# «Produktesicherheit und Supply Chain Risk Management in den Bereichen Cybersicherheit und Cyberdefence»

Bericht des Bundesrates
in Erfüllung der Postulate Dobler 19.3135 «Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff?» und 19.3136 «Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?» vom 18. März 2019

# Inhaltsverzeichnis

# Management Summary

Neben dem grossen Nutzen, den die Verwendung von Informations- und Kommunikationstechnologien (IKT) stiftet, ist deren Einsatz auch mit erheblichen Risiken verbunden. Diesen sogenannten Cyberrisiken wird mit verschiedenen Massnahmen begegnet. Diese umfassen die Prävention von Ausfällen und Manipulationen, die Stärkung der Resilienz oder den Aufbau von Abwehrdispositiven gegenüber Angriffen. Den Bemühungen zur Minderung von Cyberrisiken läuft zuwider, dass es bisher nicht gelungen ist, die Produktesicherheit von IKT-Produkten adäquat zu verbessern. Nach wie vor weisen diese oft zahlreiche Sicherheitslücken auf.

Die Anwendung von Sicherheitsstandards kann helfen, dieses Problem zu entschärfen. Der Bericht legt die vorhandenen Standards im Bereich Produktesicherheit und Supply Chain Risk Management dar und zeigt deren Verbindlichkeit für den Bund und für die Betreiber kritischer Infrastrukturen auf. Die Analyse zeigt, dass zahlreiche Standards im Bereich der Produktesicherheit und der sicheren Anwendung dieser Produkte existieren. Verschiedene dieser Standards in Bezug auf Produktesicherheit finden auch eine breite Anwendung. Vorgaben zum Supply Chain Risk Management im Bereich der Cybersicherheit sind deutlich weniger weit entwickelt.

Weiter geht der Bericht auf den Rechtsrahmen für die Anwendung der Standards in der Bundesverwaltung und bei kritischen Infrastrukturen ein. Der Bericht kommt dabei zum Schluss, dass für den Bund die rechtliche Grundlage für eine konsequente Anwendung von Standards in der IKT-Produktesicherheit und im Supply Chain Risk Management vorhanden sind, während es für kritische Infrastrukturen nur vereinzelt Bestimmungen gibt, aus welchen sich die Einhaltung von Standards für die IKT-Sicherheit ableiten lässt.

Schliesslich legt der Bericht dar, inwiefern Standards in der Bundesverwaltung, in der Armee und bei kritischen Infrastrukturen tatsächlich Anwendung finden. Innerhalb der Bundesverwaltung und in der Armee bestehen zahlreiche Vorgaben zur Sicherheit und zur sicheren Anwendung von IKT-Produkten. In Bezug auf Standards zur Produktesicherheit kommt der Bericht zum Schluss, dass der Fokus stärker auf eine durchgehende und umfassende Umsetzung der Vorgaben sowie auf die Kontrolle dieser Umsetzung gelegt werden muss, statt auf die Weiterentwicklung der bereits weitgehend ausgearbeiteten Vorgaben und Standards. Vorgaben zum Supply Chain Risk Management im Bereich der Cybersicherheit sind deutlich weniger weit entwickelt. Es existiert auch keine Grundlage, welche die Umsetzung eines systematischen Risikomanagements vorschreibt. Die meisten dieser Standards fokussieren auf Prozesse und Methoden, weswegen sie eher den Charakter von unverbindlichen Handlungsanweisungen statt von verbindlichen Normen erhalten.

Im Vergleich zur Situation in der Bundesverwaltung existieren für kritische Infrastrukturen nur wenige verbindliche Vorgaben zur Sicherheit und zur sicheren Anwendung von IKT-Produkten. Die offensichtlichste Option zur stärkeren Verbreitung von Standards ist es, neue rechtlich bindende Vorgaben zu schaffen. Auch Verweise auf Standards im Bereich der Produktesicherheit wären möglich. Denkbar wären zudem Vorgaben für die Betreibenden kritischer Infrastrukturen zum sicheren Umgang mit IKT-Produkten. Grundsätzlich könnten auch Vorgaben zum Supply Chain Risk Management über regulative Massnahmen eingeführt werden.

# 1 Einleitung

Die Digitalisierung schreitet in der Schweiz rasch voran. Die digitale Vernetzung gehört heute zum Alltag von Unternehmen und Behörden. Informations- und Kommunikationstechnologien (IKT) sind dabei so wichtig geworden, dass praktisch alle Dienstleistungen unserer Gesellschaft nicht mehr erbracht werden können, wenn diese Mittel ausfallen oder nicht mehr korrekt funktionieren. Neben dem grossen Nutzen, den die Verwendung von IKT bringt, sind durch deren Einsatz auch erhebliche Risiken entstanden, die als Cyberrisiken bezeichnet werden. Ihnen wird mit verschiedenen Massnahmen begegnet. Es wird versucht, mit technischen und organisatorischen Präventionsmassnahmen zu verhindern, dass die IKT ausfallen oder manipuliert werden können. Über Massnahmen zur Stärkung der Resilienz soll zudem dafür gesorgt werden, dass Organisationen auch dann funktionieren, wenn die IKT trotzdem ausfallen sollten. Weiter werden Abwehrdispositive aufgebaut, um Angriffe gegen die IKT abzuwehren.

Diesen Bemühungen zur Minderung von Cyberrisiken läuft jedoch zuwider, dass es bisher nicht gelungen ist, die Produktesicherheit von IKT-Produkten adäquat zu verbessern. Nach wie vor weisen diese oft zahlreiche Sicherheitslücken aus. Dafür existieren sowohl ökonomische als auch politische Gründe. Die ökonomischen Gründe wurden von verschiedenen Forschern schon vor 20 Jahren aufgezeigt.[1] Erstens lässt sich der Markt für IKT-Produkte als Netzwerkökonomie beschreiben. Konsumenten werden ein Produkt nur dann kaufen, wenn sie davon ausgehen, dass viele andere den gleichen Entscheid treffen. Damit soll zusätzlicher Aufwand bei der Zusammenarbeit mit Partnern vermieden werden. Für Produzenten ist es deshalb entscheidend, dass ihr IKT-Produkt möglichst rasch möglichst viele Nutzer findet und sich als Standardlösung etabliert. Als Folge davon versuchen sie, ihr Produkt möglichst rasch auf den Markt zu bringen und allfällige Probleme – zum Beispiel Sicherheitslücken – erst dann zu lösen, wenn das Produkt sich durchgesetzt hat.[2] Zweitens fördert die Informationsasymmetrie zwischen Anbieter und Käufer die mangelnde Sicherheit von IKT-Produkten. Weil die Käufer beim Kaufentscheid die Qualität der Produkte nicht abschätzen können, besteht umgekehrt für die Anbieter kein Anreiz, die Qualität in jedem Fall sicherzustellen. Die fehlende Transparenz in Bezug auf Sicherheit führt dazu, dass Anbieter die Sicherheit ihrer Produkte nicht priorisieren.[3]

Zusätzlich zu diesen ökonomischen Faktoren gewinnen geopolitische Faktoren an Bedeutung. Die Märkte für IKT-Produkte werden zunehmend als sicherheitspolitisches Interessensgebiet betrachtet. Spätestens seit den Enthüllungen durch Edward Snowden 2013 ist auch der breiten Öffentlichkeit unwiderlegbar bekannt, dass Regierungen nicht davor zurückschrecken, direkten Einfluss auf die Hersteller von IKT-Produkten auszuüben, um so Zugang zu Daten zu erhalten. Dies hat das Vertrauen in die Sicherheit von IKT-Produkten weiter untergraben und vielen Staaten vor Augen geführt, dass die Abhängigkeit ihrer Wirtschaft und ihrer Gesellschaft von IKT, welche insbesondere von Produzenten aus Nationen mit Grossmachtstatus hergestellt werden, aus sicherheitspolitischer Perspektive problematisch ist.

Weder die Eigenschaften des IKT-Marktes noch die Dominanz einiger weniger Hersteller aus Nationen mit Grossmachtstatus lassen sich kurz- bis mittelfristig ändern und IKT-Produkte werden nie völlig sicher sein. Dennoch müssen Möglichkeiten geprüft werden, wie die Sicherheit von IKT-Produkten in Bereichen, die für die Schweiz kritisch sind, verbessert werden kann. Die Anwendung von Standards für die Sicherheit kann dazu einen wichtigen Beitrag leisten. Es bestehen heute schon viele verbreitete Standards zur IKT-Sicherheit, welche laufend weiterentwickelt werden. Indem diese Standards klare und messbare Kriterien für die Sicherheit definieren, erhöhen sie die Transparenz und helfen dabei, dass sich die Sicherheit als feststellbares Qualitätskriterium durchsetzen kann. Werden Standards von Unternehmen und Behörden konsequent eingefordert, erhöht dies den Druck auf die Hersteller, die Sicherheit besser zu berücksichtigen.

---

[1] GORDON/LOEB: "The economics of information security investment», ACM Transactions on Privacy and Security Volume 5, Issue 4, 2002;
ANDERSON/MOORE: "The economics of information security", Science, Vol. 314, 2006, pp. 610-613.

[2] SHAPIRO/VARIAN: "Information Rules. A Strategic Guide to the Network Economy", Boston, Harvard Business School Press, 1998.

[3] GEORGE A. AKERLOF: The market for 'lemons': Quality, uncertainty and the market mechanism. The Quarterly Journal of Economics, Vol. 84, 1970, pp. 488–500;
RAINER BÖHME: A Comparison of Market Approaches to Software Vulnerability disclosure, in: G. Müller (Ed): Emerging Trends in Information and Communication Security, ETRICS 2006, pp. 298-311; part of the Lecture Notes in Computer Science book series (LNCS, volume 3995), Springer, Berlin, Heidelberg

Der vorliegende Bericht soll aufzeigen, welche Massnahmen der Bund und insbesondere die Armee bei sicherheitsrelevanten Beschaffungen umsetzen, welche Massnahmen die Betreiber von kritischen Infrastrukturen vornehmen und wo möglicher Handlungsbedarf besteht.

## 1.1 Ausgangslage

Die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018 – 2022» (NCS)[4] beschreibt die Massnahmen von Bund, Kantonen, Wirtschaft und Hochschulen zur Minderung der bestehenden Cyberrisiken. Sie enthält Massnahmen zur Standardisierung und zur Förderung der Resilienz von kritischen Infrastrukturen gegenüber Cyberrisiken, geht jedoch nicht explizit auf die spezifischen Risiken der Lieferketten, dem sogenannten «Supply Chain Risk», ein. Einen konkreten Bezug zur Sicherheit von Lieferketten und zur Bedeutung von internationalen Standards stellt dafür die neue «Strategie Cyber VBS» vom März 2021 her, welche aufzeigt, wie das VBS sich in die übergeordnete NCS einbringt.[5]
Auch die «Nationale Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022» (SKI)[6] adressiert die Risiken bei Lieferketten und die Bedeutung von Standards im Rahmen von Massnahmen zur generellen Prüfung von Vorgaben und zur Förderung der Resilienz.
Die in diesem Bericht vorgenommene Analyse und die Erkenntnisse daraus ergänzen den bestehenden strategischen Kontext. Sie sollen dazu beitragen, die Strategien mit Bezug auf das Risikomanagement im Bereich «Supply Chain» zu ergänzen.

