Cyberrisiken sind eine ernsthafte Bedrohung

Cyberangriffe nehmen in der Schweiz zu. Mit seiner neuen Strategie will der Bundesrat deshalb auch Unternehmen und Privatpersonen beim Kampf gegen kriminellen Datendiebstahl unterstützen. *Manuel Suter*

Abstract Cyberangriffe sind allgegenwärtig und betreffen sowohl Privatpersonen als auch Unternehmen und Behörden. Sie entwickeln sich rasant weiter und gefährden den Nutzen der Digitalisierung. Der Bund reagiert auf diese Bedrohungen mit einer neuen «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» (NCS). Darin ist vorgesehen, dass zu deren Umsetzung ein Kompetenzzentrum Cybersicherheit unter der Leitung eines Delegierten des Bundesrates geschaffen wird. Neu sollen zudem nicht mehr nur kritische Infrastrukturen im Kampf gegen Cyberangriffe unterstützt werden, sondern auch Unternehmen und Privatpersonen.

Täglich werden in der Schweiz Rechner angegriffen. Oft handelt es sich bei diesen Cyberangriffen um breit angelegte, weltweit durchgeführte Versuche, Daten zu entwenden oder finanzielle Transaktionen zu manipulieren. Vor allem Erpressungen über Cyberangriffe haben zugenommen. Dabei verschlüsseln die Täter die Daten beispielsweise mithilfe von Verschlüsselungstrojanern, sodass nicht mehr auf sie zugegriffen werden kann. Dann verlangen sie Geld, meist in Kryptowährungen, um die Daten wieder zu entschlüsseln. Bei anderen Erpressungsmethoden schicken die Täter ihren Opfern Auszüge aus gestohlenen Datensätzen und drohen bei ausbleibendem Lösegeld mit der Veröffentlichung von sensiblen Personendaten. Perfide dabei ist, dass es den Opfern kaum möglich ist, abzuschätzen, ob die Täter tatsächlich über diese sensiblen Daten verfügen oder nicht.

Neben diesen breit angelegten Angriffen sind Unternehmen und Behörden auch mit sehr gezielten Attacken konfrontiert. Dafür investieren die Angreifer viel Zeit und Geld, um in die Systeme einzudringen. Bei solchen Angriffen steht aber nicht die unmittelbare finanzielle Bereicherung im Zentrum. Vielmehr wollen die Täter an wertvolle Informationen kommen, welche ihnen längerfristige wirtschaftliche oder politische Vorteile verschaffen.

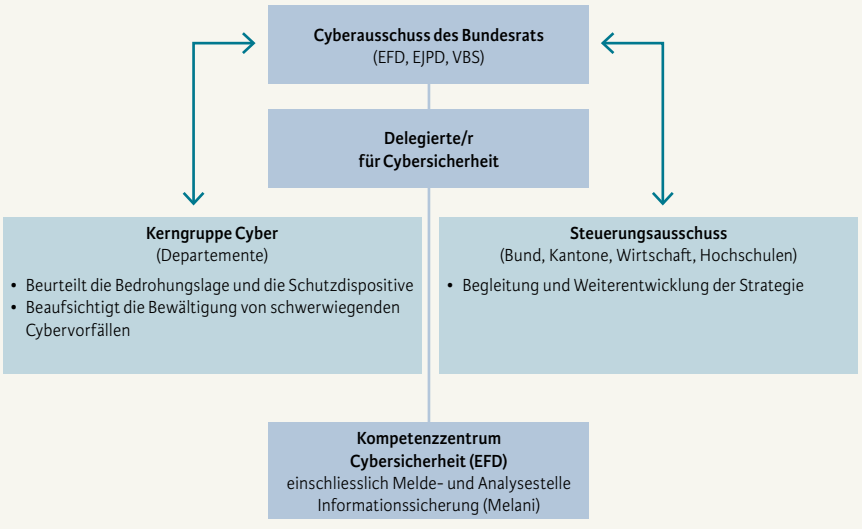
Neue Strategie zum Schutz vor Cyberrisiken

