Konzeptpapier
zur Schaffung eines

PRÜFINSTITUTS FÜR VERNETZTE GERÄTE UNTER DEM GESICHTSPUNKT DER CYBER-SICHERHEIT

Autoren:

Dr. Thomas Held
Dr. Raphael M. Reischuk

Version 1.1, 20. Juli 2020

Inhaltsverzeichnis

Zu diesem Bericht

Der Bericht zum Cyber-Prüfinstitut Schweiz entstand als Teil der 2019 lancierten Cyber-Initiative Zug. Im Rahmen des umfassenderen Investitionsprogrammes «Zug plus» wollte der Regierungsrat abklären lassen, inwieweit sich der Kanton am NCS-Umsetzungsplan 2018–2022 engagieren könnte. Im Hinblick auf zwei «Runde Tische», zu denen der damalige Bundespräsident Ueli Maurer am 8. Juli und am 27. November 2019 einige «willige Kantone» geladen hatte, wurden zwei Projektideen entwickelt. In der Folge beschloss der Regierungsrat, diese beiden Projektideen in Richtung von Businessplänen weiter zu entwickeln. Zu diesem Zweck wurde eine Leitungsdelegation aus Finanzdirektor Heinz Tännler und dem Sicherheitsdirektor Beat Villiger sowie drei Vertretern der Privatwirtschaft (Thomas Meier, InfoGuard; Andreas Umbach, Präsident Wirtschaftskammer Zug; Beat Weiss, V-ZUG Immobilien) gebildet. Als Projektsekretär wurde Dr. Thomas Held, u.a. ehem. Direktor der Denkfabrik Avenir Suisse, mandatiert, der in der Folge Prof. Dr. René Hüsler, Direktor Departement Informatik der Hochschule Luzern, und Dr. Raphael Reischuk, Head of Cyber Security Services Zühlke Engineering AG, zur Bildung und Leitung von zwei Arbeitsgruppen motivieren konnte.

Die erste Arbeitsgruppe (unter dem provisorischen Titel «Melani für KMU») erarbeitete unter der Leitung von Prof. Dr. René Hüsler, Direktor Departement Informatik der Hochschule Luzern, einen Plan für ein koordiniertes Netzwerk zu Cyber-Security Awareness und Ausbildung von KMU mit entsprechendem Angebot.[1]

Aus der zweiten Arbeitsgruppe «Prüfinstitut» ist der vorliegende Bericht hervorgegangen. Der Arbeitsgruppe gehörten neben Raphael Reischuk an:

- Markus Bischof (CISCO)
- Thomas Dullien (optimyze)
- Tobias Ellenberger (Oneconsult AG)
- Stefan Frei (Accenture)
- Christof Jungo (SecIntel)
- Andreas Kaelin (ICTswitzerland)
- Ivo Maritz (BKW)
- Bernard Plattner (Prof. em. ETH)
- Martin Steiger (RA, Steiger Legal)
- Gérald Vernez (VBS)
- Andreas von Ow (Kuldelski Security)
- Nicole Wettstein (SATW)

Die Inputs aus der Arbeitsgruppe erfolgten in insgesamt drei Sitzungen sowie in zahlreichen bilateralen Gesprächen und Mail-Umfragen. Eine Ausnahme bildet die Bestandsaufnahme der Lage in einigen ausgewählten Ländern (Kapitel 2), die in dankenswerter Weise von Nicole Wettstein (SATW) recherchiert und

verfasst wurde. Die Selektion, Gewichtung und Strukturierung der Aussagen lagen in den Händen von Thomas Held und Raphael Reischuk, letzterer ist auch verantwortlich für die Schlussredaktion. Neben den Mitgliedern der Arbeitsgruppe lieferten auch weitere Fachleute wertvolle Informationen, insbesondere Levente Dobszay (Electrosuisse), Dr. Vincent Lenders (armasuisse W+T) und Dr. Markus Mackenbrock (BSI Deutschland).

Inhaltlich schliesst der vorliegende Bericht an verschiedene Lagebeurteilungen und Forderungen aus Expertenkreisen, Fachverbänden und der Politik an. Insbesondere baut er auf dem Ende 2019 veröffentlichten White Paper der Arbeitsgruppe Supply-Chain der Cybersecurity-Kommission von ICTswitzerland auf. Die Arbeitsgruppe «Prüfinstitut» hat mit Unterstützung des Kantons während einer gewissen Zeit die Arbeiten dieser Kommission weitergeführt und ergänzt.

Organisation des Berichts

Der Bericht zeigt die wesentlichen Diskussionspunkte und Ergebnisse der Arbeitsgruppe «Prüfinstitut» auf. Er präsentiert eine Bestandsaufnahme der Prüf- und Zertifizierungssituation in vergleichbaren Staaten (Kapitel 2) und stellt technische und organisatorische Anforderungen an ein Prüfinstitut vor (Kapitel 3, 4, 5). Mögliche Pfade zur Ausgestaltung eines Schweizer Prüfinstituts für vernetzte Geräte werden vorgestellt, evaluiert und schliesslich priorisiert (Kapitel 6, 7).

1 WIESO soll geprüft werden? De quoi s'agit-il?

Das Ziel der im Folgenden präsentierten Überlegungen und Vorschläge ist der Aufbau eines **Prüfinstituts für vernetzte Geräte unter dem Gesichtspunkt der Cyber-Sicherheit**. Diese Organisation soll eine nationale Ausrichtung und – über die Zeit – eine internationale Ausstrahlung erreichen. Der vorliegende Bericht soll aufzeigen, was eine solche Institution leisten soll und wie sie eingerichtet und betrieben werden könnte. Darüber hinaus werden das organisatorische und regulatorische Umfeld in der Schweiz diskutiert und die entsprechenden Prüforganisationen in verschiedenen Ländern skizziert.

In Kapitel 1 werden die Argumente für eine solche Einrichtung sowie mögliche Schwerpunkte der Tätigkeit im Sinne einer thematischen Einleitung kurz skizziert.

1.1 Argumente für ein Cyber-Prüfinstitut Schweiz (CPIS)

Ausgangspunkt für das vorliegende Dokument sind verschiedene Lagebeurteilungen und Forderungen aus Expertenkreisen, Fachverbänden und der Politik, namentlich den Initiativen von ICTswitzerland sowie den Vorstössen von Nationalrat Marcel Dobler (19.3135, 19.3136). Diese Stimmen gipfelten in einem im September 2019 veröffentlichten White Paper der Arbeitsgruppe Supply-Chain der Cybersecurity-Kommission von ICTswitzerland.

Zusammenfassend werden die von Seiten der Experten und der Wirtschaft sowie aus politischer Sicht angeführten Argumente für die Schaffung einer Prüfinstitution präsentiert.

1.1.1 Wachsende Gefahr durch steigende Vernetzung

In jüngster Zeit verzeichnet sich ein Anstieg der Wahrnehmung (und für eine wachsende Zahl von Unternehmen und Organisationen auch die bittere Erfahrung) einer klaren und gegenwärtigen Gefahr einer grossen und wachsenden Verbreitung von Cyber-Angriffen und -Vorfällen weltweit in den verschiedensten Branchen und Umgebungen. Die vernetzte Gesellschaft wird mit der steigenden Anzahl von neuartigen Interaktionen zwischen Menschen, Maschinen, Diensten und diversen Rückkopplungsprozessen stetig komplexer. Der Anstieg der Komplexität der auf vernetzten Geräten laufenden Software bedeutet insbesondere einen Anstieg der Zahl der enthaltenen Schwachstellen. Typische Schätzungen gehen von 1 bis 100 Schwachstellen pro 2000 Zeilen Programmcode aus.[2] Ist ein Produkt nun in der Lage, sich mit anderen zu vernetzen, dann sind diese Schwachstellen mit hoher Wahrscheinlichkeit von kriminellen Akteuren aus der Ferne ausnutzbar.

Weiter bestehen durch Abhängigkeiten von Hard- und Software sowie beim Einkauf von Leistungen (direkt oder delegiert) bis dato unbekannte Risiken.[3] Mit der prognostizierten Zunahme der vernetzten Geräte (IoT in Industrie und Haushalt) droht ein eigentlicher Kontrollverlust.