## 1.2 Auftrag

Der vorliegende Bericht beantwortet die am 21. Juni 2019 überwiesenen Postulate 19.3135 Dobler und 19.3136 Dobler. Die Postulate lauten wie folgt:

- **Po. 19.3135 «Haben wir die Cybersicherheit bei Beschaffungen der Armee im Griff?»**
  Der zuverlässige Betrieb der Waffensysteme und Infrastruktur der Schweizer Armee ist entscheidend für die nationale Sicherheit. Die Armee beschafft Waffen- und Infrastruktursysteme bei verschiedenen nationalen und internationalen Lieferanten. Die Verfügbarkeit, Vertraulichkeit und Integrität der cyberphysischen[7] Komponenten der Waffen- und Infrastruktursysteme werden zunehmend zur Achillesferse für die Einsatzbereitschaft und Durchhaltefähigkeit der Schweizer Bodentruppen und Luftstreitkräfte. Insbesondere die Integrität der digitalen Lieferobjekte (nichtdokumentierte Zugänge, implantierte Fehlfunktionen) bereitet Sorge.
  Der Bundesrat wird beauftragt, zu prüfen und Bericht zu erstatten über die anwendbaren nationalen und internationalen Standards (z. B. NIST Cyber Security Framework, ISO, Common Criteria, NIST 800-161, EU4, EU5, Fips) zum Vendor Risk Management und zur Produktesicherheit der technischen, insbesondere der vernetzten cyberphysischen Komponenten der Armee. Ein Fokus des Berichtes sollte auf der sicherheitsrelevanten Prüfung bei Beschaffungen liegen. Es gilt abzuklären, ob die aktuellen Vorgaben (inkl. WTO) ausreichen, um den erhöhten Sicherheitsbedürfnissen aufgrund von neuen Cyberbedrohungen gerecht zu werden. In diesem Zusammenhang stellt sich schlussendlich auch die Frage, ob die Schweizer Armee, inklusive ihrer sicherheitspolitischen Partner, unter den gegebenen Umständen (z. B. unbekannte Quellcodes bei Produkten von ausländischen Anbietern) überhaupt in der Lage ist, die Souveränität der Schweiz zu wahren.

[4] Der Schweizerische Bundesrat, Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018 – 2022 vom 18. April 2018, https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf
[5] Departement für Verteidigung, Bevölkerungsschutz und Sport, Strategie Cyber VBS; März 2021, https://www.newsd.admin.ch/newsd/message/attachments/66200.pdf
[6] Der Schweizerische Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022 vom 8. Dezember 2017 (SKI, BBl 2018 503), https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/nationalestrategie/_jcr_content/contentPar/tabs/items/downloads/tabPar/downloadlist/downloadItems/73_1460987489220.download/natstratski2018-2022_de.pdf
[7] Der Begriff "cyberphysisch" bezeichnet die Verbindung der digitalen und physischen Welt. In einem cyberphysischen System sind mechanische Komponenten über Netzwerke und moderne Informationstechnik miteinander verbunden.

Basierend auf den Analysen ist die Einschätzung des Bundesrates gefragt, ob die heutigen Massnahmen genügen, um die Risiken zu erfassen, zu messen und sie auf ein akzeptables Mass zu reduzieren.

- **Po. 19.3136 «Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?»**
  Der zuverlässige Betrieb der kritischen Infrastrukturen der Schweiz ist entscheidend für die landesweite Versorgung und Sicherheit. Die Betreiber der kritischen Infrastrukturen beschaffen ICT-Systeme und -Komponenten bei verschiedenen nationalen und internationalen Lieferanten. Somit stammen unsere digitalen Infrastrukturen und deren Subkomponenten von einer Vielzahl Lieferanten mit unterschiedlicher Herkunft.
  Die daraus resultierende Komplexität führt zu Cyberrisiken, welche die Verfügbarkeit, die Vertraulichkeit und die Integrität der landeskritischen Infrastrukturen und die Versorgungssicherheit der Schweiz gefährden. Insbesondere die Integrität digitaler Lieferobjekte (nicht dokumentierte Zugänge, implantierte Fehlfunktionen) bereitet Sorge.
  Der Bundesrat wird beauftragt, zu prüfen und Bericht zu erstatten über die anwendbaren nationalen und internationalen Standards (z. B. NIST Cyber Security Framework, ISO, Common Criteria, NIST800-161, EU4, EU5, Fips) zum Vendor Risk Management und zur Produktesicherheit von technischen, insbesondere vernetzten Systemen. Der Bericht soll weiter die Gültigkeit sowie die aktuelle Durchsetzung der Standards und deren Einhaltung für sämtliche Bereiche der landeskritischen Infrastruktur und deren notwendige Betriebsmittel der Schweiz darlegen.
  Basierend hierauf ist die Einschätzung des Bundesrates gefragt, ob die heutigen Massnahmen genügen, um die Risiken zu erfassen, zu messen und sie auf ein akzeptables Mass zu reduzieren.

Zusätzlich zur Beantwortung dieser beiden Postulate geht der Bericht auch auf Forderungen aus dem Diskussionspapier «Supply Chain Security»[8] der Kommission Cyber Security von ICTswitzerland[9] vom September 2019 ein. Die darin formulierten Forderungen nach spezifisch auf die Problematik der Lieferkette ausgerichteten Vertragsbedingungen, nach Minimalanforderungen an die Produktesicherheit und nach einem Prüfzentrum für Cybersicherheit werden als mögliche Massnahmen zur Minimierung der Risiken bei digitalen Lieferketten im Schlusskapitel des Berichts kurz diskutiert.

Nach der Einleitung in die Thematik beschreibt der Bericht in Kapitel 2 die wichtigsten Standards in den Bereichen Produktesicherheit für IKT-Produkte und deren Supply Chain Risk Management (SCRM). In Kapitel 3 wird aufgezeigt, welche Rechtsgrundlagen für die Anwendung dieser Standards in der Schweiz bestehen, wobei zwischen den Grundlagen für den Bund, die Kantone und Gemeinden und den Grundlagen für privatrechtlich organisierte Betreiber kritischer Infrastrukturen differenziert wird. Kapitel 4 beschreibt, wo und wie die Standards konkret angewendet werden. In Kapitel 5 werden schliesslich die Erkenntnisse zusammengefasst, mögliche Massnahmen zur verbesserten Anwendung der Standards zur Produktesicherheit und des SCRM bei IKT-Produkten diskutiert und ein Ausblick auf das weitere Vorgehen gegeben.

## 1.3 Begriffsklärung

Nachfolgend sollen die für das Verständnis des Berichts zentralen Begriffe kurz erläutert werden.

[8] ICTswitzerland: Supply Chain Security, Analyse & Massnahmen zur Sicherung der digitalen Lieferkette, Arbeitsgruppe Supply Chain Security der Kommission Cybersecurity, September 2019,
https://digitalswitzerland.com/wp-content/uploads/2021/08/White_Paper_Supply_Chain_Security_2019_09_25_DE.pdf
[9] Der Dachverband ICTswitzerland hat per 01.01.2021 mit Digitalswitzerland unter dem Namen Digitalswitzerland fusioniert. Die Kommission Cybersecurity wird im fusionierten Verband weitergeführt.

### 1.3.1 Normen und Standards

Im deutschen Sprachgebrauch ist betreffend dieser zwei Ausdrücke zunehmend eine Begriffsverwirrung entstanden, weshalb die Begriffe heute nahezu identisch verwendet werden. Der Grund dafür dürfte zumindest teilweise im Umstand liegen, dass die englische Sprache sowohl für *Norm* als auch für *Standard* einheitlich den Begriff *standard* verwendet.
Um mit dem Problem des unterschiedlichen Sprachgebrauchs umgehen zu können, wird in den Bereichen Technik und Naturwissenschaften der Begriff Standard als Oberbegriff verwendet.[10] Da im Bereich der IKT internationale Standards und damit einhergehend auch der englische Sprachgebrauch vorwiegende Anwendung finden, wird diese Sprachregelung im vorliegenden Bericht übernommen und grundsätzlich nur noch der Begriff *Standard* verwendet.

### 1.3.2 Kritische Infrastrukturen (KI)

In der SKI wird der Begriff KI wie folgt definiert: Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.[11]
Für die Schweiz umfasst das Spektrum der KI folgende Bereiche/Sektoren: Behörden, Energie, Entsorgung, Finanzen, Gesundheit, Information und Kommunikation, Nahrung, öffentliche Sicherheit, Verkehr.

### 1.3.3 Cyberrisiken, Cybersicherheit, Cyberdefence

Die Begriffe mit Bezug zu Cyberrisiken werden im vorliegenden Bericht entsprechend der Terminologie der Cyberrisikenverordnung des Bundes[12] verwendet. Die dort aufgeführten, massgebenden Begriffe und Bereiche sind:

- **Cyberrisiko:** Gefahr eines Ereignisses (bemessen durch das Produkt der Eintrittswahrscheinlichkeit und des Schadensausmasses), die dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann.
- **Bereich Cybersicherheit:** Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen und die internationale Zusammenarbeit zu diesem Zweck stärken.
- **Bereich Cyberdefence:** Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.

### 1.3.4 Produktesicherheit

Der Begriff «Produktesicherheit» ist von seiner Anwendung auf physische Produkte geprägt. Dabei steht die Sicherheit und Gesundheit der Nutzenden sowie Dritten bei der Anwendung der Produkte im Zentrum. Das Bundesgesetz über die Produktesicherheit (PrSG)[13] verlangt, dass die in Verkehr gebrachten Produkte grundlegende Sicherheits- und Gesundheitsanforderungen erfüllen. Die technische Konkreti-

[10] Unter dieser Voraussetzung würde ein De-jure-Standard dem deutschen Begriff der Norm entsprechen. Zur Abgrenzung liesse sich von De-facto-Standards oder Quasi-Standards sprechen, um dem deutschen Begriff Standard gerecht zu werden.
[11] Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022 vom 8. Dezember 2017 (SKI, BBl 2018 503)
[12] Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 (Cyberrisikenverordnung; CyRV; SR 120.73)
[13] Bundesgesetz über die Produktesicherheit vom 12. Juni 2009 (PrSG; SR 930.11)

sierung erfolgt durch Verweis auf technische Normen. Es wird davon ausgegangen, dass diese Anforderungen erfüllt sind, wenn die Produkte den durch spezialisierte Gremien entwickelten technischen und/oder organisatorischen Normen bzw. Standards entsprechen (Konformitätsvermutung). [14]
Die Produktesicherheit von IKT-Produkten kann hingegen eher damit umschrieben werden, dass die Anwendung der IKT-Produkte die Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit von Daten nicht gefährdet. Wie IKT-Produkte verwendet werden müssen, damit sie sicher sind, ist im Unterschied zu zahlreichen physischen Produkten deutlich schwieriger zu beurteilen. Entsprechend müssen bezüglich Sicherheit von IKT-Produkten immer auch Vorgaben zu deren Anwendung miteinbezogen werden. Die Produktesicherheit wird hier somit als Sammelbegriff verwendet, der sowohl die Sicherheit der IKT-Produkte selbst als auch deren sichere Anwendung und Einbindung in die IKT-Infrastruktur umfasst.

### 1.3.5 Supply Chain Risk Management

Das in den Postulaten angesprochene «Vendor Risk Management» ist Bestandteil des Risikomanagements der Lieferketten, das auch als «Supply Chain Risk Management» bezeichnet wird. Um den Bericht in die aktuellen Debatten zum SCRM im Umfeld der Cybersicherheit einzubetten, wird statt Vendor Risk Management der breiter gefasste Begriff des SCRM verwendet. Hinter dem Begriff stehen über Jahre entwickelte Konzepte der Unternehmens- und Organisationsführung:


- **Risikomanagement:** Das Risikomanagement bezeichnet den systematischen Prozess zur Identifikation, Analyse, Bewertung und Bewältigung von Risiken.[15]
- **Supply Chain Management (Lieferkettenmanagement):** Dieses bezeichnet den Aufbau und die Verwaltung integrierter Logistikketten (Material- und Informationsflüsse) über den gesamten Wertschöpfungsprozess, ausgehend von der Rohstoffgewinnung über die Veredelungsstufen bis hin zum Endverbraucher.[16]
- **Supply Chain Risk Management:** Das SCRM verbindet das Risikomanagement mit dem Lieferkettenmanagement. Risiken entlang der Lieferketten sollen identifiziert, analysiert, bewertet und gemindert werden.[17]
  Verwandte und ähnliche Begriffe zum SCRM sind:
  - Vendor Risk Management: Das Vendor Risk Management ist jener Teil des SCRM, der sich auf die Beurteilung der Verkäufer von IKT-Produkten und Dienstleistungen bezieht.
  - Third Party Risk Management: Auch dieser Begriff bezieht sich auf eine Teilmenge des SCRM, fokussiert aber nicht nur auf Verkäufer von IKT-Produkten und Dienstleistungen, sondern auf alle Drittparteien mit vertraglichen Beziehungen zur Organisation.