Wie schützt sich die Schweiz vor solchen Cyberangriffen? Dazu hat der Bundesrat im vergangenen Jahr wegweisende Entscheide getroffen. Bereits im April 2018 hat er die neue «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)»[1] für die Jahre 2018 bis 2022 verabschiedet und darin Handlungsfelder und Massnahmen definiert. Im Vergleich zur Vorgängerstrategie von 2012 bis 2017 trägt die neue NCS dem Umstand Rechnung, dass Cyberrisiken zu einer relevanten Bedrohung für alle Unternehmen und für die Sicherheit und das Wohlbefinden der Bevölkerung geworden sind. Die Vorgängerstrategie fokussierte noch vornehmlich auf den Schutz kritischer Infrastrukturen wie Energieversorger, Telekommunikationsanbieter, Spitäler oder Banken. Im Gegensatz dazu verlangt die neue NCS explizit, dass der Bund alle Unternehmen und die Bevölkerung beim Schutz vor Cyberrisiken unterstützt. Die Strategie beinhaltet aber nicht nur Massnahmen, um den unmittelbaren Schutz zu stärken. Sie will die Cybersicherheit auch mit längerfristig ausgerichteten Massnahmen verbessern. Beispielsweise durch den Ausbau von Fähigkeiten und Wissen in der Schweiz, aber auch durch die Förderung und Pflege von internationalen Beziehungen. Von besonderer Bedeutung sind dabei für die Schweiz die Aktivitäten der Europäischen Union zur Stärkung der Cybersicherheit in Europa. Der bereits fertig ausgehandelte Rechtsakt zur Cybersicherheit in der EU[2] sieht einen europäischen Zertifizierungsrahmen für Produkte, Verfahren und Dienste vor. Die Schweiz wird die Entwicklung dieses Zertifizierungsrahmens aufmerksam beobachten und bei Bedarf die nötigen Schritte einleiten, damit die Schweizer

