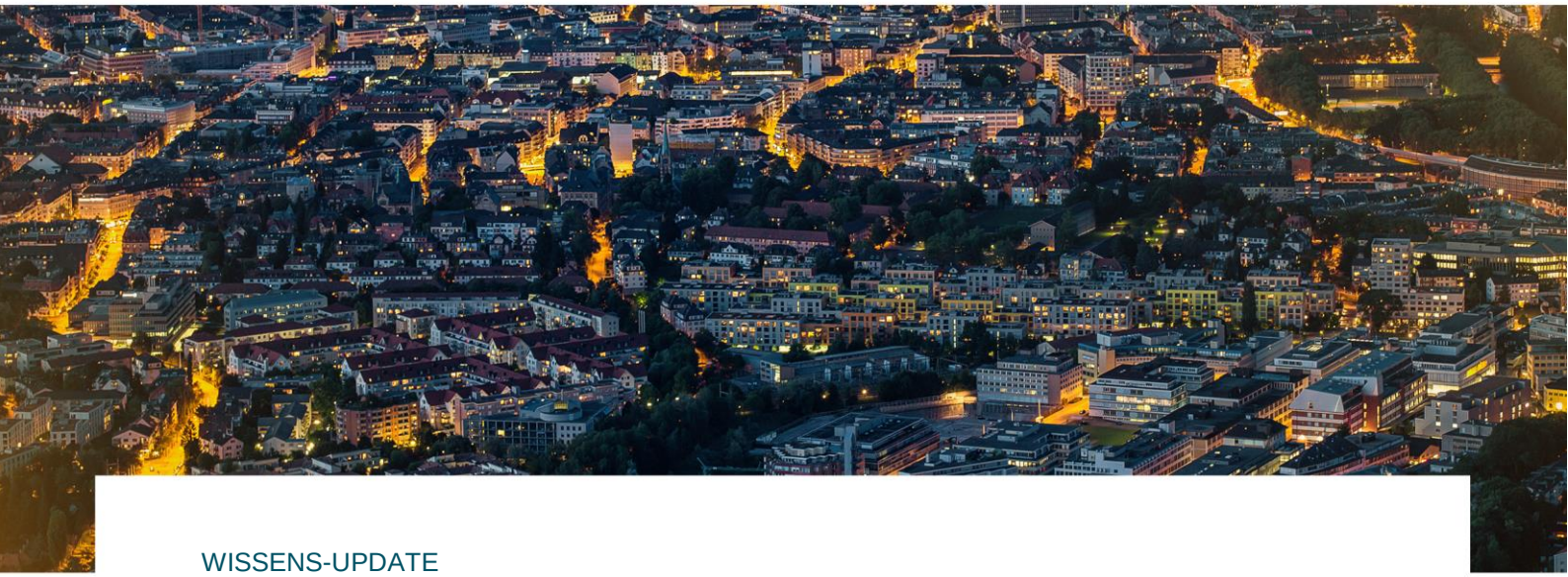
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Top-Forschung nutzen – für eine digitale und cyber-sichere Schweiz

Patrizia Reding | Senior Security Consultant | Steinhausen, 22. Oktober 2019

Damit die Schweiz die Chancen der Digitalisierung optimal nutzen und sich dabei effektiv vor Cyber-Risiken schützen kann, benötigen die Behörden neben der bereits in der Umsetzung befindlichen Nationalen Cyber-Strategie (NCS) auch eine umfassende Digitalisierungsstrategie. Beide Strategien sollen optimal aufeinander abgestimmt und ihre Weiterentwicklungen jeweils eng koordiniert sein.

Digitalisierung ohne (Cyber-)Sicherheit macht eben so wenig Sinn wie Cyber-Sicherheit ohne den Aspekt der Digitalisierung. Dazu können und sollen die Behörden eine enge Zusammenarbeit mit der Industrie und Forschung suchen. Diese «Public-Private-Partnership» kann das fehlende Fachwissen kompensieren und die benötigten Innovationen vorantreiben.

Blockchain, selbstgesteuerte Maschinen, automatisiertes Lernen – die Wirtschaft integriert gefühlt täglich neue digitale Errungenschaften. Auch die Schweizer Bundesbehörden werden zunehmend digitaler; allerdings äusserst unkoordiniert, wie Finanzminister Ueli Maurer im Sommer feststellte. Offenbar gibt es nach wie vor weder ein gemeinsames Verständnis besagter Entwicklung noch gemeinsame verbindliche Standards. Dies erschwert es erheblich, unser Land gesamtheitlich und barrierefrei zu vernetzen und notwendige Digitalisierungsprojekte effizient durchzuführen.