Zu den lieferantenbezogenen Risiken gehört auch, dass die Dienstleister oft ausländische, international tätige Firmen sind, die dem Rechtsrahmen ihres Mutterstaates unterstehen. Da sich in den letzten Jahren der internationale Wettbewerb um Einfluss im digitalen Raum stark verschärft hat, sind die Risiken einer direkten Einflussnahme von Staaten auf diese Lieferanten gestiegen.

[14] Dies entspricht der europäischen Gesetzgebung über die Sicherheit von Produkten: Der „New Approach“ von 1985, modernisiert und ergänzt durch den „New Legislative Framework“ in 2008 bildet den Ordnungsrahmen für die Europäische Produktregulierung. Dabei beschränkt sich die EU-Gesetzgebung bei den Vorgaben an ein Produkt auf die Festlegung der grundlegenden Anforderungen. Die Konkretisierung erfolgt durch harmonisierte Normen oder andere technische Spezifikationen (Normenverweis). Die Schweiz hat die New Approach-Richtlinien der EU weitgehend übernommen.
[15] ISO 31000:2018
[16] Gabler Wirtschaftslexikon
[17] NIST Special Publication Supply Chain Risk Management 800-161, S. 2

Schliesslich geht es aber auch um Risiken bezüglich Qualität und Verfügbarkeit der Dienstleistung selber. Nicht alle Dienstleister können in gleichem Mass die dauerhafte Aufrechterhaltung ihrer Dienstleistung garantieren. Gerade bei kleineren Dienstleistern besteht das Risiko, dass die Firma ihren Auftrag nicht erfüllen kann. Zu beachten ist auch, dass Firmen sehr stark vom Know-how einzelner Mitarbeitenden in Schlüsselpositionen abhängen können, was wiederum das Ausfallrisiko einer Dienstleistung erhöht. Nicht zuletzt ist es auch möglich, dass die Dienstleister selber Opfer von Angriffen auf die Integrität ihrer Dienstleistung werden. Dies kann für einen Angreifer eine attraktive Methode sein, um die Systeme von vielen Unternehmen mit nur einem gezielten Angriff zu kontaminieren.

# 2 Standards zur Produktesicherheit und zum SCRM bei IKT-Produkten

In der Informatik und in der Telekommunikation spielen Standards seit jeher eine entscheidende Rolle, da sie die Kompatibilität der Geräte überhaupt erst ermöglichen und die Nutzung von Geräten unterschiedlicher Hersteller stark vereinfachen. Viele dieser Standards werden direkt von grösseren Produzenten definiert und auf dem Markt durchgesetzt. Parallel dazu finden eigentliche Standardisierungsprozesse statt, wobei sich Produzenten, Anwender aber auch Behörden und internationale Organisationen gemeinsam auf Standards einigen. Solche Prozesse sind der Versuch, sich in der globalisierten und dynamischen IKT-Wirtschaft in jenen Bereichen auf Regeln zu einigen, in denen ein grosses gemeinsames Interesse und eine starke gegenseitige Abhängigkeit besteht. Die Sicherheit der eingesetzten IKT-Mittel ist ein solcher Bereich. Unsichere Geräte beeinträchtigen die Sicherheit aller anderen Geräte, die an das gemeinsame Netz angeschlossen sind. Es wurden darum schon früh Standards entwickelt, um die Sicherheit von Informatikmitteln zu beurteilen. Bereits 1983 publizierte die amerikanische Regierung den Standard TCSEC («Trusted Computer System Evaluation Criteria»), der zu weiten Teilen noch heute über den sogenannten «Common Criteria»-Standard zur Anwendung kommt. Neben diesen Standards, die auf die Sicherheit der Produkte ausgerichtet sind, wurden und werden zahlreiche Standards für Verfahren der IKT-Sicherheit entwickelt. Dies, weil ein Grossteil der Sicherheitsprobleme nicht in erster Linie aufgrund von Mängeln der eingesetzten Produkte, sondern aufgrund fehlerhafter Anwendungen oder der lückenhaften Umsetzung der Schutzmassnahmen entstehen.
Diese Entwicklungen haben dazu geführt, dass es eine breite Palette von Standards für Produkte und Verfahren der IKT-Sicherheit gibt. Es ist jedoch für die Anwender oft nicht einfach, die am besten geeigneten Standards zu kennen und künftige Entwicklungen in der Standardisierung abzuschätzen. Zudem konnten sich nur wenige Standards weltweit durchsetzen. Die erhoffte quasi-Verbindlichkeit der Sicherheitsstandards durch eine umfassende Anwendung wurde deshalb nur selten erreicht.

## 2.1 Verbindlichkeit von Standards

Standards haben keine eigene Rechtskraft, da sie von privatrechtlichen Organisationen erlassen werden, die nicht zur Rechtssetzung befugt sind. Die Anwendung von Standards ist somit freiwillig oder entspricht faktischem Druck. Bindend werden diese nur dann, wenn ihre Einhaltung in der Gesetzgebung zwingend vorgeschrieben wird oder wenn sie Gegenstand von Verträgen zwischen Parteien sind. Standards dienen auch der Konkretisierung ansonsten unbestimmter Rechtsbegriffe, z. B. des Begriffes *Stand der Technik* und können so trotz der fehlenden Verbindlichkeit unmittelbar zur Rechtssicherheit beitragen. Sie gelten in vielen Fällen als eindeutige und anerkannte Regeln der Technik, und die Einhaltung dieser Regeln stellt einen wichtigen Schritt beim Nachweis ordnungsgemässen Verhaltens dar.

## 2.2 Standards zur Produktesicherheit

Nachfolgende, nicht abschliessende Auflistung enthält einige der am häufigsten angewendeten Standards im Bereich Cybersicherheit – jeweils mit Angabe der Herausgeberorganisation sowie einer Beschreibung der wichtigsten Anwendungsmerkmale:

| **Bezeichnung** | **Anwendung** |
|---|---|
| NIST Cybersecurity Framework<br>*(National Institute of Standards and Technology, U.S. Department of Commerce)* | Genereller Cybersicherheits-Standard, der alle Arten von Cyberrisiken generisch adressiert. |
| ISO/IEC 2700x<br>*(International Organization for Standardization / International Electrotechnical Commission)* | Die International Organization for Standardization (ISO) veröffentlicht verschiedene sich gegenseitig ergänzende Standards zur Informatiksicherheit, die als «2700x-Familie» bezeichnet werden. Der bekannteste davon ist der Standard ISO 27001. Er spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS) unter Berücksichtigung des Kontexts einer Organisation. |
| COBIT<br>*(ISACA; Information Systems Audit and Control Association)* | COBIT (Control Objectives for Information and Related Technology) ist ein international anerkanntes Framework für die Governance und das Management der Unternehmens-IT. COBIT wurde von der Non-Profit-Organisation ISACA erstellt und von Experten entwickelt, um den Anforderungen von Geschäftsführern und IKT-Experten gerecht zu werden. Das Framework kombiniert Enterprise-Governance und Management-Techniken und bietet Prinzipien, Praktiken, Modelle und Analysewerkzeuge, die den Anwendern helfen, den Wert ihrer IKT-Systeme und das Vertrauen in diese konsequent zu steigern. |
| Common Criteria (CC)<br>*Vollbezeichnung: Common Criteria for Information Technology Security Evaluation*<br>*(Common Criteria Implementation Board)* | Common Criteria ist ein internationaler Standard, der allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologien spezifiziert und mit dessen Hilfe sich die Sicherheit von Software- und Hardware-Produkten nach allgemeinen Kriterien bewerten und prüfen lässt. Die CC entstanden in internationaler Zusammenarbeit und vereinheitlichten vorher unterschiedliche nationale Standards (Kanada CTCPE, Europa ITSEC, USA TCSEC) zu einer gemeinsamen Grundlage für die Bewertung der Datensicherheit. Mit der Verabschiedung der Norm ISO/IEC 15408 wurden die CC 1999 zu einem allgemeinen und weltweit anerkannten Standard.<br>Die Common Criteria beschreiben verschiedene funktionale Sicherheitsanforderungen, um damit die vorher festgelegten Sicherheitsziele zu erreichen. Gleichzeitig definieren sie Anforderungen an die Prüfung, die dafür sorgen, Vertrauen in die Sicherheit des Produkts zu erlangen. Ein weiteres Ziel der CC-Zertifizierung ist die Einbindung dieser Anforderungen in internationale Abkommen. Dadurch entfällt die Notwendigkeit, IKT-Produkte nach unterschiedlichen, nationalen Massstäben mehrfach zertifizieren zu müssen. |

| | |
|---|---|
| BSI Standards<br>*(Deutsches Bundesamt für Sicherheit in der Informationstechnik – BSI)* | Die BSI-Standards 200-1, 200-2 und 200-3 sind elementare Bestandteile der IKT-Grundschutz-Methodik des BSI. Inhalte der BSI-Standards sind Massnahmen, Vorgehensweisen und Empfehlungen zu Verfahren, Methoden und Prozessen rund um verschiedene Aspekte der Informationssicherheit in Unternehmen und Behörden. Ziel der Standards ist es, durch die schrittweise Einführung und Umsetzung eines ISMS Geschäftsprozesse sicherer zu gestalten und Daten zu schützen. Die Inhalte sind vollständig kompatibel zum ISO-Standard ISO/IEC 27001 und berücksichtigen die Empfehlungen aus dem ISO-Standard ISO/IEC 27002. Auch die Begrifflichkeiten ähneln den ISO-Standards. |
| Federal Information Processing Standards (FIPS)<br>*(National Institute of Standards and Technology, U.S. Department of Commerce)* | FIPS sind öffentlich bekanntgegebene minimale Standards der US Regierung, die für die Verwendung in Computersystemen von nicht-militärischen amerikanischen Regierungsbehörden und Regierungsauftragnehmern entwickelt wurden. Diese Minimalstandards decken Anforderungen unterschiedlicher Anwendungsbereiche ab. Sie werden solange angewendet, bis geeignete Industriestandards existieren. IKT-Produzenten wenden FIPS auf freiwilliger Basis auch ausserhalb von Regierungsgeschäften an. Viele FIPS-Spezifikationen beruhen auf der Modifizierung von allgemein verwendeten Standards (z. B. ANSI, IEEE, ISO). |
| ENISA Guidelines<br>*(European Union Agency for Cybersecurity (ENISA); früher: European Network and Information Security Agency)* | Die ENISA hat eine Reihe verschiedener Richtlinien im Bereich der Netzwerk- und Informationssicherheit veröffentlicht, wie z.B.:<br>- National Cyber Security Strategy (NCSS) Good Practice Guide<br>- Good Practice Guide on Incident Reporting<br>- Technical Guideline on Security Measures |
| Minimalstandard zur Verbesserung der IKT-Resilienz (IKT-Minimalstandard)<br>*(Bundesamt für wirtschaftliche Landesversorgung BWL)* | Genereller Cybersicherheitsstandard, der alle Arten von Cyberrisiken generisch adressiert (basiert auf dem NIST Cybersecurity Framework; siehe oben) |

## 2.3 Standards zum SCRM

Im Bereich des SCRM mit Bezug zur Cybersicherheit sind deutlich weniger etablierte Standards vorhanden. Einige der Standards zur IKT-Sicherheit weisen auch auf die Wichtigkeit des SCRM hin, machen aber nur wenige konkrete Vorgaben. Verbindlichen Regeln für die Anwendung von Standards werden daher nur für Teilaspekte des SCRM erlassen. Beispiele dafür sind vorgeschriebene Prüfungen und Zertifizierungen von Produkten bei der Beschaffung.[18]

[18] In der Schweiz müssen beispielsweise intelligente Messsysteme (Smartmeters) gestützt auf die Stromversorgungsverordnung (StromVV) auf ihre Datensicherheit überprüft werden. Diese werden durch das eidgenössische Institut für Metrologie zertifiziert.

In Bezug auf SCRM sind folgende Standards von besonderer Bedeutung:

| **Bezeichnung** | **Anwendung** |
|---|---|
| NIST Special Publication 800-161 «Supply Chain Risk Management Practices for Federal Information Systems and Organizations»<br>*(National Institute of Standards and Technology, U.S. Department of Commerce)* | Entwicklung und Implementierung von Strategien, Massnahmen und Kontrollen zum Management von Supply-Chain-Risiken.<br>Diese Publikation bietet Bundesbehörden eine Anleitung zur Identifizierung, Bewertung und Minderung von IKT-Supply-Chain-Risiken auf allen Ebenen ihrer Organisation. |
| ISO/IEC 27001 – Annex A.15: Supplier Relationships | In Anhang A.15.1 geht es um die Informationssicherheit in Lieferantenbeziehungen. Das Ziel ist der Schutz der wertvollen Vermögenswerte der Organisation, die für Lieferanten zugänglich sind oder von ihnen beeinflusst werden. |
| ISO/IEC 90003 | Die ISO/IEC 90003 ist eine Richtlinie zur Anwendung der ISO 9001 (Anforderungen an Qualitätsmanagementsysteme) im Rahmen von Beschaffung, Entwicklung, Betrieb und Wartung in der Softwareentwicklung zwischen Lieferant, Auftragnehmer und Kunde. |
| Standardized Information Gathering (Questionnaire) SIG<br>*(The Santa Fe Group / Shared Assessments)* | Standardisierter Fragebogen, um die Qualität der Lieferantenbeziehung zu beurteilen und Lieferrisiken zu bewerten, der hauptsächlich im angelsächsischen Raum angewendet wird.<br>Der SIG ist eine Sammlung von Fragen zur Informationssicherheit und zum Datenschutz von Dritten, die sich auf mehrere Vorschriften und Kontrollrahmen bezieht. Der SIG wird von einer Non-Profit-Organisation namens Shared Assessments herausgegeben. Diese aktualisiert den SIG-Fragebogen jährlich und berücksichtigt dabei neue Sicherheits- und Datenschutzherausforderungen, Änderungen der Vorschriften sowie die neuesten Trends und Best Practices im Risikomanagement für Drittanbieter. |

Neben diesen häufigsten, international etablierten Standards existieren zahlreiche weitere Standards, Leitfäden und Richtlinien, die zur Verbesserung der Informationssicherheit im Allgemeinen und zur Verbesserung des Lieferantenmanagements im Speziellen geeignet sind. Beispiele dafür sind Empfehlungen von Branchenverbänden oder auch Forschungsarbeiten von Universitäten und IKT-Sicherheits-Firmen. Solche Standards umfassen unter anderem Themenbereiche wie Verschlüsselung, digitale Signaturen, Hash-Funktionen, Authentifizierung, Kommunikationsnachweise, Zeitstempeldienste, Brandschutz, Einbruchshemmung, sicheres Löschen von Datenträgern, usw.

# 3 Rechtsrahmen für die Anwendung der Standards

Die rechtlichen Grundlagen sind die Basis für Massnahmen zur Erhöhung der Produktesicherheit und für Massnahmen zur Minimierung der Risiken der Lieferantenkette. Sie enthalten üblicherweise keinen direkten Verweis auf Standards, bilden jedoch die Grundlage für deren Anwendung.
Bei Beschaffungen bewegt sich der Staat gleichzeitig in zwei völlig unterschiedlichen Rechtssphären. Um seine öffentlichen und damit gesetzlichen Aufgaben zu erfüllen, ist er, soweit er sie nicht mit eigenen

Mitteln bewerkstelligen kann, regelmässig auf einen Leistungsbezug aus der Privatwirtschaft angewiesen. Dabei beschreibt das Beschaffungsrecht das Verfahren, in welchem die behördliche Willensbildung zu erfolgen hat. Ist dieser Wille – unter Berücksichtigung aller Auflagen, inklusive der erforderlichen Sicherheitsauflagen – gebildet, wird im Vergabeverfahren die geeignete Anbieterin gewählt. Welche Leistungen mit welchen Eigenschaften der Staat zur Aufgabenerfüllung benötigt, beschreibt er in den Ausschreibungsunterlagen. Eine direkte Anwendung der geltenden Verwaltungsvorschriften findet dabei nicht statt. Vielmehr muss sich die Behörde die Einhaltung der Vorschriften vertraglich zusichern lassen. In der Folge lassen sich Verletzungen solcher Vereinbarungen auch nur mit privatrechtlichen Mitteln ahnden, namentlich durch Schadenersatz. Dies gilt sowohl für die Bundesverwaltung selbst (und damit auch für Beschaffungen zu Gunsten der Armee[19]) als auch für kritische Infrastrukturen des öffentlichen und des privaten Rechts, soweit sie Tätigkeiten in definierten Sektoren gemäss BöB Art. 4 Abs. 2 in der Schweiz ausüben.
Beim Leistungsbezug am Markt ist daher der Beschaffungsvertrag, der primär den Vertragsgegenstand bzw. die zu erbringende Leistung beschreibt, das zentrale Element zur jeweiligen Durchsetzung der Sicherheitsaspekte. Die Einhaltung internationaler Standards oder Anforderungen zur Sicherstellung eines gewissen Schutzniveaus mittels Musskriterien (Eignungskriterien und technische Spezifikationen) resp. bewerteten Kriterien (Zuschlagskriterien) können dazu bereits im Rahmen der Ausschreibung definiert, anschliessend im Vertrag vereinbart und anlässlich der Leistungserbringung nachgeprüft werden. Im Bereich SCRM steht die Beziehung zwischen Auftraggeber/Besteller/Kunde/Käufer und dem Auftragnehmer/Produzenten/Lieferanten im Fokus des Interesses. Auch diese Beziehung wird in der Regel im Vertrag beschrieben und definiert.

## 3.1 Rechtliche Grundlagen für die Anwendung von Standards in der Bundesverwaltung

Die Möglichkeiten und Verfahren zur Anwendung von Standards zur Produktesicherheit und zum SCRM sind in mehreren Bundesgesetzen und Verordnungen geregelt. Spezifisch für den Bereich der Sicherheit von IKT-Produkten und den Informationen, die durch solche Produkte bearbeitet werden, bestanden bis vor Kurzem keine übergeordneten bundesgesetzlichen Vorgaben. Mit dem neuen Informationssicherheitsgesetz (ISG) wurde diese Lücke adressiert.

### 3.1.1 Das Informationssicherheitsgesetz (ISG)[20]

Das Parlament hat am 18. Dezember 2020 das Bundesgesetz über die Informationssicherheit beim Bund (ISG) verabschiedet.[21] Das ISG führt die wichtigsten Regelungsaspekte der Informations- und Cybersicherheit in einem einzigen Gesetz zusammen. Es beinhaltet sowohl Vorschriften zur Produktesicherheit als auch zum SCRM bei IKT-Produkten, so insbesondere über das Risikomanagement, die Klassifizierung von Informationen, die Informatiksicherheit, die Personensicherheitsprüfungen, den physischen Schutz, die Sicherheit bei sensitiven Beschaffungen durch das Betriebssicherheitsverfahren sowie auch über die Unterstützung der Betreiber kritischer Infrastrukturen im Bereich der Informationssicherheit durch den Bund. Das ISG gilt für die Behörden und Organisationen des Bundes (einschliesslich der Armee) und legt die minimalen Anforderungen fest, welche diese zum Schutz ihrer Informationen und Informatikinfrastrukturen erfüllen müssen. Das Gesetz verpflichtet aber auch kantonale Behörden und privatrechtliche Unternehmen, die den Bund bei der Wahrnehmung seiner Aufgaben unterstützen und dabei klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen. Der Bund sucht damit die enge Zusammenarbeit mit den Kantonen und der Privatwirtschaft, um den aktuellen, ständig zunehmenden Cybergefahren zu begegnen.

[19] Die Armee selber kann nicht beschaffen, da sie nicht Bestandteil der Bundesverwaltung (gemäss RVOV), sondern eine spezialgesetzliche Institution gestützt auf das Militärgesetz ist. Ihre Selbstverwaltung ist nur im Rahmen der Verordnung über die Verwaltung der Armee (VVA; SR 510.301) möglich.
[20] Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz; ISG; BBl 2020 9975)
[21] Das ISG ist noch nicht in Kraft. Die spezifischen Ausführungsverordnungen werden derzeit erarbeitet.

Das ISG basiert auf international anerkannten Standards, insbesondere ISO/IEC 27001 und ISO/IEC 27002. Um die Informationssicherheit beim Bund nachhaltig und wirtschaftlich zu verbessern und um ein möglichst einheitliches Sicherheitsniveau zwischen den Bundesbehörden und weiteren Stellen zu erreichen, legt es den Fokus auf die kritischen Informationen und Systeme sowie auf die Standardisierung der Massnahmen. Nicht zuletzt aufgrund der raschen technologischen Entwicklungen legt das ISG aber keine detaillierten Massnahmen fest, sondern schafft lediglich einen formell-gesetzlichen Rahmen, auf dessen Grundlage die Bundesbehörden auf Verordnungs- und Weisungsebene die Informationssicherheit möglichst einheitlich konkretisieren können.
Dass der Bund die verschiedenen Aspekte der Informationssicherheit in einem Bundesgesetz vereint, zeigt, dass er diesem Thema eine grosse Bedeutung zumisst.

### 3.1.2 Standards der IKT-Produktesicherheit

Die Basis für die Umsetzung von Standards in Bezug auf die Produktesicherheit (inklusive Vorgaben zur sicheren Anwendung der Produkte) in der Bundesverwaltung ist in der Cyberrisikenverordnung, in der Informationsschutzverordnung sowie im Datenschutzgesetz und der Datenschutzverordnung festgehalten.

**Cyberrisikenverordnung (CyRV)**[22]**:** Vorgaben zur Informatiksicherheit und zur sicheren Anwendung von IKT-Mitteln in der Bundesverwaltung werden in der CyRV definiert. Die CyRV regelt die Kompetenz der oder des Delegierten für Cybersicherheit, Informatiksicherheitsvorgaben für die Verwaltungseinheiten der Bundesverwaltung zu erlassen (Art. 11 Abs. 1 Bst. e). Sie oder er kann sich zudem an der Erarbeitung der übrigen Informatikvorgaben und -vorhaben mit Bezug zur Cybersicherheit beteiligen (Art. 11 Abs. 3). Weiter verpflichtet die CyRV zur Durchführung von definierten abgestuften Sicherheitsverfahren (Art. 14b ff; siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**), die über die Informatiksicherheitsvorgaben der oder des Delegierten ergänzt und erweitert werden können. Diese Sicherheitsverfahren bilden die Grundlage für eine sichere Abwicklung aller durch die Informatik unterstützten Geschäftsprozesse und stellen sicher, dass die richtigen Stellen zum richtigen Zeitpunkt involviert werden. Dies wird entlang des gesamten Lebenswegs von IKT-Systemen, das heisst ab Beginn eines neuen Projekts über den Life Cycle bis zur Ausserdienststellung, angewendet. Damit wird sichergestellt, dass alle ihre Verantwortung in den verschiedenen Phasen richtig wahrnehmen können.

**Informationsschutzverordnung (ISchV)**[23]**:** Die ISchV regelt den Schutz von Informationen des Bundes und der Armee, soweit er im Interesse des Landes geboten ist. Sie legt insbesondere die Klassifizierung (Art. 4 ff) und die daraus resultierenden Formen der Bearbeitung dieser Informationen (Art. 13 ff) fest. Im Anhang zur ISchV hat der Bundesrat technische Anforderungen an die Produktesicherheit von IKT-Systemen festgelegt, die zur Bearbeitung klassifizierter Informationen vorgesehen sind. Die ISchV wird mit dem Inkrafttreten des ISG aufgehoben. Soweit die notwendigen Inhalte nicht bereits im Gesetz enthalten sind, werden sie in eine neue Informationssicherheitsverordnung überführt.

**Bundesgesetz über den Datenschutz und Verordnung (DSG und VDSG)**[24]**:** Das Bundesgesetz über den Datenschutz (DSG) und die Verordnung dazu definieren, welche technischen und organisatorischen Anforderungen bei der Bearbeitung von Personendaten gelten (Art. 7, 11 und 17a DSG, Art. 8-11, 20 und 21 VDSG). Dadurch definieren sie Mindeststandards an die Sicherheit derjenigen IKT-Produkte, welche für die Bearbeitung solcher Daten eingesetzt werden.

[22] Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung; CyRV; SR 120.73)
[23] Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung; ISchV; SR 510.411)
[24] Bundesgesetz über den Datenschutz (Datenschutzgesetz; DSG; SR 235.1) und Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11).

### 3.1.3 Standards für das SCRM

Für die Anwendung von Standards im Bereich SCRM gilt es zunächst festzustellen, welche rechtlichen Möglichkeiten bei der Ausgestaltung von Beschaffungsprozessen bestehen. Die Grundlagen dafür sind im Beschaffungsrecht festgehalten. Darüber hinaus werden in der Geheimschutzverordnung und in der Verordnung über Personensicherheitsprüfungen wichtige Voraussetzungen geschaffen, um Anbieter von besonders sicherheitsrelevanten Dienstleistungen und Produkten genauer zu prüfen.

**Beschaffungsrecht – Abkommen im Rahmen der Welthandelsorganisation (WTO) und Bundesgesetz über das öffentliche Beschaffungswesen (BöB)[25]:** Mit ihrem Beitritt zur Welthandelsorganisation (WTO) hat sich die Schweiz verpflichtet, in ihrer Rechtsordnung den internationalen Handel zu liberalisieren und allfällige Handelshemmnisse abzubauen. Das internationale Recht anerkennt aber, dass die Staaten zum Schutz überwiegender Sicherheitsinteressen Ausnahmen vom Grundsatz des freien Handels benötigen. So sehen sowohl das Abkommen vom 15. April 1994 zur Errichtung der Welthandelsorganisation[26] als auch das revidierte Übereinkommen über das öffentliche Beschaffungswesen[27] vor, dass die Signatarstaaten Massnahmen treffen können, die zum Schutz ihrer wesentlichen Sicherheitsinteressen notwendig sind. Weiter können Auskünfte verweigert werden, wenn deren Offenlegung diesen Sicherheitsinteressen zuwiderlaufen würde. Das betrifft insbesondere die Beschaffung von Waffen, Munition und Kriegsmaterial sowie Beschaffungen, die für die nationale Sicherheit oder die Landesverteidigung unerlässlich sind. Für Verträge im Bereich der nationalen Sicherheit und der Landesverteidigung dürfen die Vertragsparteien also von der Anwendung der Kerngebote des internationalen Beschaffungsrechts sowie insbesondere von den Prinzipen der Inländerbehandlung und der Nichtdiskriminierung absehen.[28]

Der Gesetzgeber hat zum Schutz wesentlicher nationaler Sicherheitsinteressen vom Vorbehalt des revidierten Übereinkommens über das öffentliche Beschaffungswesen Gebrauch gemacht. So hat er in Artikel 10 Absatz 4 Buchstabe a BöB festgelegt, dass dieses Gesetz auf die Vergabe von öffentlichen Aufträgen keine Anwendung findet, wenn dies für den Schutz und die Aufrechterhaltung der äusseren oder inneren Sicherheit oder der öffentlichen Ordnung als erforderlich erachtet wird. Diese Ausnahme ist für alle dem BöB unterworfenen Auftraggeber, also nicht nur der zentralen Bundesverwaltung, stets im Rahmen ihrer Ermessensausübung (vgl. oben Ziffer 3) anzuwenden. Allerdings darf diese Abweichung zu den Grundsätzen des Freihandels nur unter den Bedingungen des Abkommens in Anspruch genommen werden: Die Beschaffungsstelle muss belegen können, dass es nicht möglich ist, das Risiko mit verhältnismässigen, nichtdiskriminierenden Massnahmen auf ein tragbares Mass zu reduzieren. Dabei gelten die verfassungsrechtlichen Massstäbe auch weiterhin. Insbesondere sind diese Entscheide willkürfrei und begründet zu fällen.

**Geheimschutzverordnung[29]:** In der Geheimschutzverordnung vom 29. August 1990 werden die Sicherheitsmassnahmen festgehalten, die zur Anwendung kommen, wenn Aufträge mit militärisch klassifizierten Inhalten der Stufen VERTRAULICH und GEHEIM durch Dritte ausgeführt werden sollen. Sie bildet die rechtliche Grundlage für die Durchführung von Betriebssicherheitsprüfungen für Auftragnehmer des Bundes und damit für ein zentrales Element des SCRM. Das sogenannte Betriebssicherheitsverfahren wird im ISG nunmehr auf eine formell-gesetzliche Grundlage gestellt.

**Verordnung über die Personensicherheitsprüfungen (PSPV)[30]:** Basierend auf den Artikeln 19-21 des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)[31] und den Artikeln 23 Abs. 2, Bst. d, 103 Abs. 3 Bst. d und 113 Abs. 4 Bst. d des Bundesgesetzes über die Arme und die Militärverwaltung (MG)[32] regelt die Verordnung vom 4. März 2011 über die Per-

[25] Bundesgesetz über das öffentliche Beschaffungswesen (BöB; SR 172.056.1)
[26] Abkommen zur Errichtung der Welthandelsorganisation (SR 0.632.20)
[27] Revidiertes Übereinkommen über das öffentliche Beschaffungswesen (SR 0.632.231.422)
[28] Vgl. Art. III des revidierten Übereinkommens über das öffentliche Beschaffungswesen (SR 0.632.231.422)
[29] Verordnung über das Geheimschutzverfahren bei Aufträgen mit militärisch klassifiziertem Inhalt (Geheimschutzverordnung; SR 510.413)
[30] Verordnung über die Personensicherheitsprüfungen (PSPV; SR 120.4)
[31] Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120)
[32] Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz; MG; SR 510.10)

sonensicherheitsprüfungen die Voraussetzung für die Durchführung von Personensicherheitsprüfungen. Diese Grundlage ist zentral für das Risikomanagement mit Bezug auf die Mitarbeitenden von Drittanbietern. Mit dem Inkrafttreten des ISG wird diese Verordnung auf eine neue formell-gesetzliche Grundlage gestellt und total revidiert.

## 3.2 Rechtliche Grundlagen für die Anwendung von Standards bei kritischen Infrastrukturen

In der Schweiz gibt es kein Gesetz, das über alle Sektoren der kritischen Infrastrukturen Vorgaben in Bezug auf die Sicherheit oder die Beschaffung von IKT-Mitteln erlässt.[33] Solche Vorgaben werden, wo vorhanden, in erster Linie in den sektorspezifischen Erlassen gemacht. Weil diese Erlasse in ihrem jeweiligen regulativen Kontext stehen, unterscheiden sie sich auch bezüglich der Vorgaben der Sicherheit stark. Generell lässt sich feststellen, dass für Betreiber und Betreiberinnen kritischer Infrastrukturen wenig verbindliche Vorgaben in Bezug auf die Anwendung von Standards zur Produktesicherheit oder zum SCRM gemacht werden. Verschiedene Erlasse verweisen indirekt auf Standards, indem sie von Betreibern kritischer Infrastrukturen verlangen, dass sie Massnahmen zur Sicherheit entsprechend dem «Stand der Technik» ergreifen.[34] Solche indirekten Verweise sind in Bezug auf die IKT-Sicherheit vergleichsweise schwierig interpretierbar, da sich nur schwer feststellen lässt, welches der aktuelle Stand der Technik sein soll. Es bleibt unklar, inwiefern die internationalen Standards umgesetzt werden müssen, damit dieses Kriterium als erfüllt gilt.
Die folgende Tabelle listet diejenigen rechtlichen Grundlagen auf, die direkte Vorgaben zu Fragen der Sicherheit machen. Zudem zeigt sie auf, aus welchen dieser Grundlagen sich eine verpflichtende Anwendung von Standards zur sicheren Verwendung von IKT-Produkten und deren Beschaffung ergibt.

| Sektoren | Vorgaben |
|---|---|
| Behörden und öffentliche Sicherheit | Für die Bundesverwaltung gelten die in Kapitel 3.1. aufgeführten Grundlagen. |
| Energie | • Die Stromversorgungsverordnung[35] (Art. 8b) definiert eine Prüfung der intelligenten Messsysteme (Smartmeter) hinsichtlich deren Datensicherheit durch das Eidgenössische Institut für Metrologie. Das Stromversorgungsgesetz[36] (Art. 20a) verlangt eine periodische Personensicherheitsüberprüfung für Mitarbeitende und beauftragte Personen der nationalen Netzbetreibergesellschaft, welche die Sicherheit des Übertragungsnetzes beeinflussen können.<br>• Die Starkstromverordnung[37] (Art. 4) und die Schwachstromverordnung[38] (Art. 4) verweisen zur Sicherheit der Anlagen direkt auf die geltenden internationalen und schweizerischen Normen und erklären diese als verbindlich.<br>• Das Kernenergiegesetz[39] und die Kernenergieverordnung[40] enthalten diverse Vorgaben für die Sicherheit beim Betrieb von Kernenergieanlagen. Die Verordnung über die Personensicherheitsprüfungen im Bereich Kernanlagen[41] hält fest, dass alle Personen, welche |

[33] Das neue Informationssicherheitsgesetz (vgl. Kapitel 3.1) enthält Regelungen, die auch für die Betreiber kritischer Infrastrukturen gültig sind.
[34] z.B. Art. 3 der Verordnung über den Schutz vor Störfällen (Störfallverordnung; StFV; SR 814.012); Art. 3 des Bundesgesetzes über die Produktesicherheit (PrSG; SR 930.11). Besonders prominent diskutiert wird der Verweis auf den Stand der Technik in Bezug auf die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union (EU).
[35] Stromversorgungsordnung (StromVV; SR 734.71)
[36] Bundesgesetz über die Stromversorgung (Stromversorgungsgesetz; StromVG; SR 734.7)
[37] Verordnung über elektrische Starkstromanlagen (Starkstromverordnung; SR 734.2)
[38] Verordnung über elektrische Schwachstromanlagen (Schwachstromverordnung; SR 734.1)
[39] Kernenergiegesetz (KEG; SR 732.1)
[40] Kernenergieverordnung (KEV; SR 732.11)
[41] Verordnung über die Personensicherheitsprüfungen im Bereich Kernanlagen (PSPVK; SR 732.143.3)

| | |
|---|---|
| | Zugang zu klassifizierten Informationen über sicherungs- oder sicherheitsrelevante Systeme von Kernanlagen und Kernmaterialien haben, einer Personensicherheitsüberprüfung unterzogen werden müssen (Art. 1).<br>• Gemäss Stauanlagengesetz[42] (Art. 2) sind Stauanlagen so zu bemessen, zu bauen und zu betreiben, dass ihre Standsicherheit bei allen voraussehbaren Betriebs- und Lastfällen gewährleistet ist. |
| Entsorgung | • Die Störfallverordnung[43] (Art. 3) schreibt bestimmten Betrieben vor, Sicherheitsmassnahmen auf dem Stand der Technik umzusetzen, die betriebliche und umgebungsbedingte Störfälle und das Eindringen Unbefugter berücksichtigen. Ein expliziter Bezug auf IKT-Sicherheit und entsprechende Standards wird jedoch in der Verordnung nicht hergestellt. |
| Finanzen | • Das Bundesgesetz über die Eidgenössische Finanzmarktaufsicht[44] erteilt der Eidgenössischen Finanzmarktaufsicht (FINMA) die Kompetenz, Ausführungsbestimmungen zur Sicherheit und zum Schutz von Daten zu erlassen (Art. 13a Abs. 3). Die Verordnung zum Finanzmarktaufsichtsgesetz[45] legt fest, wie die FINMA diese Kompetenz wahrnimmt und dass sie dabei internationale Standards zu berücksichtigen hat (Art. 5 und Art. 6).<br>• Die FINMA Rundschreiben[46] 2017/01 «Corporate Governance – Banken»[47], 2008/07 «Outsourcing Banken»[48] und 2008/21 «Operationelle Risiken Banken»[49] verpflichten die Banken zur Umsetzung von Standards, die den Vorgaben des NIST-Standards entsprechen. |
| Gesundheit | • Die Verordnung über das elektronische Patientendossier (EPDV)[50] schreibt vor, dass Gemeinschaften ein Datenschutz- und Datensicherheitsmanagementsystem betreiben müssen (Art. 12). Weiter verweist die EPDV bezüglich Vorgaben zur Sicherheit von Identifikationsmitteln direkt auf die ISO/IEC Norm 29115:2013 (Art. 23). Geregelt sind ferner die Akkreditierung von Zertifizierungsstellen (Art. 28) sowie die Anforderungen, Voraussetzungen und Verfahren der Zertifizierung (Art. 30-38). |
| Information und Kommunikation | • Das Fernmeldegesetz (FMG)[51] (Art. 48a) gibt dem Bundesrat die Kompetenz, den Anbietern technische und administrative Vorschriften zur Sicherheit der Fernmeldeinfrastrukturen zu erlassen. |
| Nahrung | • Keine Sicherheitsanforderungen an Informatik oder Zulieferer in Verordnungen gefunden. |
| Verkehr | • Keine Sicherheitsanforderungen an Informatik oder Zulieferer in Verordnungen gefunden.<br>• Die Störfallverordnung schliesst teilweise auch Verkehrswege mit ein. |

# 4 Anwendung der Standards

Da die bestehenden Standards die möglichen technischen und organisatorischen Massnahmen zur Cybersicherheit weitgehend abdecken, lässt sich ein Grossteil der technischen und organisatorischen Massnahmen zum Schutz vor Cyberrisiken auf die Anwendung von Standards zurückführen. In diesem Kapitel werden die wichtigsten Massnahmen der Bundesverwaltung und der Betreiber von kritischen

[42] Bundesgesetz über die Stauanlagen (Stauanlagengesetz; StAG; SR 721.101)
[43] Verordnung über den Schutz vor Störfällen (Störfallverordnung; StFV; SR 814.012)
[44] Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtgesetz; FINMAG; SR 956.1)
[45] Verordnung zum Finanzmarktaufsichtgesetz (SR 956.11)
[46] Mit Rundschreiben führt die FINMA aus, wie sie die Finanzmarktgesetzgebung in der Aufsichtspraxis anwendet. Die Rundschreiben sind unter folgendem Link abrufbar: https://finma.ch/de/dokumentation/rundschreiben/
[47] Unter folgendem Link abrufbar: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-01-20200101.pdf?la=de
[48] Unter folgendem Link abrufbar: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-07.pdf?la=de
[49] Unter folgendem Link abrufbar: https://finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=de
[50] Verordnung über das elektronische Patientendossier (EPDV; SR 816.11)
[51] Fernmeldegesetz (FMG; SR 784.10)

Infrastrukturen aufgezeigt, die eine direkte Anwendung von Vorgaben aus den Standards zur Produktesicherheit und zum SCRM von IKT-Produkten darstellen.

## 4.1 Anwendung von Standards in der Bundesverwaltung

Die Sicherheit der IKT-Produkte hat für die Bundesverwaltung und die Armee höchste Priorität. Die bestehenden Vorgaben bezüglich Produktesicherheit und SCRM werden laufend angepasst. Sie orientieren sich stark an international gültigen Standards, aber ein direkter Verweis auf die zu berücksichtigenden Standards bleibt die Ausnahme.[52]

### 4.1.1 Anwendung von Standards zur Sicherheit von IKT-Produkten

Im Rahmen der geltenden Vorgaben ist die Umsetzung der wichtigsten Massnahmen zur IKT-Sicherheit während des gesamten Lebenswegs eines IKT-Systems (Planung, Beschaffung, Betrieb, Ausserdienststellung) von entscheidender Bedeutung für die Qualität der Cybersicherheit. In der Bundesverwaltung erhebt das Nationale Zentrum für Cybersicherheit (NCSC) deshalb jährlich den Stand der Umsetzung und bringt diesen dem Bundesrat zur Kenntnis. Eine Zusammenfassung dieser Erhebungen ist öffentlich[53]. In der Folge wird aufgezeigt, welche Rolle die Standards für IKT-Produktesicherheit bei der Umsetzung der Massnahmen spielen.

**Die Sicherheitsverfahren der Bundesverwaltung**
Die in der CyRV definierten Sicherheitsverfahren bestehen aus folgenden aufeinander abgestuften Elementen:

- Schutzbedarfsanalyse: Bei jedem Informatikvorhaben ist vorab eine Schutzbedarfsanalyse durchzuführen. Das Resultat der Schutzbedarfsanalyse ist eine Einstufungsbeurteilung der Anwendung oder des Projektes. Alle Informatikschutzobjekte müssen über eine aktuelle Schutzbedarfsanalyse verfügen. Teil der Schutzbedarfsanalyse ist auch der Prozess zur Reduktion von nachrichtendienstlicher Ausspähung (RINA). Dieser Prüfprozess wurde erarbeitet, um den Schutzbedarf einer Informatikleistungserstellung mit Blick auf die Bedrohung durch instrumentalisierte Informatikanbieter zu erkennen, allfällige Schutzmassnahmen zu treffen und diese mit einem möglichen Beschaffungsverfahren zu koordinieren. Weiter werden Risiken identifiziert und Massnahmen festgelegt, die in das Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) eingebunden werden müssen.
- Vorgaben für den Grundschutz: Der «IKT-Grundschutz in der Bundesverwaltung» legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Für jedes Informatikschutzobjekt ist mindestens dieser IKT-Grundschutz umzusetzen. Die Umsetzung ist durch die verantwortlichen Verwaltungseinheiten zu dokumentieren und regelmässig zu überprüfen.
- Vorgaben für den erhöhten Schutz: Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so definieren die Verwaltungseinheiten, zusätzlich zur Umsetzung der Sicherheitsvorgaben für den Grundschutz und basierend auf einer Risikoanalyse, weitere Sicherheitsmassahmen, dokumentieren diese und setzen sie um. Das Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) beinhaltet die Beschreibung dieser zusätzlichen Sicherheitsmassnahmen und ihrer Umsetzung für das Informatikschutzobjekt sowie der Restrisiken.

[52] Die Weisungen über die Informationssicherheit im VBS (WIns VBS) vom 16. Dezember 2016 sowie die Weisungen der Informationssicherheitsverantwortlichen VBS über die Informationssicherheit (WSVIns VBS) vom 26. April 2017 enthalten verbindliche Regeln für das ISMS auf Stufe VBS sowie für das ISMS der Gruppen und Ämter des VBS. Es wird explizit festgehalten, dass das ISMS VBS auf dem Standard SN ISO/IEC 27001:2015 basiert.
[53] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/informatiksicherheitsberichte-bund.html

Daneben werden beim Bund folgende weitere Schutzmassnahmen umgesetzt:

- Prüfung kryptographischer Produkte: Kryptografische Produkte[54] dienen dem Schutz von Informationen im Sinne der Vertraulichkeit, Integrität, Authentizität und/oder Verbindlichkeit. Die Beschaffung und der Betrieb dieser Produkte ist besonders heikel, weil die korrekte kryptografische Funktionsweise nur von ausgewiesenen Fachexperten beurteilt und geprüft werden kann. Ohne fachgerechte Prüfung und Verifikation besteht das Risiko, dass kryptografische Produkte ihren gewünschten Anwendungszweck nicht erfüllen, ohne dass dies effektiv bemerkt wird. Aus diesem Grund werden Produkte im Bereich Kryptologie grundsätzlich durch das Bundesamt für Rüstung (armasuisse) als dafür spezialisierte Stelle beschafft.[55] armasuisse wird dabei durch die Fachstelle für Kryptologie in der Führungsunterstützungsbasis der Armee (FUB KRYPT) unterstützt. Deren Experten führen sowohl während der Beschaffung als auch bei Systemänderungen (z. B. nach Updates von Firm- oder Software) während des gesamten Lebenswegs des Systems detaillierte kryptologische Prüfungen durch.

- Schwachstellenanalysen durch das NCSC: Das NCSC ist die zentrale Meldestelle für entdeckte Schwachstellen bei Anwendungen der Bundesverwaltung. Es plausibilisiert die eingegangenen Meldungen, nimmt eine Risikoeinschätzung der Schwachstellen vor und leitet in Absprache mit den betroffenen Leistungserbringern und Verwaltungseinheiten entsprechende Massnahmen ein. Im VBS suchen Spezialisten des Cyber Defence Campus systematisch nach möglichen Schwachstellen und Angriffspunkten in der Software von Systemen und Anwendungen des Departements.

- Informationssicherheitsmanagementsystem (ISMS) im VBS: Ein ISMS definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten. Es dient dazu, Risiken der Informations- und Cybersicherheit (Informationen, Daten und Informatik) im Einklang mit den übergeordneten Organisationszielen systematisch zu identifizieren und zu bewältigen. Im VBS wurde ein ISMS nach der Norm ISO/IEC 27001 aufgebaut.

### 4.1.2 Anwendung von Standards zum SCRM

**Beschaffungsrechtliche Massnahmen:** Gemäss Artikel 20 Absatz 3 BöB kann für die Beschaffung von Waffen, Munition und Kriegsmaterial oder, sofern sie für Verteidigungs- und Sicherheitszwecke unerlässlich sind, sonstigen Lieferungen, Bauleistungen, Dienstleistungen, Forschungs- oder Entwicklungsleistungen, bei berechtigten Bedarfsträgern das Einladungsverfahren angewendet werden. Dabei bestimmt die zuständige Beschaffungsstelle, welche Anbieter sie ohne öffentliche Ausschreibung direkt zur Angebotsabgabe einladen will. Das Beschaffungsrecht lässt demnach bei sicherheitsempfindlichen Informatikbeschaffungen Raum für die Anwendung von Standards zum SCRM. Einschränkungen bei der Auswahl der Anbieter sicherheitsrelevanter IKT-Produkte, zum Beispiel aufgrund ihrer Staatszugehörigkeit, sind bei Beschaffungen für Sicherheits- und Verteidigungszwecke, und damit auch für solche der Armee, gestützt auf das BöB möglich.

**Abschluss von Informationsschutzabkommen:** Die Schweiz ist für Ihre Verteidigung sowie für ihre äussere und innere Sicherheit von einer engen Zusammenarbeit mit internationalen Partnern und deren industrieller Basis abhängig. Da in diesen Bereichen oft sicherheitsempfindliche Aufträge erteilt werden,

[54] Beispiele: Chiffriergerät, SmartCard, Hardware Security Module, Random Number Generator, Chiffriersoftware, Krypto-Library, etc.
[55] Vgl. Art. 10 Lit 1 Bst d der Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB; SR 172.056.15)

hat die Schweiz mit zahlreichen Staaten und internationalen Organisationen sogenannte Informationsschutzabkommen[56] abgeschlossen. Diese regeln den gegenseitigen Schutz klassifizierter Informationen und legen die Sicherheitsmassnahmen bei sicherheitsrelevanten bilateralen Beschaffungen fest. Der Abschluss von Informationsschutzabkommen setzt voraus, dass die Vertragsparteien in ihrem nationalen Recht über Sicherheitsinstrumente verfügen, die international anerkannte Standards erfüllen. Konkret verlangen die Informationsschutzabkommen, dass Firmen und Personen, die klassifizierte Aufträge der anderen Partei erfüllen sollen, im Rahmen eines Zertifizierungsverfahrens auf deren Vertrauenswürdigkeit hin geprüft werden.
Der internationale Standard zur Beurteilung der Vertrauenswürdigkeit von Firmen[57] verlangt unter anderem, dass geprüft wird, ob das Unternehmen von ausländischen Staaten oder Organisationen des öffentlichen oder privaten Rechts kontrolliert oder beeinflusst wird («Foreign Ownership, Control and Influence – FOCI»). Besteht ein zu hohes Risiko, müssen risikomindernde Massnahmen getroffen oder die Firma vom Vergabeverfahren ausgeschlossen werden. Dasselbe gilt auch für natürliche Personen.
Die Informationsschutzabkommen legen zwar in der Regel keine Anforderungen an die Produktesicherheit fest. Darin wird allerdings oft stipuliert, dass Informationssysteme, in denen Informationen der anderen Partei verarbeitet werden sollen, von einer kompetenten nationalen Sicherheitsbehörde akkreditiert werden. Die Akkreditierung belegt, dass das System die Sicherheitsanforderungen der anderen Partei erfüllt, was einer formellen Bestätigung der Produktesicherheit entspricht.

**Durchführung von Geheimschutzverfahren:** Mit dem Geheimschutzverfahren werden dem Auftragnehmer vom Auftraggeber hoheitlich Sicherheitsmassnahmen auferlegt.[58] Dieses Verfahren kommt jedoch nur zur Anwendung, wenn VERTRAULICH oder GEHEIM klassifizierte Informationen bearbeitet werden müssen.
Im Geheimschutzverfahren wird in einem ersten Schritt in Zusammenarbeit mit dem Nachrichtendienst des Bundes (NDB) die Vertrauenswürdigkeit der Firma geprüft, die für den Auftrag in Frage kommt. Anschliessend legt eine Fachstelle in einem Sicherheitsprotokoll die konkreten Massnahmen, die die Firma während der Auftragserfüllung umsetzen muss, hoheitlich fest. Wenn alle Massnahmen umgesetzt sind, erhält die Firma eine Betriebssicherheitserklärung. Diese entspricht einem auf internationaler Ebene anerkannten Zertifikat und ermächtigt die Firma, den klassifizierten Auftrag auszuführen. Die Fachstelle kann eine Firma mit einer gültigen Betriebssicherheitserklärung jederzeit und ohne Ankündigung inspizieren, um die Einhaltung der Sicherheitsauflagen zu kontrollieren.
Als Auftraggeber kommen grundsätzlich die Verwaltungseinheiten des VBS und das Bundesamt für Bauten und Logistik (BBL) in Betracht.[59] Auftragnehmer sind öffentliche Stellen ausserhalb des VBS und des BBL, private Unternehmen oder Personen, die für den Empfang und die Bearbeitung klassifizierter Informationen vorgesehen sind. Handelt es sich beim Auftragnehmer um ein Unternehmen mit Sitz in einem Drittstaat, so werden die sicherheitsmässige Auftragsabwicklung und die Modalitäten der Zusammenarbeit zwischen den jeweiligen nationalen Sicherheitsbehörden im entsprechenden Informationsschutzabkommen geregelt (siehe oben). Die Überprüfung des Unternehmens erfolgt in diesem Fall durch die Sicherheitsorgane des Drittstaats.
Mit dem ISG wird das Geheimschutzverfahren zu «Betriebssicherheitsverfahren» umbenannt und das Verfahren auf Firmen erstreckt, die im Rahmen eines Vertrags kritische Informationssysteme des Bundes (oder Teile davon) betreiben, verwalten, warten oder überprüfen müssen.

**Durchführung von Personensicherheitsüberprüfungen:** Bei Personen, die IKT-Dienstleistungen erbringen oder IKT-Produkte entwickeln, wird eine Personensicherheitsprüfung durchgeführt, wenn sie dabei Zugang zu Informationen haben sollen, die VERTRAULICH oder GEHEIM klassifiziert sind. Diese

[56] Siehe zum Beispiel Vereinbarung zwischen dem Schweizerischen Bundesrat und der Regierung der Republik Frankreich über den gegenseitigen Austausch und Schutz klassifizierter Informationen (SR 0.514.134.91) oder Vereinbarung zwischen dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport, im Namen des Schweizer Bundesrates und dem Bundesminister für Landesverteidigung der Republik Österreich über den Schutz von militärisch klassifizierten Informationen (SR 0.514.116.31)
[57] Die Standards im Bereich der internationalen Industriesicherheit werden durch die Multinational Industrial Security Working Group (MISWG) erarbeitet. Sie sind zwar nicht verbindlich, bilden aber die Grundlage für die Anerkennung der Gleichwertigkeit von Massnahmen.
[58] Siehe Verordnung über das Geheimschutzverfahren bei Aufträgen mit militärisch klassifiziertem Inhalt (Geheimschutzverordnung; SR 510.413)
[59] Die heutige Beschränkung des Geheimschutzverfahrens auf Aufträge mit militärisch klassifiziertem Inhalt wird mit dem Inkrafttreten des Informationssicherheitsgesetzes behoben.

Vorschrift gilt auch für das Personal von Lieferanten und Dienstleistern. Die prüfenden Stellen können dabei auf das Strafregister, auf den nationalen Polizeiindex und das Informationssystem Innere Sicherheit des NDB zurückgreifen. In einem abschliessenden Entscheid erlassen die prüfenden Stellen eine Verfügung, in welcher die geprüfte Person entweder für unbedenklich erklärt oder als Sicherheitsrisiko beurteilt wird. Eine Unbedenklichkeitserklärung verleiht jedoch nicht automatisch den Anspruch, einen Auftrag zu erhalten. Die Auftragserteilung steht dem Auftraggeber immer noch frei. Die Durchführung solcher Überprüfungen entspricht den Vorgaben des NIST 800-161 Standard zur «Third Party Personnel Security» (PS-7).
Mit dem ISG wird die Durchführung von Personensicherheitsprüfungen neu auch bei Personen möglich, die kritische Informationssysteme des Bundes (oder Teile davon) betreiben, verwalten, warten oder überprüfen müssen.

**Massnahmen bei der Vertragsgestaltung:** Gemäss der CyRV stellen die Verwaltungseinheiten des Bundes sicher, dass beim Bezug von Leistungen bei einem externen Leistungserbringer die Informatiksicherheitsvorgaben Teil des Vertragsverhältnisses sind. Um die Verwaltungseinheiten dabei zu unterstützen, wurde das Dokument «Referenz zu den Informatiksicherheitsvorgaben der Bundesverwaltung für die Beschaffungsunterlagen»[60] erstellt. Die enthaltenen Textbausteine können situativ angepasst oder ergänzt in die offiziellen Beschaffungsunterlagen (insbesondere für IKT-Software-Beschaffungen) integriert werden, beispielsweise in einem Musterpflichtenheft.
Verträge des Bundes beinhalten immer die der Vertragsart entsprechenden Allgemeinen Geschäftsbedingungen des Bundes (AGB). Abweichungen von den AGB sind nur in begründeten Ausnahmefällen zulässig. Solche AGB existieren für Dienstleistungen, Forschungsaufträge, Güterbeschaffungen und für verschiedene Rechtsgeschäfte. Sie beinhalten standardmässig auch Bestimmungen zur Sicherheit. Das Thema Sicherheit hängt jedoch überwiegend von den Vertragsklauseln ab, die im konkreten Vertragsverhältnis vereinbart wurden.
Für die Beschaffungsstellen des Bundes ist es besonders wichtig, der Informationssicherheit beim Geschäftspartner der Bundesverwaltung erhöhte Aufmerksamkeit zu schenken. Die Beschaffungskonferenz des Bundes (BKB) stellt den Beschaffungsstellen der Bundesverwaltung eine Musterklausel für Beschaffungsvertragsvorlagen zur Verfügung, die den Schutz der IKT-Systeme vor Angriffen und eine entsprechende Meldepflicht enthält[61]. Die Musterklausel ist als eigenständige Vertragsbestimmung ausgestaltet und kann in einen Beschaffungsvertrag übernommen werden. Ziel ist sowohl der Schutz der Daten und Informationen als auch der Systeme, namentlich vor und bei Cyberangriffen auf Vertragspartner der Bundesverwaltung. Für den Fall eines Cyberangriffs auf einen Lieferanten oder Dienstleister der Bundesverwaltung wird von den betroffenen Unternehmen gefordert, ihre Auftraggeberinnen beim Bund umgehend und direkt zu informieren und in Absprache mit ihnen adäquate Sofortmassnahmen zu ergreifen. Daher ist die Musterklausel in erster Linie für Beschaffungen geeignet, die ein hohes Risikopotential für Cyberangriffe aufweisen. Die Anwendung der Klausel ist nach Bedarf zu beurteilen und auf die konkreten Verhältnisse abzustimmen. Für jeden Vertrag soll eine individuelle und risikogerechte Ausgestaltung vereinbart werden.

Mittels einer sorgfältigen Vertragsgestaltung können folglich zahlreiche Aspekte der Sicherheit abgedeckt werden und der Bund kann sich Kontrollrechte ausbedingen. Der Bund kann jedoch in diesen Fällen seine Sicherheitsbedürfnisse nicht wie im Geheimschutzverfahren hoheitlich (einseitig) durchsetzen, sondern muss gegebenenfalls den Weg über den Zivilprozess beschreiten. Für Beschaffungen der Armee regelt armasuisse als zuständige Beschaffungsstelle in den Vertragsvereinbarungen den Umgang und die Bearbeitungsvorschriften mit schutzwürdigen Informationen.

[60] Siehe Newsletter September 2020 der Beschaffungskonferenz des Bundes (BKB)
[61] Siehe Mustervertragsklausel (sowie Erläuterungen) der BKB betreffend Cyberrisiken (PDF, 385 kB, 31.08.2020).

## 4.2 Anwendung von Standards bei kritischen Infrastrukturen

Wie in Kapitel 3.2 dargelegt, existieren für kritische Infrastrukturen wenige rechtliche Vorgaben bezüglich der Anwendung von Standards zur Produktesicherheit und zum SCRM. Dennoch sollte die Bedeutung von Standards für die Unternehmen in den kritischen Sektoren nicht unterschätzt werden. Standards werden oft als massgebliche Orientierungshilfen bei der Umsetzung von Massnahmen verwendet und helfen international tätigen Unternehmen, ihre Cybersicherheit über die Landesgrenzen hinaus zu koordinieren.
Im vorliegenden Kapitel wird zunächst auf die Bedeutung der Standards in den kritischen Infrastrukturen eingegangen und aufgezeigt, welche Rolle Standards im Bereich Produktesicherheit und SCRM spielen, obwohl ihre Anwendung nur in wenigen Fällen rechtlich vorgeschrieben ist. Der Bund fördert die Anwendung von Standards, indem er systematische Risikoanalysen in den kritischen Sektoren durchführt und die Sektoren bei der Erarbeitung von IKT-Minimalstandards fachlich unterstützt. Beide Massnahmen werden ebenfalls kurz beschrieben.

### 4.2.1 Generelle Einschätzung zur Anwendung der Standards bei kritischen Infrastrukturen

Obwohl die Anwendung von Standards nicht verpflichtend ist, orientieren sich viele Unternehmen bei der Umsetzung von Massnahmen der Informatiksicherheit an internationalen Standards. In der in Deutschland durchgeführten Studie «TÜV-Cybersicherheitsstudie» von 2019 wurde dies von 64% der befragten Unternehmen bestätigt.[62] In der Schweiz dürfte dies ähnlich sein. Gemäss einer Studie zur Cybersicherheit in KMU der Schweiz richten sich 60% der befragten Unternehmen nach internationalen Standards.[63] Dabei handelt es sich um einen pragmatischen Ansatz, bei dem Standards im Sinne von Richtlinien oder Hilfsmitteln zur Stärkung der IKT-Sicherheit umgesetzt werden. Eine vollständige und zertifizierte Implementierung wird dabei nicht angestrebt. Aus diesem Grund ist es nicht einfach zu beurteilen, in welchem Ausmass die Betreiber kritischer Infrastrukturen die Standards umsetzen. Um diese Frage besser einschätzen zu können, hat das Bundesamt für Wirtschaftliche Landesversorgung (BWL) ihre Expertinnen und Experten zur Bedeutung von Standards in ihren Branchen befragt[64]. Diese bestätigen, dass Standards zur sicheren Anwendung von IKT-Mitteln in den meisten Unternehmen bekannt sind und nach Bedarf angewendet werden. Gemäss Einschätzung der Befragten sind dabei die Standards der ISO-Reihen für Schweizer Unternehmen am relevantesten. Die Expertinnen und Experten stellen fest, dass sich die Anwendung der Standards auf methodische oder prozedurale Vorgehen beschränkt. Physische Tests von Hardware oder Analysen des Quellcodes von Software übersteigen gemäss übereinstimmenden Aussagen der befragten Experten die in den Unternehmen vorhandenen finanziellen und personellen Ressourcen bei weitem.
In Bezug auf das SCRM wenden nur sehr wenige Firmen ein systematisches, auf die Informationssicherheit bezogenes Lieferantenmanagement an. Einige Firmen definieren sicherheitsbezogene Evaluationskriterien und integrieren die Risiken des Lieferantenmanagements systematisch in das unternehmensweite Risikomanagement. Typischerweise handelt es sich dabei um eher grössere, finanzkräftige Unternehmen sowie besonders exponierte Unternehmen.

### 4.2.2 Risikoanalysen in den kritischen Sektoren

Die Risiken- und Verwundbarkeiten in den kritischen Sektoren werden im Rahmen der Umsetzung der NCS und der Strategie zum Schutz kritischer Infrastrukturen (SKI) regelmässig durch Experten aus der

[62] TÜV Cybersicherheitstudie 2019
[63] Cyberrisiken in Schweizer KMUs, gfs Zürich, 2017
[64] Die Befragung erfolgte im Juni 2019.

Wirtschaft und der Verwaltung analysiert. Ein Fokus wird dabei auf Cyberrisiken gelegt. Die gewonnenen Erkenntnisse helfen, Cyberrisiken im Kontext der gesamten Gefährdungslage der kritischen Infrastrukturen besser einzuordnen, entsprechende Massnahmen abzuleiten und diese zu priorisieren.
Koordiniert durch das Bundesamt für Bevölkerungsschutz BABS werden im Rahmen der Umsetzung der zweiten NCS von 2018-2022 alle bestehenden Risiko- und Verwundbarkeitsanalysen aktualisiert und bei Bedarf neue Resilienz-Massnahmen abgeleitet. Die im Rahmen der ersten NCS-Periode bereits beschlossenen und laufenden Resilienz-Massnahmen werden gemäss den vereinbarten Verantwortlichkeiten weitergeführt.

### 4.2.3 Minimalstandards, Handbücher und Richtlinien

Das BWL hat einen Minimalstandard zur Verbesserung der IKT-Resilienz entwickelt.[65] Dieser Minimalstandard basiert auf dem NIST-Standard und soll den Betreibern kritischer Infrastrukturen als Empfehlung und mögliche Richtschnur zur Verbesserung der IKT-Resilienz (inkl. SCRM) dienen. In enger Zusammenarbeit mit den Branchen entwickelt das BWL abgeleitet vom generellen Minimalstandard sektorspezifische Standards und Richtlinien.[66]
Die Minimalstandards sind rechtlich nicht bindend, haben aber den Vorteil, dass sie sich in die etablierten Strukturen in den Sektoren einbetten. Die dort entwickelten technischen Vorgaben werden in den Sektoren seit vielen Jahren angewendet und beachtet. Wenn diese mit Vorgaben zur Informatiksicherheit ergänzt werden, kann dies einen grossen Effekt auf die Sicherheit im Sektor haben.

# 5 Fazit

Die Herausforderungen in den Bereichen Produktesicherheit und SCRM in der Cybersicherheit und der Cyberdefence sind sehr gross. Risiken, die auf mangelnde Sicherheit bei den Produkten selber zurückzuführen sind und die in Bezug auf die Lieferanten bestehen, können heute nur reduziert, aber nicht verhindert werden. Die beiden Aspekte betreffen Kernelemente beim Schutz vor Cyberrisiken. Die Prüfung, mit welchen Massnahmen diesen Herausforderungen begegnet werden kann, ist deshalb von grosser Bedeutung. Die Anwendung von international anerkannten Standards kann dabei einen wichtigen Beitrag leisten.
Die Analyse der bestehenden Standards hat gezeigt, dass zahlreiche Standards im Bereich der Produktesicherheit und der sicheren Anwendung dieser Produkte existieren. Dies ist eine Folge davon, dass die mangelnde Sicherheit von IKT-Produkten schon seit vielen Jahren erkannt ist. Verschiedene dieser Standards zur Produktesicherheit finden auch eine breite Anwendung.
Vorgaben zum SCRM im Bereich der Cybersicherheit sind deutlich weniger weit entwickelt. Einerseits wurde die Wichtigkeit des Themas von den Standardisierungsgremien erst in den letzten Jahren aufgenommen. Die Risiken in den Lieferketten wurden erst zum Thema, als erkannt wurde, in welchem Ausmass Staaten aus geopolitischen Interessen Einfluss auf strategisch wichtige Lieferanten nehmen. Andererseits macht die Mischung aus technischen, rechtlichen und politischen Fragen das Thema für Standardisierungsvorhaben kompliziert. Weil es schwierig ist zu definieren, ab wann ein Risiko in Lieferketten zu gross wird, fokussieren die meisten Standards zum SCRM auf Prozesse und Methoden, wodurch sie ebenfalls eher den Charakter von unverbindlichen Handlungsanweisungen als von verbindlichen Normen erhalten.
Der Bericht hat analysiert, wie die Schweiz mit den internationalen Standards in den untersuchten Bereichen in Bezug auf die Bundesverwaltung und die Armee sowie hinsichtlich der kritischen Infrastrukturen umgeht. Die Resultate dieser Analyse sollen nachstehend kurz zusammengefasst werden.

[65] IKT-Minimalstandard (admin.ch)
[66] Branchenstandards (admin.ch)

## 5.1 Die Rolle von Standards in der Bundesverwaltung und in der Armee

Innerhalb der Bundesverwaltung und in der Armee bestehen zahlreiche Vorgaben zur Sicherheit und zur sicheren Anwendung von IKT-Produkten. Das System der Vorgaben basiert sehr stark auf den ISO/IEC Standards der Reihe 2700X und deren Ausführungen in den BSI-Standards. Mit der 2020 in Kraft getretenen CyRV wurden diese Vorgaben auf eine neue rechtliche Grundlage gehoben. Die jährlich vom NCSC zuhanden des Bundesrates durchgeführte Analyse zum Umsetzungsstand der IKT-Sicherheit im Bund zeigt jeweils auf, dass die Arbeit mit der Schaffung von Vorgaben längst nicht getan ist. Die Umsetzung von Standards ist anspruchsvoll und erfordert ein dauerhaftes Engagement. Als Fazit zur Situation in der Bundesverwaltung mit Bezug auf Standards zur Produktesicherheit kann festgehalten werden, dass der Fokus stärker auf eine durchgehende und umfassende Umsetzung der Vorgaben sowie auf die Kontrolle dieser Umsetzung gelegt werden muss statt auf die Weiterentwicklung des bereits weitgehend ausgearbeiteten Regelwerks. Der Bundesrat nimmt jährlich den Umsetzungsstand der IKT-Sicherheitsvorgaben zur Kenntnis und informiert die zuständigen Kommissionen des Parlaments detailliert über diesen Stand.
Für die Anwendung von Standards im Bereich SCRM trifft dieses Fazit für die Bundesverwaltung und die Armee nicht in gleichem Masse zu. Es gibt an verschiedenen Stellen einzelne Vorgaben zur Umsetzung eines SCRM, es gibt aber keine Grundlage, welche die Umsetzung eines systematischen SCRM vorschreibt. Dies liegt einerseits daran, dass nur wenige direkt umsetzbare Standards zum SCRM existieren. Andererseits liegt es an den rechtlichen Rahmenbedingungen. Die Grundlagen für die einzelnen Schritte des SCRM waren bisher in verschiedenen Gesetzen geregelt. Mit dem Informationssicherheitsgesetz (ISG), das jedoch noch nicht in Kraft getreten ist, wird nun ein einheitlicher rechtlicher Rahmen für die verschiedenen Massnahmen geschaffen. Es verfolgt bezüglich Informationssicherheit einen integralen Ansatz bestehend aus dem Informationsschutz (Staatsschutz), Informatiksicherheit, Personen- und Betriebssicherheit. Zusammen mit den im BöB festgehaltenen Grundprinzipien sowie den Ausnahmen zu den Grundsätzen des Freihandels wird es künftig möglich sein, bereits in einem frühen Stadium der Beschaffung (Supply Chain) Einfluss zu nehmen (z. B. frühzeitiger Ausschluss risikobehafteter Lieferanten) und damit innerhalb des Bundes ein stringentes System zum SCRM aufzubauen.

## 5.2 Die Rolle von Standards bei kritischen Infrastrukturen

Im Vergleich zur Situation in der Bundesverwaltung existieren für kritische Infrastrukturen nur wenige verbindliche Vorgaben zur Anwendung von Standards im Zusammenhang mit der Produktesicherheit und dem SCRM. In vielen Sektoren wurden in den letzten Jahren die Bemühungen verstärkt, solche Vorgaben über Branchenvereinbarungen, Handbücher oder Richtlinien einzuführen. Da diese Arbeiten ebenso wie die Umsetzung der Vorgaben jedoch massgeblich auf freiwilligem Engagement der Unternehmen beruhen, bleibt die Einführung von Standards bei kritischen Infrastrukturen unvollständig. Weil kritische Infrastrukturen aufgrund der Digitalisierung stark voneinander abhängig sind, bleibt das Risiko, dass schlecht geschützte Systeme die Sicherheit aller anderen Infrastrukturbetreibenden beeinträchtigen, bestehen.
Die offensichtlichste Option zur stärkeren Verbreitung von Standards ist die Schaffung neuer rechtlich bindender Vorgaben. Da im Bereich der Produktesicherheit bereits verschiedene etablierte Standards bestehen, wäre dies über Verweise auf diese Standards möglich. Denkbar wären Vorgaben für die Betreibenden kritischer Infrastrukturen zum sicheren Umgang mit IKT-Produkten. Es gilt zu prüfen, welche Vorgaben in welchen Bereichen sinnvoll sind. Dabei soll berücksichtigt werden, dass die IKT-Produkte in verschiedenen kritischen Infrastrukturen unterschiedliche Anwendungen finden und die Vorgaben dem jeweiligen Kontext anzupassen sind. Zudem ist die Schaffung von Vorgaben zur Sicherheit der IKT-Produkte selbst möglich. Dabei werden üblicherweise Zertifizierungen von IKT-Produkten in besonders wichtigen Anwendungsbereichen verlangt. Die Entwicklung solcher Zertifizierungsschemen wird

aktuell auch innerhalb der EU stark vorangetrieben.[67] Der Nachteil solcher Vorschriften besteht darin, dass sie oft zu sehr aufwändigen Zertifizierungsverfahren führen. Zertifizierungen durchzuführen und aktuell zu halten ist wegen der Komplexität vieler IKT-Systeme und den häufigen Updates, die bei solchen Systemen durchgeführt werden, für die Hersteller und die Einkäufer mit einem hohen Zeit- und Kostenaufwand verbunden. Der Bundesrat prüft im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS), in welchen Bereichen Regulierungsbedarf besteht, klärt ab, in welchen Fällen die Zuständigkeit für die Regulierung beim Bund liegt und schlägt dem Parlament bei Bedarf und gegebener Bundeskompetenz Vorlagen zur Einführung von verbindlichen Vorgaben für die Anwendung von Standards bei kritischen Infrastrukturen vor.[68]

Grundsätzlich können auch Vorgaben zum SCRM über regulative Massnahmen eingeführt werden. Beispiele für mögliche Vorgaben zum SCRM finden sich im IKT-Minimalstandard des BWL in Kapitel 2.2.6.[69] Es gilt jedoch generell festzuhalten, dass Vorschriften für kritische Infrastrukturen bei der Beschaffung von Dienstleistungen und bei der Ausgestaltung der Beziehungen zu Lieferanten einen vergleichsweise starken regulativen Eingriff darstellen und es muss vorgängig geklärt werden, unter welchen Bedingungen sie überhaupt durch den Bund erlassen werden können. Solche Lösungen stehen deshalb in Bezug auf die Förderung der Anwendung von Standards zum SCRM nicht im Vordergrund.

Zu prüfen ist generell, wie die Kapazitäten zur Analyse von Produkten und den Produktionsprozessen, die ihrer Herstellung zugrunde liegen, verbessert werden können. Dies entspricht einer der zentralen Forderungen, welche das Whitepaper «Supply Chain Security» von ICTswitzerland erhoben hat. Der Bund begrüsst private Initiativen für den Ausbau diesbezüglicher Kapazitäten bzw. für den Aufbau von Prüfzentren für Hard- und Softwarekomponenten in der Schweiz und ist bereit, solche Initiativen mit Fachwissen zu unterstützen.

[67] Vgl. dazu die neue Cybersicherheitsstrategie der EU: New EU Cybersecurity Strategy (europa.eu)
[68] Das BABS hat im Rahmen der nationalen SKI-Strategie 2018-2022 mit Massnahme 2 bereits den Auftrag erhalten, die Schaffung oder Anpassung von Rechtsgrundlagen mit sektorübergreifenden Vorgaben für die Betreiber zu prüfen.
[69] Bundesamt für wirtschaftliche Landesversorgung: IKT-Minimalstandard (admin.ch)