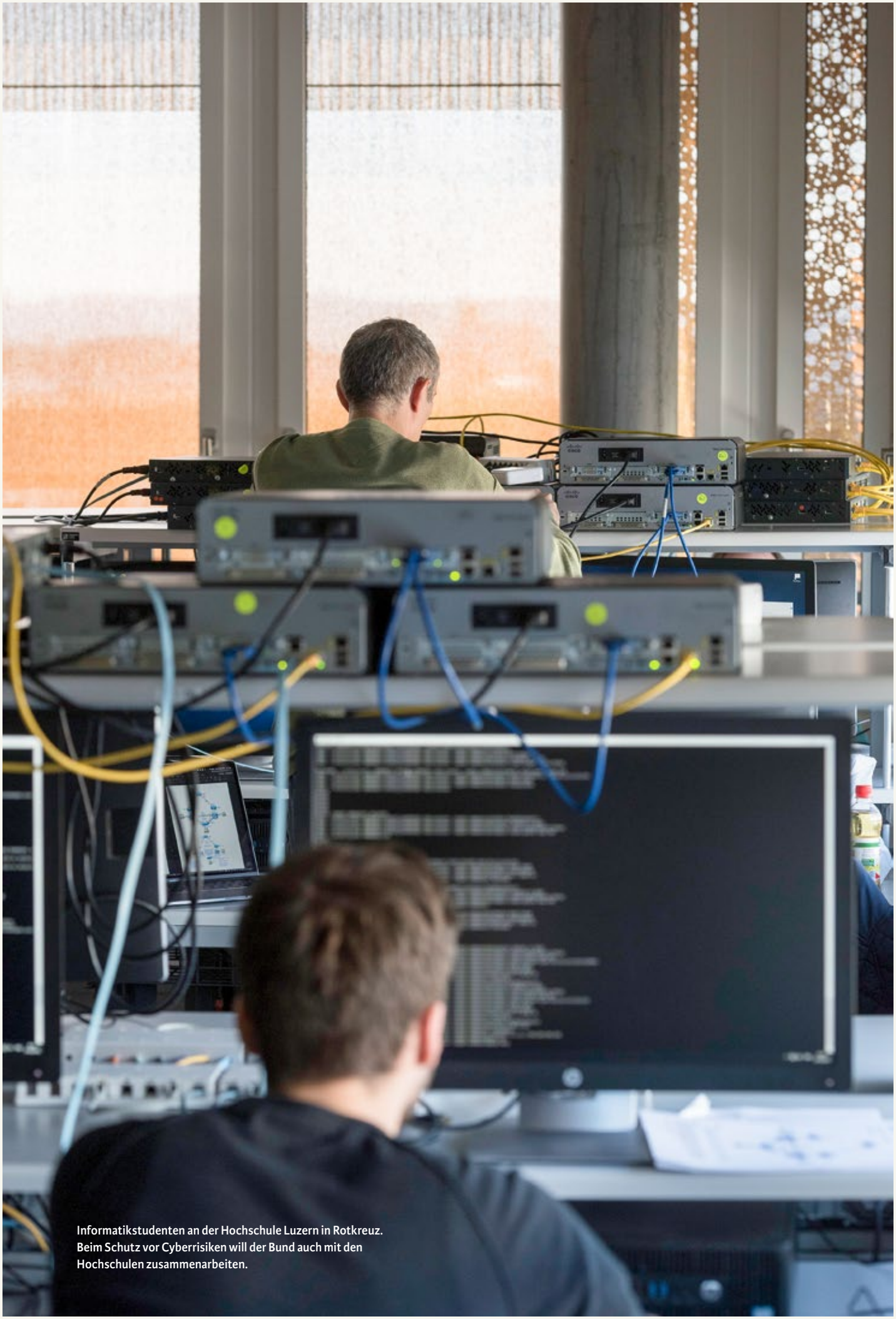
1 Die vollständige Strategie ist online auf Isb.admin.ch verfügbar.

2 Siehe European Commission (2017). Regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification («Cybersecurity Act») (nur in Englisch verfügbar).

So will der Bundesrat den Bereich Cyberrisiken reorganisieren:



BUNDESKANZLEI/ DIE VOLKSWIRTSCHAFT



Informatikstudenten an der Hochschule Luzern in Rotkreuz. Beim Schutz vor Cyberrisiken will der Bund auch mit den Hochschulen zusammenarbeiten.

KEYSTONE

Wirtschaft mit den europäischen Vorgaben zur Cybersicherheit kompatibel bleibt.

Mit der Verabschiedung der NCS hat der Bundesrat auch entschieden, die Bundesstellen im Bereich Cyberrisiken neu zu organisieren (siehe *Abbildung*). Diesen Januar hat er die dazu nötigen Beschlüsse gefasst und einen Cyberausschuss geschafft, in dem das Finanzdepartement (EFD), das Justiz- und Polizeidepartement (EJPD) sowie das Verteidigungsdepartement (VBS) vertreten sind. Damit hat der Bundesrat seine eigene Führungsrolle in diesem Bereich gestärkt. Die Vorstehenden der drei Departemente werden sich künftig regelmässig über die Cybersicherheit austauschen und dafür sorgen, dass die Strategie zielgerichtet umgesetzt wird. Unterstützt werden sie dabei von zwei Gremien: der «Kerngruppe Cyber» und dem «Steuerungsausschuss NCS». In der Kerngruppe beraten Vertreter der drei Departemente unter situationsbedingtem Einbezug weiterer Departemente und der Kantone die Lage im Cyberbereich. Zudem beurteilen sie die vorhandenen technischen und organisatorischen Schutzdispositive des Bundes. Der Steuerungsausschuss NCS stellt die koordinierte und zielgerichtete Umsetzung der NCS-Massnahmen sicher und erstattet dem Bundesrat jährlich Bericht über den Stand der Umsetzung. Im Steuerungsausschuss vertreten sind nicht nur die zuständigen Bundesstellen, sondern auch Vertretungen der Kantone, der Wirtschaft und der Hochschulen.

