Strategien für Cyber-Sicherheit

Ein entscheidender Faktor für das Gelingen der Digitalisierung ist die Gewährleistung von Cyber-Sicherheit. Da die Zahl der Cyber-Angriffe ständig zunimmt, sind Cyber-Sicherheitsstrategien wichtig.

Die digitale Welt bietet immer neue Möglichkeiten – begleitet von Herausforderungen. Ein entscheidender Faktor für unsere Zukunft und das Gelingen der Digitalisierung ist die Gewährleistung unserer Cyber-Sicherheit. Netz- und Informationssysteme sind ein Schlüsselelement für die Sicherstellung der nationalen Sicherheit, des Wohlstandes und der Stabilität. Cyber-Angriffe, Software- und Hardwarefehler sowie menschliche Fehler in der Bedienung von IT-Systemen können das Funktionieren von wesentlichen Diensten stören und zu schwerwiegenden Ausfällen führen. Solche Ausfälle offenbaren die zunehmende Abhängigkeit unserer Gesellschaft. Eine Mehrheit von Staaten und die EU begegnet diesen Herausforderungen durch die Entwicklung von Cyber-Sicherheitsstrategien. Im Dezember 2020 hat die Europäische Union eine neue Cyber-Sicherheitsstrategie vorgestellt, Deutschland stellte im September 2021 seine Cyber-Sicherheitsstrategie vor, und Österreich steht knapp davor, eine neue Strategie zu veröffentlichen.

Cyber-Angriffe können das Funktionieren von wesentlichen Diensten stören und zu schwerwiegenden Ausfällen führen.

Leitlinien. Um ein hohes Niveau an Cyber-Sicherheit zu erreichen und aufrechtzuerhalten, muss jeder Staat über eine nationale Cyber-Sicherheitsstrategie verfügen, in der die strategischen Ziele und politische Maßnahmen vorgesehen sind. Auf europäischer Ebene ergibt sich diese Pflicht für Mitgliedsstaaten aus der NIS-Richtlinie. Der Staat hat die Aufgabe, zum einen das rasche Fortschreiten der Digitalisierung zu fördern und gleichzeitig dem Interesse der Bürger/-innen nach einem sicheren Cyber-Raum zu wahren. Die Leitlinien dafür und vor allem für eine gelungene Zusammenarbeit mit Wirtschaft, Wissenschaft und Zivilgesellschaft müssen in einer Cyber-Sicherheitsstrategie festgelegt werden. Cyber-Sicherheitsstrategien sollen nationale Ressourcen darstellen und die Leitlinie für die Steuerung vorgeben. Die Definition und Festlegung der Ambitionen im internationalen und europäischen Kontext ist zentral. Der Cyber-Raum kennt keine Grenzen und eine ambitionierte Zusammenarbeit auf europäischer Ebene ist wichtig.

Die Themen Cyberkrisenmanagement, Lagebild und Bedrohungsanalyse sind wichtige Bausteine zur Förderung der Resilienz. Zuletzt sollte an den Aufbau von Kapazitäten und die Ausgestaltung zukünftiger Bildungsangebote sowie an die Zusammenarbeit mit Forschungseinrichtungen gedacht werden.

Die deutsche Cyber-Sicherheitsstrategie hat den Schutz der Behörden, kritischer Infrastruktur, Unternehmen und Bürger im Fokus. Die Regierung verweist auf die gestiegene Bedrohung im Laufe der vergangenen Jahre. Die Unsicherheiten im Cyberspace betreffen sowohl den privaten als auch den öffentlichen Sektor. Um Daten der Behörden zu schützen, soll künftig sichergestellt werden, „dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) frühzeitig in Digitalisierungsvorhaben des Bundes eingebunden wird".

Die deutsche Cyber-Sicherheitsstrategie hat unter anderem als Ziel, den Schutz kritischer Infrastrukturen weiter zu verbessern, eine leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur zu garantieren oder die Strafverfolgung im Cyber-Raum, auch international, zu intensivieren.

