Der Bund will den Schutz vor Cyberrisiken ausbauen

Mit Cyberattacken können Daten von Unternehmen und Privatpersonen entwendet und ganze Strominfrastrukturen lahmgelegt werden. Deshalb schützt der Bund kritische Infrastrukturen vor solchen Angriffen mit einem Frühwarnsystem. Zukünftig will er die Kapazitäten in diesem Bereich sogar ausbauen. *Max Klaus*

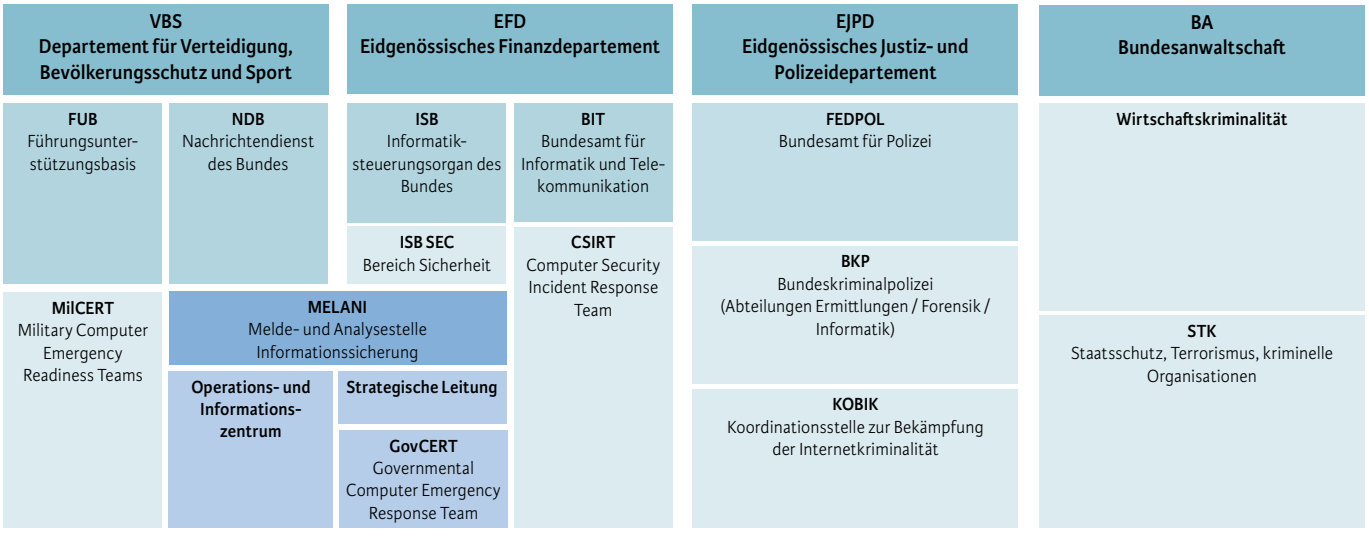
Abstract Der Bundesrat hat früh erkannt, wie wichtig es ist, sich mit der Gefahr zu befassen, die von Cyberattacken ausgeht. Mit verschiedenen Einheiten geht er gegen solche Angriffe vor. So etwa mit der Melde- und Analysestelle Informationssicherung (Melani), mit der er nicht nur die Bundesstellen, sondern auch die kritischen Infrastrukturen von Banken, Energieversorgern und Telekommunikationsunternehmen schützt. Da der digitale Raum länderübergreifend ist, muss sich die Schweiz auch international gut vernetzen und Informationen austauschen. Im Rahmen multilateraler Organisationen setzt sie sich für mehr Kooperation und Transparenz im digitalen Raum ein. Der Bund ist sich auch der zukünftigen Bedeutung dieser Gefahr bewusst. Mit einer Strategie will er deshalb die vorhandenen Kapazitäten in Verwaltung und Wirtschaft weiter ausbauen und damit die Widerstandskraft der Schweiz gegenüber Cyberangriffen stärken.

