cybersecurity-Kompetenzzentrum die Resilienz und Selbstverantwortung der Behörden und Wirtschaft weiter stärken?

Die strategischen Fragen und ihre Hintergründe:

Wie werden die existierenden Stakeholder koordiniert?

In der föderalistischen Schweiz beschäftigt sich eine Vielzahl von Akteuren mit dem Thema Cybersecurity. Diese Akteure leisten in der Regel gute Arbeit, sind jedoch untereinander schlecht vernetzt. Das führt im besten Fall zu Doppelspurigkeiten, im schlechtesten Fall werden durch die fehlende Koordination Anstrengungen und Initiativen zu nichte gemacht. Das föderalistische System verhindert zudem, dass alle Themen die notwendige Beachtung finden, d.h. dass Lücken in den bestehenden Aktivitäten erkannt werden. Es braucht dringend eine koordinierende Stelle, welche alle Akteure an einen Tisch bringt, bestehende sowie neue Initiativen stärkt und weiter auf- und ausbaut.

Wie wird sichergestellt, dass der gesamte Wirtschaftsstandort Schweiz umfassend geschützt wird?

Bestehende Initiativen fokussieren meist auf ausgewählte Themen der Strafverfolgung (Betrug, illegale Pornographie) sowie kritische Infrastrukturen. Die wirtschaftliche Leistung der Schweiz wird aber überwiegend von KMUs erbracht. Diese erhalten keine Unterstützung, sind jedoch deutlich verwundbarer als Betreiber kritischer Infrastrukturen, welche in der Regel über ausgebaute IT-Abteilungen verfügen.

Die Bedrohungen für KMUs sind also erheblich. Auch hier hilft ein zentrales Cybersecurity-Kompetenzzentrum bestehende Initiativen zu stärken und allfällige Lücken, allenfalls in Zusammenarbeit mit Partnern, zu schliessen. Dazu ist sehr wichtig, dass im Vorfeld eine zielgerichtete Strategie entwickelt wird. Diese muss klären, was die Erwartungen an das Kompetenzzentrum sind und wie es aufgebaut werden soll. Zusätzlich braucht das Zentrum eine starke Führung, welche auch die relevanten Verbände für ihre Anliegen gewinnen kann.

Welche Weisungsbefugnis hat das Cybersecurity-Kompetenzzentrum?

Die Antwort ist heikel: Klar ist jedoch, dass Weisungen einer unabhängigen Stelle viel eher akzeptiert werden als solche einer Organisation, die auch andere Interessen verfolgt. Die Erfahrung aus dem Ausland zeigt, dass ein gut aufgestelltes Zentrum, das die Beziehungen zu seinen Kunden pflegt, selten von der Weisungsbefugnis Gebrauch machen muss. Das bedingt aber ein starkes und glaubwürdiges Zentrum.

Vertreter der Privatwirtschaft haben wiederholt deutlich gemacht, dass sie keine Probleme haben, mit einer staatlichen Stelle zusammen zu arbeiten. Inakzeptabel ist für sie jedoch, gleichzeitig mit mehreren Stellen das gleiche Thema bearbeiten zu müssen. Aktuell werden ICT-Betreiber regelmässig von BWL, MELANI, Bakom und weiteren Bundesstellen mit verschiedensten Anliegen kontaktiert. Das ist weder glaubwürdig noch effizient.

Wie können bestehende Cybersecurity-Initiativen der verschiedenen Stakeholder gestärkt und in das Zentrum eingebunden werden?

Ein vielversprechendes Modell lebt das niederländische NCSC: Wichtige Partner entsenden regelmässig sogenannte Liaison Officers an das NCSC. Diese Officers arbeiten jeweils einen Tag pro Woche vor Ort und können Gäste einladen. Das stellt den Informationsfluss sicher und ermöglicht es, eine Vertrauensbeziehung zu allen Partnern aufzubauen. Frequenz und Form dieses Modells lassen sich natürlich diskutieren. Elementar ist jedoch der regelmässige und kontinuierliche Kontakt. Nur so kann eine krisensichere und informations-transparente Arbeitsbeziehung aufgebaut werden.

Ein wichtiges Element der NCS 2.0 ist das nationale Lagebild. Es ist zu bezweifeln, dass eine Organisation, welche vor allem mit sich selbst beschäftigt ist, ein solches Lagebild erstellen kann. Woher kommen die notwendigen Informationen? Wer sammelt sie? Wer stellt

sicher, dass sie vollständig sind? Wer analysiert sie? Diese Fragen sind zentral und werden von den bestehenden Vorschlägen nicht beantwortet.

