satw it's all about technology

Vision und Grundsätze «Advanced Cybersecurity» für die Schweiz

«Die SATW setzt sich für ein gemeinsames Verständnis der Bedeutung von Cybersecurity als Basis einer vertrauenswürdigen, digitalen Entwicklung der Schweiz ein.»

Schweizerische Akademie der Technischen Wissenschaften SATW
St. Annagasse 18 | 8001 Zürich | +41 44 226 50 11 | info@satw.ch | www.satw.ch

Vision und Mission

Um die Chancen der Digitalisierung optimal zu nutzen, benötigt die Schweiz eine gemeinsame Vision bzw. ein gemeinsames Verständnis der gewünschten, gesellschaftlichen und volkswirtschaftlichen Entwicklung und der dazu notwendigen Massnahmen im Bereich Cybersecurity. Das Advisory Board Cybersecurity SATW hat hierzu Schwerpunkte definiert, die basierend auf der Strategie «Digitale Schweiz» sowie der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 (NCS)» prioritär adressiert werden müssen.

«Die Voraussetzung für eine erfolgreiche digitale Entwicklung in der Schweiz ist ein sicheres, vertrauenswürdiges, digitales Fundament. Dieses ist DER Standortvorteil für die Schweiz – für dessen Aufbau und Erhalt setzt sich die SATW ein.»

1 Grundsatz «Umsetzung lokal – Nationale Cybersecurity-Aktivitäten»

Nationale Cybersecurity-Aktivitäten müssen flexibel und koordiniert den internationalen, gesellschaftlichen und wirtschaftlichen Entwicklungen angepasst werden. Dabei sollen die Chancen genutzt, die Risiken frühzeitig erkannt und bestmöglich behandelt werden.

1.1 Entwicklungen im Bereich Cybersecurity verstehen und Chancen nutzen

Die wissenschaftlichen Akteure in der Schweiz erkennen neue Technologien und Entwicklungen zeitnah und stellen diese der Wirtschaft, der Bevölkerung, der Politik und der Verwaltung zur Verfügung.

Auswirkung: Mit dem aktuellen und laufend ergänzten Wissen kann die Schweiz eine hochwertige Cybersecurity-Kompetenz aufbauen und international zur Weltspitze aufschliessen.

1.2 Rasche und konsequente Umsetzung der Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 (NCS)

Mit der NCS verfügt die Schweiz im Cybersecurity-Bereich über eine national gültige Strategie, die die Herangehensweise und den Umgang mit den Herausforderungen des Cyberraumes definiert.

Auswirkung: Doppelspurigkeiten und ein unkoordiniertes sowie träges Vorgehen können künftig vermieden werden, wenn sich alle beteiligten Akteure in der Schweiz in Bezug auf Cybersecurity an der NCS orientieren und entsprechend rasch und koordiniert an der wirkungsvollen Umsetzung arbeiten.

1.3 Verstärkung der Synergien, Vermeidung von Fragmentierung

Die Aufgaben, Kompetenzen und Verantwortungen sind aktuell zwischen vielen Akteuren des Bundes, der Kantone, der Unternehmen sowie der Bildung und Forschung aufgeteilt. Viele Einzelinitiativen von Verbänden, Organisationen und Einzelpersonen bestehen in der Schweiz.

Auswirkung: Trotz des Föderalismus wird ein gemeinsames, koordiniertes Vorgehen benötigt. Dieses basiert auf der NCS und geht vom neu zu schaffenden und mit entsprechenden Mitteln ausgerüsteten Kompetenzzentrum für Cybersicherheit des Bundes aus. Das Kompetenzzentrum soll möglichst unabhängig handeln und von Partikularinteressen unbeeinflusst sein. Für das Kompetenzzentrum ist im Rahmen der NCS und der zu definierenden interdepartementalen Verantwortlichkeiten Weisungsbefugnis vorzusehen.

1.4 Kurze und flexible Entscheidungs- und Entwicklungszyklen

Mit der heutigen globalen Entwicklung im Bereich der Hard- und Softwareentwicklung wird typischerweise von Quartalszyklen und einem Planungshorizont von maximal einem Jahr gesprochen und demgemäss gehandelt. In vielen Fällen wird die Hard- und Software sogar kontinuierlich entwickelt und laufend freigegeben. Geschäfts- und Betriebsmodelle entwickeln sich heute, getrieben durch neue Technologien und Datenverfügbarkeit, schnell weiter.

Auswirkung: Entsprechend der Marktbedürfnisse müssen sich die Entscheidungsprozesse in der Politik / Verwaltung sowie Wirtschaft verkürzen und internationale Netzwerke müssen stärker eingebunden werden. Die wesentlichen Akteure in der Schweiz können nicht mehr isoliert und mit langem Planungshorizont arbeiten. So sollen etwa die Massnahmen, die die Umsetzung der NCS konkretisieren, kurzfristig ausgearbeitet und angepasst sowie aktuelle, internationale Entwicklungen stärker miteinbezogen werden. Ebenso sind neuste Methoden sowie Technologie- und Produkteinnovationen laufend miteinzubeziehen.