Die Verschlüsselungstrojaner «Wanna Cry» und «Petya» haben vor wenigen Monaten weltweit für Schlagzeilen gesorgt. Im Fall «Wanna Cry» waren 200 000 Geräte in 150 Ländern infiziert, betroffen waren zahlreiche Spitäler in Grossbritannien oder Fahrplanmonitore der Deutschen Bahn sowie ein Telekommunikationsunternehmen in Spanien. Dabei wurden bestimmte Dateien eines Computers verschlüsselt und die Nutzer aufgefordert, einen Betrag in Bitcoin zu überweisen, um so einem Datenverlust zu entgehen. Doch solche Angriffe sind keine Einzelfälle: Der Internetkonzern Yahoo teilte vor einigen Monaten mit, ihm seien über 500 Millionen Passwörter von Firmenkunden entwendet worden. In der Ukraine waren im Dezember 2015 die Konsequenzen eines solchen Angriffs sogar am eigenen Leib erfahrbar, als ein offensichtlicher Cyberangriff die Strominfrastruktur lahmlegte und über eine Viertelmillion Menschen ohne Strom blieb. Diese Aufzählung liesse sich beliebig verlängern. Die Gefahr von Cyberattacken besteht für alle und zu jeder Zeit. Wie gut ist die Schweiz gewappnet, und was tut der Bund gegen solche Angriffe?

Grundlegende Infrastrukturen schützen

In der Bundesverwaltung befassen sich verschiedene Verwaltungseinheiten mit der Cybersicherheit (siehe *Abbildung*). In erster Linie stehen die bundeseigenen Netze im Fokus: Das Bundesamt für Informatik und Telekommunikation (BIT) ist verantwortlich für den Schutz der zivilen Bundesnetze. Die Führungsunterstützungsbasis (FUB) im Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) kümmert sich um die Sicherheit der militärischen Netze. Für einheitliche und für alle Bundesverwaltungseinheiten verbindliche Sicherheitsvorgaben sorgt schliesslich das Informatiksteuerungsorgan des Bundes (ISB). Zu diesen Vorgaben gehört beispielsweise das Einhalten des Grundschutzes in der Informations- und Kommunikationstechnik (IKT).

Die Organisationen des Bundes zur Bekämpfung von Cyberrisiken



MELANI / DIE VOLKSWIRTSCHAFT

KEYSTONE

Im Internet lauern Gefahren. Der Bund will private Nutzer besser schützen.

So wie die Bundesverwaltung ihre Infrastrukturen schützen muss, schützen auch die Unternehmen ihre IKT-Systeme. Allerdings hat der Bundesrat schon 2003 die Notwendigkeit erkannt, die Betreiber von kritischen Infrastrukturen in der Schweiz beim Schutz vor Cyberrisiken zu unterstützen. Er hat dem Eidgenössischen Finanzdepartement (EFD) deshalb den Auftrag erteilt, die Melde- und Analysestelle Informationssicherung (Melani) aufzubauen. Diese ist seit Oktober 2004 operativ tätig und wird täglich über Cyberangriffe aller Art informiert.

Dem Grundauftrag des Bundesrates gemäss befasst sich Melani vorwiegend mit dem Schutz von kritischen Infrastrukturen von Schweizer Grossunternehmen wie Banken, Energieversorgern, Telekommunikationsunternehmen usw. Täglich tauscht Melani mit diesen Unternehmen Informationen zu aktuellen Angriffen und Bedrohungen aus. Diese Informationen stammen häufig aus öffentlich nicht zugänglichen Quellen und bieten einen wichtigen Mehrwert für die Sicherheitsarchitektur der verschiedenen Unternehmen.

