CH++ fordert ein Staatssekretariat für Cybersicherheit

November 2021

Der rasche technologische Wandel ist ein weltweites Phänomen, das auch vor der Schweiz nicht Halt macht. Unser Land muss die Digitalisierung erfolgreich meistern, und investiert dementsprechend in die notwendigen technologischen Infrastrukturen. Dadurch verschiebt sich jedoch das Gefahrenpotential: Cyberattacken stellen von der Lahmlegungen der Grundversorgung bis zur Veröffentlichung von hochsensitiven Bürgerdaten ein enormes Sicherheitsrisiko dar. Die jüngsten Beispiele von Angriffen auf Gemeinden, Spitäler und E-Government-Dienste zeigen, dass Cyberattacken eine systematische Bedrohung aller Bereiche des öffentlichen Lebens sind.

Der Bund hat im Frühjahr 2018 eine nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken verabschiedet. Darin erwähnt er die stark intensivierte Bedrohungslage. Operativ zentral ist dabei das *Nationale Zentrum für Cybersicherheit* NCSC, welchem der Delegierte des Bundes für Cybersicherheit vorsteht. Der Delegierte wiederum untersteht dem Departementsvorsteher des Eidgenössischen Finanzdepartements. Eine Kerngruppe Cyber koordiniert die Zusammenarbeit mit den Departementen EFD, EJPD und VBS sowie der Konferenz der kantonale Polizeikommandanten der Schweiz; ein Steuerungsausschuss koordiniert die Zusammenarbeit mit den Verwaltungseinheiten des Bundes (z.B. Armasuisse, Bundeskanzlei, etc.), der Wirtschaft, der Kantonen und den Hochschulen. Das NCSC hatte per Mai dieses Jahres 32 Mitarbeiter, dreizehn offene Stellen sollen bis Ende Jahr noch besetzt werden.

Parallel dazu verfolgt das VBS die Strategie "Cyber VBS", welche im April 2021 verabschiedet wurde. Der Bund unterscheidet dabei *Cyberdefence von Cybersicherheit*. Mit Cyberdefense sind "nachrichtendienstliche und militärische Massnahmen zum Schutz der für die Sicherheit des Landes kritischen Systeme, zur Abwehr von Cyberangriffen, zur Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und zum Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden"[1] gemeint.

[1] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-83160.html

Cybersicherheit fasst die “Gesamtheit der Massnahmen, welche die Prävention, die Bewältigung von Vorfällen und die Verbesserung der Resilienz gegenüber Cyber-Risiken zum Ziel haben und die internationale Zusammenarbeit zu diesem Zweck stärken”[2] zusammen.

Vor dem Hintergrund der bisherigen Aktivitäten und der exponentiell steigenden Bedrohungslage im Cyberbereich stellen wir drei Kernprobleme fest.

1. **Cybersicherheit für alle Bereiche des öffentlichen Sektors:** Cyberattacken kommen von überall und können alle treffen. Die Erwartung, dass alle Gemeinden und Kantone im Thema Cybersicherheit laufend auf dem allerhöchsten technischen Niveau sind, ist unrealistisch. Der Bund muss deshalb die Cybersicherheit für alle Staatsebenen und alle Bereiche des öffentlichen Lebens sicherstellen können.

2. **Sicherheits-Basis für digitale Souveränität:** Es besteht ein rasch wachsendes Bedürfnis für eine stärkere digitale Souveränität (Cloud, kritische Netzwerkinfrastruktur, etc.) der Schweiz. Ohne die entsprechende Sicherheit-Basis ist diese digitale Souveränität von Grund auf in Frage gestellt.

3. **Bündelung von Ressourcen und Expertise:** Die Gewährleistung der nationalen Cybersicherheit kann nicht einzig durch einen Delegierten des Bundes für Cybersicherheit mit einem Team in der aktuellen Grösse gewährleistet werden. Cybersicherheit-Expertise in verschiedenen Ämtern und Departementen muss in einem neuen Staatssekretariat für Cybersicherheit mit den für die wachsende Bedrohung adäquaten Ressourcen gebündelt werden.

Zweifellos werden auf der administrativen Ebene weitere Cyberaktivitäten folgen. Es ist davon auszugehen, dass der Bereich Cybersicherheit sehr stark ausgebaut und parallel zur Bedrohungslage anwachsen wird. Im Weiteren gilt es festzuhalten, dass die Cybersicherheit sämtliche Aufgaben des Bundes, der Kantone, und der Gemeinden betreffen wird. Aus all diesen Gründen ist die Schaffung eines neuen Staatssekretariats für Cybersicherheit als zentrale Stelle eine entscheidende strategisch organisatorische Weichenstellung, um die Schweiz operationell auf die neue, rasch wachsende und sich laufend ändernde

[2]https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht_Umsetzungsstand_NCS_2018-2022_Mai_2019.pdf.download.pdf/Bericht_Umsetzungsstand_NCS_2018-2022_Mai_2019.pdf

Bedrohungssituation einzustellen. Nur so lässt sich die digitale Souveränität gewährleisten. Wir fordern den Bund auf, diesen Schritt so rasch wie möglich zu gehen.