Auch in Österreich steht eine neue Cyber-Sicherheitsstrategie vor der Veröffentlichung. Die Federführung in der Ausarbeitung der Strategie hat das Bundeskanzleramt. Die 1. Österreichische Strategie für Cyber-Sicherheit (ÖSCS) stammt aus 2013. Die neue ÖSCS 2021 wird die strategischen Ziele und angemessenen Politik- und Regulierungsmaßnahmen für die nächsten Jahre bestimmen. Ein hohes Sicherheitsniveau von Netz- und Informationssystemen soll erreicht und aufrechterhalten werden. Sie ist ein zukunftsweisendes Dokument. Die Vision der ÖSCS 2021 ist die langfristige Schaffung eines sicheren Cyber-Raums als Beitrag zur Steigerung der Resilienz Österreichs und der Europäischen Union durch einen gesamtstaatlichen Ansatz.

Die ÖSCS 2021 wird aus einem allgemeinen Teil bestehen, der durch konkrete Maßnahmen der einzelnen Ressorts ergänzt werden muss. Die ÖSCS

Fotos: Syda Productions - stock.adobe.com

2021 weist konkrete Ziele aus: Österreich soll über die Fähigkeit verfügen seine kritischen Informationssysteme und Infrastrukturen im Krisenfall zu schützen und zu verteidigen. Ebenso soll es ein gesamtstaatliches Lagebild im Cyber-Bereich geben. Klare gesetzliche und operative Möglichkeiten müssen vorhanden sein, um ein sicheres und attraktives Unternehmensumfeld im Cyber-Raum zu bieten und gegebenenfalls eine adäquate Strafverfolgung zur gewährleisten. Die Zusammenarbeit vor allem im Rahmen der EU und im internationalen Bereich wird eine zentrale Rolle in den nächsten Jahren spielen.

Der Bereich Cyber-Sicherheit bringt Chancen. Dies ist in der ÖSCS 2021 besonders hervorgekehrt. Der Cyber-Raum ist ein wichtiger Partizipationsraum für die Gesellschaft, umso wesentlicher ist seine Sicherheit. Auch die Wirtschaft kann von Cyber-Sicherheit nur profitieren. Es ergeben sich Möglichkeiten für neue Geschäftsfelder und Märkte. Eine widerstandsfähige und cybersichere Unternehmensinfrastruktur garantiert Betriebskontinuität. Cyber-Sicherheit birgt Potenzial zur Erweiterung des Bildungsbereiches. Der öffentliche Sektor kann den Ausbau der sicheren und direkten Interaktion mit Bürger/-innen und der Wirtschaft ausbauen. Ein verlässliches Cyber-Krisenmanagement stärkt das Vertrauen in die staatlichen Institutionen und sichert ihr Handlungsfähigkeit.

Zusammenarbeit. Zusammenfassend sei nochmal darauf hingewiesen, dass die Zahl der Cyber-Angriffe in den letzten Jahren zugenommen hat und auch weiterhin steigen wird. Der Cyber-Raum kennt keine Landesgrenzen, eine Zusammenarbeit mit anderen Staaten genauso wie eine ausgezeichnete gesamtstaatliche Kooperation sind entscheidend, um ihn sicher zu machen. Nur wenn es gelingt, Risiken im Cyber-Bereich niedrig zu halten, können sich die Vorteile der Digitalisierung voll entfalten. Strategische Leitlinien in der Form einer nationalen Cyber-Sicherheitsstrategie sind hier sehr wichtig. Sowohl die deutsche als auch die österreichische Strategie zur Cyber-Sicherheit geben den Rahmen für die Cyber-Sicherheit vor und werden dafür sorgen, dass der volle Nutzen der digitalen Welt ausgekostet werden kann.

Caroline Schmidt