Die Beschaffung dieser Informationen ist mitunter ein Grund, weshalb Melani auf zwei Departemente aufgeteilt ist. Die strategische Leitung, welche die Gesamtverantwortung trägt, sowie das Governmental Computer Emergency Response Team (Govcert) befinden sich im EFD. Govcert[1] bildet die technische Abteilung von Melani. Hier sitzen Spezialisten, die in der Lage sind, Schadsoftware zu analysieren und dadurch Hinweise auf die möglichen Absichten und die Herkunft der Täterschaft zu gewinnen. Das Operations- und Informationszentrum (OIC) ist der operative Teil von Melani und ist beim Nachrichtendienst des Bundes (NDB) im VBS angesiedelt. Das OIC ist der Ansprechpartner für die Betreiber von kritischen Infrastrukturen und kann beispielsweise die Sperrung von Internetsites beantragen, die in Zusammenhang mit Cyberangriffen stehen.

Bekämpfung der Internetkriminalität

Doch Melani ist nicht die einzige Bundesstelle im Kampf gegen die neuen digitalen Gefahren. Bereits seit 2001 betreibt das Eidgenössische Justiz- und Polizeidepartement (EJPD) innerhalb des Bundesamts für Polizei (Fedpol) die Koordinationsstelle zur Bekämpfung der Internetkriminalität.

Die Stelle ist eine Kooperation zwischen dem Bund und den 26 kantonalen Polizeikorps und dient als Ansprechstelle für Privatpersonen und KMU, wenn diese Opfer von Cyberangriffen geworden sind. Die eingegangenen Meldungen werden nach Überprüfung an die zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet. Die Koordinationsstelle verfügt, wie auch die Bundesanwaltschaft, über einen Ermittlungsauftrag und sucht deshalb im Internet auch proaktiv nach strafrechtlich relevanten Inhalten.

Internationale Zusammenarbeit entscheidend

Es wäre fatal, zu glauben, eine Meldestelle könne die kritischen Infrastrukturen im eigenen Land ohne ausländische Unterstützung schützen. Denn die Grosszahl von Cyberangriffen macht nicht halt vor Landesgrenzen. Oft sind zahlreiche Unternehmen und Privatpersonen in verschiedensten Staaten betroffen. Ein internationales Netzwerk von Melani-ähnlichen Organisationen in Europa und Übersee ist unabdingbar, um rund um die Uhr rasch an zuverlässige Informationen aus vertrauenswürdigen Quellen zu kommen.

Aus diesem Grund existieren Organisationen wie European Government Certs (EGC) und Forum for Incident Response and Security Teams (First), bei welchen Melani Mitglied ist. EGC ist ein europäischer Verbund

1 Weitere Informationen finden Sie unter Govcert.ch.

von staatlichen Stellen, welche die kritischen Infrastrukturen in ihrem Land vor Cyberangriffen schützen sollen. Täglich tauschen die Mitgliedsstaaten Informationen über Angriffe oder Bedrohungen aus. First ist eine weltweit tätige Organisation von Sicherheitsexperten, die auch für die Privatwirtschaft offen ist. Die Mitglieder stammen hauptsächlich aus Nordamerika und Asien, sodass Melani ihr Netzwerk auch auf diesen Kontinenten pflegen und ausbauen kann.

Diese Kontakte zahlen sich aus. Im Fall des Trojaners «Wanna Cry» beispielsweise hat Melani von einem EGC-Mitgliedsstaat mehrere Stunden vor dem öffentlichen Bekanntwerden des Angriffs wichtige Informationen dazu erhalten und konnte dadurch die Betreiber der kritischen Infrastrukturen warnen, bevor die Angriffswelle in der Schweiz ankam. Ebenfalls ein wertvoller Informant ist der Nachrichtendienst des Bundes, der ebenfalls über ein breites internationales Netzwerk verfügt.

Aussensicherheitspolitik im digitalen Raum

Neben dem Technisch-Operationellen ist die internationale Zusammenarbeit auch auf diplomatischer Ebene wichtig. Der digitale Raum ist neben Boden, Luft und Wasser zu einer neuen Dimension der staatlichen Interaktion geworden und kann entsprechend auch für machtpolitische, militärische oder nachrichtendienstliche Zwecke benutzt werden. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) setzt sich im Rahmen multilateraler Prozesse und bilateraler Konsultationen für einen digitalen Raum ein, der friedlich genutzt und nicht zum Austragungsort von Konflikten oder zum Katalysator von Spannungen zwischen Staaten wird.