Diese unkoordinierten Insel-Ansätze auf allen staatspolitischen Stufen verhindern auch die optimale Ausrichtung der dazu benötigten Cyber-Sicherheit, verursachen Abwehr-Lücken und könnten im schlimmsten Fall zu verheerenden Cyber-Zwischenfällen im Behördenumfeld führen. Ein abgestimmtes Vorgehen der Behörden auf Bundes-, aber auch auf Kantons- und Gemeindeebene ist darum zwingend nötig.

Es geht jedoch noch weiter: Um unseren zunehmend digitalisierten Staat, die digitalisierte Wirtschaft und Bevölkerung vor Cyber-Gefahren zu schützen – und damit weiterhin eine stabile Konjunktur zu sichern und den Wohlstand zu garantieren, braucht es ausserdem eine gemeinsame Strategie mit Schweizer Herstellern sowie der hier ansässigen Forschung. Konkret heisst dies, Mechanismen zu entwickeln, die es erlauben, die jeweils neusten Technologien der Industrie genauso zu nutzen wie das grosse Wissen an den hiesigen Universitäten und Fachhochschulen.

Cyber-Risiken verändern sich stetig

Eines steht nämlich fest: Die Cyber-Risiken von heute und morgen sind nicht dieselben – sie verändern sich laufend. Diese akzentuieren sich mit der fortschreitenden Digitalisierung fundamental. Die gute Nachricht: Unser Land erbringt bereits gute Leistungen in der Cyber-Sicherheitsforschung. Diesen Vorteil gilt es jetzt zu nutzen. Erstes Ziel muss sein, die Schweiz weniger abhängig von ausländischen Cyber Defence-Lösungen zu machen und das eigene technologische Know-how einzusetzen, um neue Sicherheitslücken selber aufdecken zu können.

Schlüsselelemente für staatliche Cyber Security

Es gilt also, vom reaktiven in den aktiven Modus zu wechseln, wenn es um den Schutz vor Gefahren im Netz geht. Für eine koordinierte Cyber Defence- und Cyber Security-Strategie über alle Ebenen hinweg braucht es gemäss Florian Egloff, Senior Researcher in Cybersecurity am Center for Security Studies der ETH Zürich, folgende Schlüsselelemente, die er vergangenen Frühling im Rahmen der Studie «Nationale Cybersicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz» vorstellte:

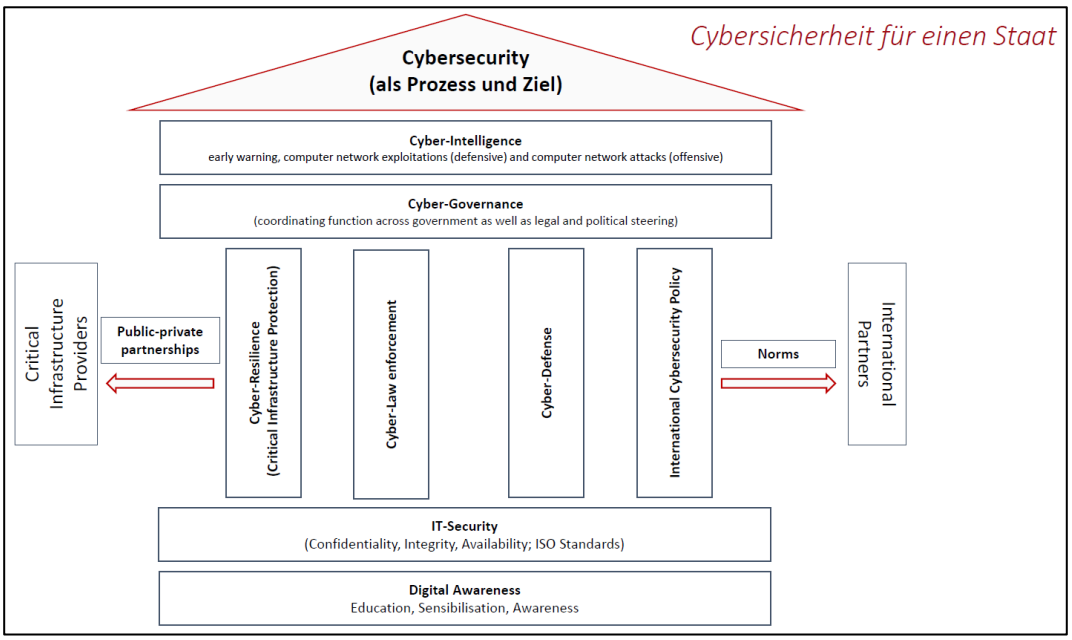


Abbildung 1: Studie «Nationale Cybersicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz», https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18März2019.pdf),
Dr. Florian Egloff, Senior Researcher in Cybersecurity, Center for Security Studies, ETH Zürich

In Egloffs Modell stellen Forschung, Bildung und Sensibilisierung für das Thema zusammen mit IT-Sicherheit das Fundament für Cyber Security dar. Darauf basieren folgende wichtige Stützpfeiler: (internationale) Normen und Gesetze, Cyber Defence (z. B. Gefahreneinschätzung mittels Cyber-Forensik) und -Resilienz (Krisenmanagement bei grösseren Cyber-Vorfällen). All das kann allerdings nur in Zusammenarbeit mit Partnern (weltweit) erreicht werden. Auf den Stützpfeilern bauen wiederum zwei weitere Elemente für einen cybersicheren Staat auf: Cyber-Governance (Koordination und Steuerung) sowie Cyber-Intelligence (intelligente Frühwarnsysteme).

Die fünf relevanten Handlungsfelder für Staat, Forschung und Wirtschaft

Egloff macht fünf Hauptbereiche aus, in denen Staat, Forschung und die Schweizer Industrie mit ihren innovativen Lösungen zusammenarbeiten und ihre Synergien nutzen sollten – unter Federführung des Bundes für eine digitale und cybersichere Schweiz:

1. **Sichere Systeme und Technologien**

   Zum Beispiel Kryptografie (Verschlüsselung von Nachrichten / Daten) verwenden / weiterentwickeln oder komplexe und damit sichere IT-Landschaften bauen

2. **Verifikation und Garantien**

   Zum Beispiel Supply Chain Security herstellen: transparente und angriffssichere Wertschöpfungsketten

3. **Organisatorische und ökonomische Cyber-Risiken**

   Das können zum Beispiel Mitarbeitende sein – Schulungen und Informationsveranstaltungen reduzieren dieses Risiko

4. **Identität, Verhalten, Kriminologie, Recht und Ethik**

   Zum Beispiel besser verstehen, wie Daten digitale Identitäten kreieren und wie sich dies auf den Persönlichkeitsschutz auswirkt

5. **Nationale Sicherheit und internationale Beziehungen**

   Zum Beispiel resiliente IT-Strukturen schaffen, um wichtige Dienstleistungen und Güter auch bei grösseren Cyber-Vorfällen gewährleisten zu können

Chance: Eigene Cyber Security-Produktideen und -Lösungen kommerzialisieren

Erlangen Behörden, Industrie und Forschung ein gemeinsames Verständnis dieser Handlungsfelder sowie der nötigen Mittel und Technologien, bedeutet das ein effektiver Schutz vor Gefahren im Cyberspace. Allerdings nicht nur. Schafft es die Schweiz nämlich, eigene Cyber Security-Produkt-ideen und -lösungen zu entwickeln, ergibt sich auch das Potenzial, diese Ideen zu kommerzialisieren und damit ökonomisch zu nutzen.

Eine weltweite Nutzung von Schweizer Cyber Security-Lösungen erweitert wiederum das Verständnis der aktuellen Cyber-Angriffsmethoden und kann direkt in neue innovative Schweizer Produkte einfliessen. Durch die «Public-Private-Partnerschaft» kann damit auch die Cyber-Sicherheit der Schweiz als Ganzes erhöht werden. Dadurch entsteht eine Aufwärtsspirale der kontinuierlichen Verbesserung.

CyOne Security ist der vertrauensvolle Industriepartner dafür

Es gilt also, die Schweiz vor Cyber-Risiken zu schützen, indem einheitliche Cyber-Sicherheitsstandards für die Schweiz definiert und umgesetzt werden. Diese sollen in einer schweizweiten umfassenden und in allen wichtigen Aspekten aufeinander abgestimmt sein und in einer abgestimmten Sicherheitsarchitektur münden.

Denn moderne und effiziente Informations- und Kommunikationstechnologie bildet das Rückgrat von Staat und Wirtschaft und ist unabdingbar. Agil, skalierbar und mit einer gesicherten Verfügbarkeit trägt sie entscheidend zum nachhaltigen Erfolg in der Schweiz bei.

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Cyber-Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Ihre Organisation vor Cyber-Risiken zu schützen und tragen Sie so zu einer sicheren Schweiz bei.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Cyber Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.