Soll sich der Bund nicht ausschliesslich auf kritische Infrastrukturen fokussieren?

Der Begriff kritischer Infrastrukturen impliziert, dass diese vom Rest der Infrastruktur abgegrenzt werden können, wie zum Beispiel ein Kraftwerk, das klar als solches erkennbar ist. Im Internet ist diese Abgrenzung jedoch nicht mehr gegeben. Millionen kleinster Geräte werden, wenn kompromittiert, eine gefährliche Waffe. So geschehen beispielsweise als das Mirai Botnet, das aus billigen Webcams bestand, das Internet in den USA für einen Tag lahm gelegt hat. Es braucht also eine zentrale Stelle, welche die Gesamtsicht sowie Einzelfälle im Blick hat und erkennt, wenn die Summe kleiner IT-Probleme zu einem grossen Problemfall wird.

Wie wird der Erfolg der geplanten Massnahmen gemessen?

Alle aktuellen Initiativen beschäftigen sich mit Sektor-Fragen. Es ist darum nicht klar, wie der Erfolg der einzelnen Initiativen gemessen wird. Ohne eine Gesamtschau ist es tatsächlich schwierig, zu beurteilen, ob eine Aktivität zielführend ist. Eine zentrale Stelle kann, basierend auf einem vollständigen Lagebild, erfolgreiche Initiativen erkennen und stärken.

Weniger ist mehr

Man mag nun einwenden, dass der Bundesrat sich der Sache wenigstens annimmt,den „Umständen entsprechend“ nach der besten Lösung sucht und man damit besser dastehen wird als bisher. Dies ist leider ein Trugschluss. Viel Geld in die falsche Lösung zu investieren, richtet Schaden an. Bei einem nicht koordinierten Vorgehen gewinnen vor allem die Angreifer. Diese profitieren ja bereits heute von der schwierigen internationalen Zusammenarbeit. Diese Situation nun mit komplizierten interkantonalen und interdepartementalen Strukturen zu erweitern, wäre ein grosser, kostspieliger Fehler, der die Schweiz in der Bekämpfung von Cyber-Bedrohungen praktisch handlungsunfähig machen würde.

Fazit

Die vom Bundesrat vorgeschlagene Lösung greift in vielen Belangen zu kurz. Sie widerspiegelt die ablehnende Haltung, welche die Exekutive dem Anliegen von Beginn weg entgegengebracht hat.
Es ist nun Zeit, dass sich die Schweiz der Thematik der Cyber-Bedrohung stellt und das departementale Gärtchendenken hinter sich lässt. Es steht viel auf dem Spiel, die Schweiz droht, sich auf ein “Cyber-Abstellgleis” zu manövrieren. Wenn die Schweiz aber ein Hub für ein Crypto Valley und führend in der ICT-Forschung sein will, muss sie auch die Cybersecurity sicherstellen. Dazu braucht es definitiv mehr als ein Mr/Ms Cyber und einige Experten, welche strukturbedingt in erster Linie mit sich selbst beschäftigt sind.

Das Rad muss nicht ganz neu erfunden werden: Ein Vergleich mit bestehenden, erfolgreichen Initiative im Ausland bietet sich an und wird wertvolle Impulse zum Aufbau einer auf die Schweiz angepasste Lösung bieten.

Dr. Daniel Stauffacher, Gründer und President, ICT4Peace Foundation, Zürich
Dr. Stefanie Frey, Geschäftsführerin von Deutor Cyber Security Solutions, Bern
Dr. Serge Droz, Direktor des Forum of Incident Response and Security Team, Zürich

Anhang: NZZ Kommentar vom 26.6.2018

Für einen sicheren Internetplatz Schweiz

Im Bereich Cyber-Security besteht die Notwendigkeit der Schaffung eines integrierten Kompetenzzentrums, das alle Fäden zusammenführt.

Serge Droz, Stefanie Frey und Daniel Stauffacher26.6.2018, 10:50 Uhr

In der NZZ vom 6. 6. 18 berichtet der Bundeshauskorrespondent Lukas Mäder über Ansätze der Umsetzung eines parlamentarischen Vorstosses zur Schaffung eines zentralen Cyber-Security-Kompetenzzentrums. In typisch föderaler Manier und guteidgenössischer Gärtchenpflege wird um Hoheiten gestritten und ein Jekami-Modell favorisiert. Vergessen geht in der Bundesverwaltung, dass die Welt nicht schwarz oder weiss ist: Die Schaffung eines starken Kompetenzzentrums heisst nicht, dass bestehende und gut funktionierende Strukturen aufgelöst werden.