Ein Kompetenzzentrum für Cybersicherheit

Neben der Stärkung der Führungsrolle des Bundesrates und der verbesserten Koordination soll es neu auch eine Delegierte oder einen Delegierten für Cybersicherheit und ein Kompetenzzentrum geben. Der oder die Delegierte wird die zentrale Ansprechperson des Bundes für Cybersicherheit. Sie ist direkt dem Departementsvorsteher des EFD unterstellt. Ihre Aufgaben sind die strategische Leitung des Kompetenzzentrums Cybersicherheit sowie der Vorsitz über die Koordinationsgremien «Kerngruppe Cyber» und «Steuerungsausschuss NCS». Der oder die Delegierte führt somit die wichtigsten Gremien des Bundes im zivilen Bereich der Cybersicherheit. Ausserdem steht er oder sie in der Verantwortung, die Umsetzung der NCS voranzubringen, die Strategie und die Organisation des Bundes weiterzuentwickeln und den Bund im Bereich Cybersicherheit zu repräsentieren.

Mit dem Kompetenzzentrum für Cybersicherheit will der Bundesrat schliesslich die Forderungen aus Politik und Wirtschaft nach einer nationalen Anlaufstelle umsetzen. Das Zentrum basiert auf der bestehenden Melde- und Analysestelle Informationssicherung (Melani), die so ausgebaut werden soll, dass sie die Funktion einer nationalen Anlaufstelle übernehmen kann. Zudem soll sich das Kompetenzzentrum stärker bei der Sensibilisierung engagieren und gemeinsam mit Partnern aus der Wirtschaft und den Kantonen dazu beitragen, die Bevölkerung über Cybersicherheit zu informieren.

Zusammenarbeit aller Akteure

Weil Cyberrisiken alle betreffen, können sie auch nur durch gemeinsame Anstrengungen bekämpft werden. Der Bund ist deshalb beim Schutz der Schweiz vor Cyberrisiken auf die Zusammenarbeit mit den Kantonen, der Wirtschaft und den Hochschulen angewiesen. Der Umsetzungsplan zur NCS, welcher aktuell noch in Erarbeitung ist, legt fest, wer welche Aufgaben übernimmt. Er wird somit die Grundlage für die koordinierte Zusammenarbeit aller Akteure bilden. Die Umsetzungsarbeiten zur NCS mit den wichtigsten Partnern zu koordinieren, ist der Zweck der gemeinsamen Plattform des Steuerungsausschusses NCS.

Mit der Verabschiedung der NCS, der Stärkung und Klärung der Strukturen des Bundes und den geschaffenen Gremien für die Zusammenarbeit sind nun die wesentlichen Voraussetzungen für einen effektiven Schutz vor Cyberrisiken vorhanden. Es steht den verantwortlichen Stellen und Gremien jedoch viel Arbeit bevor. Die in der NCS festgehaltenen Massnahmen müssen rasch umgesetzt werden, und neue Herausforderungen müssen rechtzeitig erkannt und angegangen werden. Strategien und Organisationsstrukturen sind zwar wichtige Grundlagen, um den Schutz vor Cyberrisiken zu verbessern, sie erfüllen ihren Zweck aber nur, wenn sie durch ein grosses, breit abgestütztes Engagement getragen werden. Zudem müssen alle beteiligten Akteure verstehen, dass Cybersicherheit im Umfeld der digitalen Transformation eine Daueraufgabe und die gemeinsame Verantwortung aller ist.

Manuel Suter
Dr. sc. ETH, Leiter Koordinationsstelle NCS, Eidgenössisches Finanzdepartement (EFD), Bern