1.5 Verstärkung von Bildung und Forschung

Eine der Kernkompetenzen der Schweiz besteht in der hochstehenden Bildung und der internationalen Spitzenforschung sowie in der innovativen Entwicklung neuer Produkte und Dienstleistungen basierend auf neusten Technologien.

Auswirkung: Bereits bestehende Programme zur Förderung von Innovation sowie von Start-Ups sollen aktiver und unternehmerischer betrieben werden. Ziel ist es, eine wirkungsvolle Anzahl Start-Ups in der Schweiz zu etablieren und eine nationale Industriebasis von Produkten und Dienstleistungen mit neusten Technologien zu schaffen. Die Wichtigkeit der Cybersecurity wird aktiv kommuniziert, um das Thema noch intensiver in das Bewusstsein zu rücken und so u.a. die Anzahl an Lehr- und Hochschulabsolvierenden zu erhöhen.

1.6 Fördern und stärken der cyber-physischen Souveränität

In der Strategie «Digitale Schweiz» wird die Entwicklung der Digitalisierung hierzulande als Ganzes beschrieben. Wichtige Themengebiete wie Blockchain, Künstliche Intelligenz, Robotik und Smart Cities sind darin ebenso enthalten wie die NCS. Was in der Strategie fehlt, ist eine Vorstellung zur Ausprägung der cyber-physischen Souveränität der Schweiz im globalen Cyberraum. Unter Cyber-Souveränität verstehen wir die Fähigkeit eines Landes, im digitalen Raum eigene Entscheidungen zu treffen, diese um- und durchsetzen zu können sowie seine strategischen Interessen zu wahren. Es geht somit explizit nicht um das politikwissenschaftliche Verständnis der Kontrollausübung durch den Staat über die digitalen Anwendungen, wie beispielsweise der Idee eines «nationalen Internets» in Deutschland, sondern um ein selbstbestimmtes Verhalten und Handeln der Akteure im Cyberspace.

Auswirkung: Eine angemessene, formell durch den Staat definierte und konsequent eingeforderte cyber-physische Souveränität mit klaren Rahmenbedingungen wird künftig zu einem wirtschaftlichen Wettbewerbsvorteil im globalen Standortwettbewerb, indem beispielsweise für Anwendungen bei kritischen Systemen nationale Lösungen bevorzugt werden. Es ist daher zentral, dass die Schweiz für die Bevölkerung, die Wirtschaft und den Staat das geeignete Mass an Cyber-Souveränität definiert und entsprechende Handlungen initiiert. Dazu gehört ein Verständnis davon, ab wann die Souveränität für unsere direktdemokratische, föderalistische, freiheitliche und wohlhabende Gesellschaft so eingeschränkt wird, dass dies zu Konflikten führen könnte.

2 Grundsatz «Internationale Beziehungen»

Wesentliche internationale Wertschöpfungsketten, Beziehungsnetze und Abhängigkeiten im ICT-Bereich müssen laufend erkannt, berücksichtigt und spezifisch auf Cybersecurity-Risiken und Verletzlichkeiten untersucht werden.

2.1 Integration der internationalen Logistik- und Wertschöpfungsnetzwerkpartner

Heutige Liefernetze sind international verknüpft und voneinander abhängig, Hard- und Software wird mittels globaler Prozesse und Systeme entwickelt und produziert. Allfällige Kompromittierungen von Komponenten der Lieferketten sind nur schwer zu entdecken und stellen für Nutzerinnen und Nutzer ein potentielles Sicherheitsrisiko dar. Zertifizierungen im Sinne einer Baseline-Security analog dem «Cybersecurity Act» der europäischen Kommission, sind für gewisse Elemente der Lieferkette sinnvoll.

Auswirkung: Im Bereich der Zertifizierung der Liefernetze sowie deren Schlüsselkomponenten sollte die Schweiz mit allen relevanten nationalen und internationalen Partnern, insbesondere der EU, zusammenarbeiten. Dies ermöglicht einen angemessenen Schutz und Resilienz der Liefernetze, wobei es Machbarkeit, Wirtschaftlichkeit und Verhältnismässigkeit zu berücksichtigen gilt. Für vitale Dienstleistungen sollte die Schweiz verbindliche, bindende und überprüfbare Standards und Regeln einführen, die definieren, welche Massnahmen Unternehmen und die öffentliche Hand zur Sicherung ihrer Liefernetze treffen müssen.