In einem politischen Umfeld, das stark von Misstrauen und Ungewissheit geprägt ist, ist es zentral, das Vertrauen zwischen Staaten auch im digitalen Raum zu fördern. Dazu dienen vertrauensbildende Massnahmen, die den Informationsaustausch und die Transparenz fördern und somit die Grundlage zu mehr Kooperation schaffen. Ein solcher freiwilliger Informationsaustausch kann beispielsweise die Bekanntgabe von gegenseitigen staatlichen Kontaktstellen bei Cyberattacken oder die Veröffentlichung der als kritisch eingestuften Infrastrukturen umfassen. Die Schweiz engagiert sich diesbezüglich vor allem in der OSZE, wo sie bei der Erarbeitung und der Operationalisierung solcher Massnahmen massgeblich beteiligt ist.

Nationale Strategie

Die beschriebenen Aktivitäten tragen alle dazu bei, die Schweiz vor Cyberrisiken zu schützen. Sie bilden zentrale Elemente der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)»[2], welche 2012 vom Bundesrat verabschiedet wurde.
Die NCS umfasst insgesamt 16 Massnahmen, welche in Zusammenarbeit zwischen den zuständigen Behörden, der Wirtschaft und den Betreibern kritischer Infrastrukturen umgesetzt werden. Zudem wurden im Rahmen der NCS für die Sektoren der kritischen Infrastrukturen Risiko- und Verwundbarkeitsanalysen durchgeführt, die Forschung und Bildung im Bereich Cyberrisiken gestärkt sowie die Fähigkeiten des NDB im Bereich der Früherkennung von Cyberbedrohungen und in Bezug auf Täteridentifikation ausgebaut. Die Umsetzung der NCS wird bis Ende 2017 abgeschlossen sein. Deshalb soll das ISB, das die Strategie koordiniert, bis Ende 2017 in Zusammenarbeit mit allen betroffenen Stellen der Verwaltung und mit Partnern aus der Wirtschaft eine Nachfolgestrategie für die Jahre 2018–2022 ausarbeiten.

Die neue Strategie versteht sich als Fortsetzung, Weiterentwicklung und Optimierung der ersten NCS. Die Fähigkeiten des Bundes bei der Erkennung und Einschätzung von Cyberrisiken, bei der Bekämpfung von Vorfällen und bei der Strafverfolgung müssen weiter ausgebaut werden. Die Zusammenarbeit innerhalb der Bundesverwaltung wird in diesen Bereichen verstärkt, und es wird eine Erhöhung der Mittel für die Vorfallbekämpfung, die Cyberabwehr und die Strafverfolgung angestrebt.

Die Zusammenarbeit zwischen Staat und Wirtschaft bleibt ein Kernanliegen der NCS. Während die erste NCS den Fokus auf den Schutz kritischer Infrastrukturen legte, zählt die Nachfolgestrategie auch die KMU und die Bevölkerung zu den Zielgruppen. Der Bund will diesen Zielgruppen beim Umgang mit Cyberrisiken verstärkt Unterstützung anbieten, ohne dabei in Konkurrenz zu privaten Anbietern von Sicherheitslösungen zu treten. Beispiele für vorgesehene Massnahmen zur Stärkung der Resilienz der Wirtschaft gegenüber Cyberrisiken sind die Evaluation und Einführung von branchenspezifischen Mindeststandards, die Prüfung einer Meldepflicht für sicherheitsrelevante Vorfälle und die Aufbereitung von Informationen zu Cyberbedrohungen für die Wirtschaft und die Bevölkerung.

Max Klaus
stellvertretender Leiter Melde- und Analysestelle Informationssicherung (Melani), Informatiksteuerungsorgan des Bundes (ISB), Bern

2 Siehe VBS (2012). Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken.