Digitalisierung | E-Government

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Digitalisierung ist der Sammelbegriff für die immer stärkere, unverzichtbare Nutzung von Informations- und Kommunikationstechnologien in Wirtschaft und Gesellschaft. Dabei kann Digitalisierung im einfachsten Fall den 1:1 Ersatz manueller oder papiergebundener Abläufe durch elektronisch geführte Abläufe bedeuten. Die Mehrheit der Digitalisierungsvorhaben soll jedoch bestehende Abläufe verbessern oder neue ermöglichen, die bislang nicht umsetzbar oder zu aufwändig waren.

Wenn sich digital geführte Abläufe stark verändern, verändert sich auch die individuelle Arbeitsweise, die Zusammenarbeit oder sogar das Berufs- und Tätigkeitsbild der Anwenderinnen und Anwender, die in der Regel keine IT-Spezialkenntnisse haben. Daher wird in diesem Zusammenhang oft von «digitaler Transformation» gesprochen, auch um anzuzeigen, dass solche Vorhaben keine reinen IT-Projekte sind, sondern auf das enge Zusammenwirken von IT und Anwendern bei der Definition, Erarbeitung, Umsetzung und Inbetriebnahme entsprechender Projekte angewiesen sind.

Länder wie Estland, Lettland, Norwegen oder Schweden sind auf nationaler Ebene bereits weit fortgeschritten und agieren in Geschäftsleben und Verwaltung weitgehend papierlos – ebenso ist Bargeld durch digitale Zahlungsmittel verdrängt worden. In der Schweiz führt eine konservativ geprägte Grundhaltung der Gesellschaft, der hohe Anspruch an IT-Sicherheit und Privatsphäre sowie der stark ausgeprägte Föderalismus zu einem eher vorsichtigen, stark etappierten und fragmentierten Vorgehen, insbesondere seitens Behörden und Verwaltungen. Vorhaben wie die e-ID, e-Voting oder das elektronische Patientendossier werden entsprechend kontrovers diskutiert.

Empfehlungen

Dokumente, Absichtserklärungen und der Wille zur Anwendung der Digitalisierung und sicheren Bereitstellung entsprechender Dienste sind in ausreichendem Masse vorhanden. Jedoch müssen nun zeitnah konkrete Taten folgen. Das Advisory Board empfiehlt in diesem Kontext, die geplanten Vorhaben trotz föderaler Grundstrukturen zu koordinieren und aufeinander abzustimmen, und bei Vorhaben mit Auswirkungen auf die Sicherheit der Bevölkerung und des Staates die nötigen flankierenden Massnahmen (Transparenz, öffentlicher Diskurs, kontrollierte Erprobung, ausreichende Überwachung und Notfallplanung) rechtzeitig zu ergreifen.

2019 wurde in der Schweiz mit der Schaffung der Position eines Cyber-Delegierten des Bundesrates ein wichtiger Meilenstein erreicht. Der damalige Bundespräsident Ueli Maurer hat zudem die Ziele des Bundesrates für 2020 präsentiert. Diese sind auf die drei Leitlinien zur Legislatur 2019 bis 2023 abgestimmt, mit den Schwerpunkten «Wohlstand» (umfasst u.a. die Weiterentwicklung der Strategie «Digitale Schweiz» und die IKT-Strategie bis 2023 sowie E-Government-Vorhaben), «Zusammenhalt» und «Sicherheit» (umfasst die Bewirtschaftung von «Cyber-Risiken», u.a. durch einen Bericht, wie im rasch wachsenden, kaum kontrollierten «Internet der Dinge» die Sicherheit erhöht und Missbrauch erschwert werden kann).

Herausforderungen

Es ist wichtig, sich über das Thema rechtzeitig und fundiert zu informieren, um eigene Ansprüche, Bedenken und Unklarheiten fundiert und rechtzeitig in den laufenden Diskurs einzubringen. Sich wegen Sicherheitsbedenken gar nicht damit zu befassen, wäre genau so wenig zielführend, wie eine unzureichend reflektierte und ggf. zu schwach abgesicherte Einführung solcher Dienste mit entsprechend hohen Risiken.

Seitens Behörden, öffentlichen Verwaltungen usw. muss dabei insbesondere auf die jederzeitige Aufrechterhaltung der staatlichen und hoheitlichen Souveränität und die Wahrung der nationalen Interessen in einem zunehmend kompetitiven und globalisierten wirtschaftlichen und politischen Umfeld geachtet werden.

Sind diese Voraussetzungen gegeben, besteht kein Grund zur existenziellen Sorge. Die Chancen der Digitalisierung für Wirtschaft und Gesellschaft nicht zu nutzen, wäre langfristig schädlicher als das gezielte, kontrollierte Eingehen erkannter und handhabbarer Risiken. Die Herausforderung wird jedoch darin bestehen, alle Anspruchsgruppen in einem föderalen Umfeld ausreichend einzubeziehen und tragfähige, konsensfähige Lösungen zu entwickeln, kontrolliert zu erproben, bei erkanntem Bedarf zu verbessen und schrittweise in Betrieb zu nehmen.

Handlungsbedarf

In den folgenden Bereichen und der genannten Reihenfolge besteht dringlicher Handlungsbedarf:

– Ein breites und gemeinsames Verständnis aller Anspruchsgruppen bezüglich Cyber-Risiken anhand von Risikogruppen, Risikoszenarien und deren Zusammenwirken.

– Eine breit abgestützte Diskussion und stringente Definition der Grundlagen und Grenzen der Aufrechterhaltung der staatlichen Souveränität und «Staatsgrenze» im digitalen Raum.

– Eine ausreichend sichere, datenschutzkonforme, erprobte und breit akzeptierte digitale Identität inklusive einer der staatlichen Hoheit über diese Identitäten angemessenen Betriebsorganisation für natürliche und juristische Personen. Diese bildet die Grundlage für eine breite Palette von E-Government-Diensten des Bundes, der Kantone und der Gemeinden.

– Die föderal geführte Planung und Bewirtschaftung eines Portfolios von Digitalisierungsvorhaben in Behörden und Verwaltungen und von entsprechenden E-Government-Diensten.

– Die Definition, Erprobung und Führung der nötigen Prozesse zum effektiven, breit akzeptierten Zusammenwirken öffentlicher und privatwirtschaftlicher Akteure der Digitalisierung zur Schaffung und Nutzung von Chancen für den Ausbildungs- und Werkplatz Schweiz.

– Die frühzeitige Erkennung und Kompensation oder Vermeidung von unakzeptabel hohen Abhängigkeiten (z.B. von fremdstaatlich beherrschten Anbietern) und kumulativen Risiken inklusive einer ausreichenden Notfall- und Wideranlaufplanung im Störungsfall.

Referenzen

– Strategie «Digitale Schweiz» 2018-2020: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz.html und https://www.digitaldialog.swiss/de

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS): https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022: https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-herausforderungen

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020