2.2 Professionelle Bekämpfung von Straftaten im Cyberraum

Die Kriminalität im cyber-physischen Raum wird zunehmend länderübergreifend ausgeführt, die digitalen Spuren sind über viele verschiedene Länder verteilt und verwischt. Bedrohungen haben ihren Ursprung in einem Netz von hochgerüsteten, fremdstaatlichen, militärischen, behördlichen oder privatwirtschaftlichen Aufklärungs- und Nachrichtendiensten. Zusätzlich handeln grosse Internet-Dienstleister in einem multinationalen Umfeld, bei dem die Gesetze der einzelnen Staaten beschränkt oder nicht anwendbar sind. Dadurch entstehen rechtsfreie Räume, bei denen die Aufgaben eines Rechtsstaats nicht mehr souverän wahrgenommen werden können, was eine mangelhafte Wirkung in der Prävention und Verfolgung der kriminellen Phänomene zur Folge hat. Noch problematischer wird die Situation, falls solche Konzerne selbst ausserhalb der Gesetze einzelner Staaten wirken und z.B. die Interessen eines einzelnen Staates vorziehen.

Auswirkung: Die Internationale Zusammenarbeit muss gefördert und beschleunigt werden. Es soll definiert werden, welche Individuellen Rahmenabkommen mit einzelnen Regierungen oder der internationalen Staatengemeinschaft auszuhandeln sind und welche Lösungen einen Beitrag leisten können, damit diese Straftaten erschwert werden. Im nicht militärischen bzw. nachrichtendienstlichen Bereich ist die Zusammenarbeit zu fördern, um Geräte und Websites zu sperren, welche für Angriffe genutzt werden.

2.3 Fördern von internationalen, gemeinsamen Grundlagen für Sicherheit und Resilienz in den globalen Netzen

Da der Cyberraum keine geografischen Grenzen hat, ist es zentral, dass sich die Schweiz, ihre Unternehmen und Verbände im Sinne der internationalen Gemeinschaft für ein sicheres Internet einsetzen. Internationale Erklärungen wie der «Paris Call for Trust & Security im Cyberspace» oder die Konzeption einer digitalen «Geneva Convention» haben eine grosse Bedeutung und benötigen jegliche Unterstützung.

Auswirkung: Im Rahmen einer auf bestehenden Organisationen und Initiativen beruhenden digitalen «Geneva Convention», die nationalstaatliche Aufrüstungen im Cyberspace ächtet und somit limitiert, ist der Aufbau einer Organisation notwendig (z.B. eine international Cyber Protection Agency). Diese überwacht die Einhaltung der Regeln, berichtet über Verstösse und schlägt der UNO Sanktionen vor. Die aktuelle Ausrichtung der Geneva Convention sollte auf die grossen Internetkonzerne ausgeweitet werden: Es reicht nicht, nur die Staaten in die Pflicht zu nehmen. Auch Technologie-Unternehmen müssen Verantwortung übernehmen und ihre Sicherheitslücken selber schliessen bzw. gar nicht erst welche zulassen, wie dies z.B. vom Cybersecurity TecAccord gefordert wird.

3 Verankerung der Vision einer cyber-physischen Schweiz in der Bundesverfassung

Die Schweiz braucht eine verfassungsmässige sowie gesetzliche Ausweitung des Entwicklungs- und Schutzanspruches auf die digitalen Räume.

3.1 Den Schutzanspruch für den digitalen Raum in der Bundesverfassung verankern

Mit Gesetzen auf Basis der aktuellen Bundesverfassung lässt sich der Souveränitäts- und Sicherheitsanspruch des Staates, der nationalen und international tätigen Unternehmen sowie der Bürgerinnen und Bürger in virtuellen Räumen wie dem Internet nicht mehr sauber definieren. Klassische «Grenzkontrollen» sind im virtuellen Raum kaum möglich.

Auswirkung: Der Souveränitätsanspruch im digitalen Raum muss auf Augenhöhe mit anderen grundlegenden Rechten und Ansprüchen des Staates auf Verfassungsebene geregelt werden. Nicht zu unterschätzen ist internationale Signalwirkung – die Schweiz wäre eines der ersten Länder der Welt, welches seinen Schutz und Selbstbestimmungsanspruch für digitale Räume auf Verfassungsstufe erhebt. Es braucht eine vertiefte Diskussion aller Beteiligten sowie politische Massnahmen von Entscheidungsträgerinnen und -trägern zu einer geschickten und zukunftsweisenden Anpassung von Bundesverfassung, Gesetzen oder Verordnungen.

satw it's all about technology

Impressum

Schweizerische Akademie der Technischen Wissenschaften SATW

Autoren und Autorinnen: Karl Aberer (EPFL) | Umberto Annino (ISSS) | Alain Beuchat (UBS) | Matthias Bossardt (KPMG) | Adolf Dörig (Doerig & Partner) | Roger Halbheer (Microsoft) | Pascal Lamia (MELANI) | Martin Leuthold (Switch) | Hannes Lubich (FHNW) | Adrian Perrig (ETHZ) | Riccardo Sibilia (VBS) | Bernhard Tellenbach (ZHAW) | Stephanie Teufel (Uni Fribourg) | Daniel Walther (Swatch Group Services) | Andreas Wespi (IBM Research Lab)

Redaktion: Esther Koller-Meier (SATW) | Nicole Wettstein (SATW)

30. April 2019