Melani

Tatsächlich besteht die Notwendigkeit für ein Kompetenzzentrum, das zentral alle Fäden zusammenführt. Beispielsweise ist der bundesrätliche Grundauftrag der Melde- und Analysestelle Informationssicherung (Melani) der Schutz kritischer IT-Infrastrukturen. Diese Aufgabe erledigt Melani trotz zum Teil erschwerten Umständen hervorragend. Herzlich wenig hilft dies jedoch KMU, die zwar in der Summe den Grossteil der wirtschaftlichen Leistung erbringen, aber einzeln keine kritische Infrastruktur sind. Auch besitzt Melani nicht die, richtigerweise, beim EDA angesiedelte Kompetenz, spezifische Interessen bei ausländischen Partnern einzubringen. Ausserdem stoppt das Internet bekanntlich nicht an den Kantonsgrenzen. Deshalb müssen sich auch die kantonalen Akteure, die schwergewichtig für die Strafverfolgung verantwortlich sind, in einer moderierten Plattform koordinieren können.

Ausserdem stoppt das Internet bekanntlich nicht an den Kantonsgrenzen.

Auch bei der Reaktion auf erfolgreiche Hackerangriffe kocht die Schweiz auf Sparflamme: GovCERT.ch, das nationale Computer Emergency Response Team des Bundes, ist zwar mit Topleuten besetzt, doch es fehlt an ausreichenden Ressourcen. Auch ist die IT-Industry (Produktehersteller) nur ungenügend in die heutige Konstellation eingebunden. Dass heute Industrieanlagen angegriffen werden, ist kein Geheimnis mehr, es fehlt jedoch an einer spezialisierten Organisation (ICS-CERT), welche sich dieses Themas annimmt. Die Schweiz ist nicht das einzige Land, das sich gegen Bedrohungen aus dem Cyber-Raum schützen muss.

Ein Blick auf europäische Länder lohnt sich. Er zeigt, dass sich die erfolgreichen Länder entwickelt haben: von einem dem Schweizer Modell ähnlichen Konstrukt, das sich auf den Schutz kritischer Infrastrukturen konzentriert hat, zu einem System mit einem starken nationalen Cyber-Security-Zentrum. So wurden in den Niederlanden, in Grossbritannien und Finnland National Cyber Security Centers (NCSC) geschaffen, welche alle bestehenden Akteure zusammenbringen. Exemplarisch und durchaus ein Vorbild für eine mögliche Schweizer Variante ist das NCSC.nl, das alle relevanten Stakeholder durch Liaison-Officers einbindet, welche mindestens einen Tag in der Woche, quasi als ständige Gäste, im Kompetenzzentrum arbeiten. Das physische Zusammenbringen aller Akteure impliziert auch, dass relevante Information zentral zur Verfügung steht und ausgewertet werden kann. Dies ist für das in der NCS-Strategie geforderte Lagebild unabdingbar.

Milizorganisationen

Wichtig ist in der Schweiz auch das Einbinden von Milizorganisationen: Hier könnte das lettische Modell Pate stehen, das zur Unterstützung der Behörden qualifizierte Freiwillige einbindet, welche ein bis zwei Tage im Monat zur Verfügung stehen. Die Schweiz ist mit solchen Arrangements bestens vertraut.

Der erwähnte parlamentarische Vorstoss zielt in die richtige Richtung. Es gilt nun, das Momentum zu nutzen, damit der Internetplatz Schweiz weiterhin zu den sichersten der Welt gehört. Und hier scheint ein NCSC an einem zentralen Ort notwendig zu sein. Von dem ewigen Gerangel der Departemente, wer denn nun die prestigeträchtige Aufgabe Cyber-Security übernehmen könnte, profitieren gemäss der Doktrin «Divide and Conquer» vor allem ausländische Nachrichtendienste und Kriminelle.

Serge Droz ist Direktor des Forum of Incident Response and Security Team
Stefanie Frey ist Geschäftsführerin von Deutor Cyber Security Solutions
Daniel Stauffacher ist Gründer und Präsident von ICT4Peace Foundation