1.1.2 Cyberspace als scheinbar gesetzloser Raum

Im Vergleich zu anderen, z. T. besser bekannten und managebaren Gefahren/Risiken (mechanische, chemische und biologische Prozesse, Nukleartechnik, Gentechnik usw.) ist der Cyberspace nach Meinung vieler Experten ein scheinbar gesetzloser Raum.[4] Der ICT-Sektor verfügt, abgesehen vom Datenschutz, kaum über verbindliche und rechtsgültige Normen, welche die Sicherheit und die Integrität der eingesetzten Produkte auf gesetzlicher Ebene regeln. Es gibt weder gesetzlich verbindliche Minimalverpflichtungen noch eine gesetzlich verankerte Produktehaftung für Software.[5]

Die Technikgeschichte zeigt, dass sich beim Aufkommen neuer Technologien überprüfbare und regulierte Standards langfristig durchsetzen – gegen den anfänglichen Widerstand der Industrie und häufig erst nach schwerwiegenden Zwischenfällen. In allen kritischen Industriesektoren sind Qualitätsprüfungen durch unabhängige Stellen heute fester Bestandteil der Produktezulassung, wie z.B. in der Automobilindustrie, Luftfahrt, Medizinaltechnik, Pharmazie, Energie, Nahrungsmittelindustrie usw.

1.1.3 Unterschätzte Gefahr aus der Supply-Chain

Im Vergleich zu den Risiken, ausgehend von Schadsoftware, und den vielfältigen Bemühungen entsprechende Cyber-Angriffe zu erkennen bzw. zu verhindern und abzuwehren, werden die Risiken in der Beschaffungskette von Firmen und Organisationen tendenziell unterschätzt.[6] Die Hardware/Firmware gilt in den Augen vieler Experten als ein wenig geschützter Bereich, weil mit dem Besitz von Geräten die «Illusion der Kontrolle» verbreitet ist. Cyber-Sicherheit ist fälschlicherweise häufig auf Software und Netzwerksicherheit beschränkt; die Integrität und Sicherheit der Hardware und ihrer Bestandteile wird selten miteinbezogen. Finden digitale Produkte mit Sicherheitsdefekten den Weg in den Markt, können sich Schwachstellen über Jahrzehnte auswirken. Davon betroffen sind auch fest verbaute Geräte in Haus- oder Industriesteuerungen. Kompromittierte Hardware/Firmware macht häufig alle anderen Sicherheitsmassnahmen zunichte.[7]

1.1.4 Bedrohungen für kritische Infrastrukturen

In kritischen Infrastrukturen kann die Unkenntnis über das Sicherheitsniveau der eingesetzten Produkte zu flächendeckenden Bedrohungen führen und die Versorgung mit Strom und Wasser, aber auch den Verkehr, das

Gesundheitssystem und die Sicherheits- und Schutzorganisationen stark beeinträchtigen oder ganz lahmlegen. Ebenso kann der Einsatz von unzureichend gesicherten Geräten in Privathaushalten zu gravierenden Schäden an kritischen Infrastrukturen führen.[8] Ein effektiver Schutz gegen derart gesellschaftlich-relevante Bedrohungen ist heute so gut wie inexistent. Gezielte Cyber-Angriffe auf Versorgungseinrichtungen in verschiedenen europäischen Staaten zeigen deutlich das Schadenpotenzial: neben dem Primärzweck der Zerstörung wird auch die Bevölkerung verunsichert und mindestens indirekt geschädigt.[9] Die Eintrittsbarriere für diese Art von Angriff ist unnötig tief, weil

- sich kompromittierte Produkte aufgrund mangelnder Prüfkapazitäten und -fähigkeiten oft nicht detektieren lassen[10],
- Qualitätsmerkmale vom Hersteller und dessen Lieferanten aufgrund fehlender Standards und deren Überprüfbarkeit oft nicht eingefordert werden können,
- der Unterhalt der Infrastruktur oft nicht hinreichend sichergestellt ist, da gewisse Produkte manuelle Modifikationen erfordern und regelmässige Prüfungen nach vorgenommenen Modifikationen fehlen.

1.1.5 Nationale Notwendigkeiten

Die Standardisierung und Regulierung von Hardware/Firmware spielt sich hauptsächlich auf einer internationalen bzw. europäischen Ebene ab (vgl. auch Kapitel 2). Damit die Schweiz als wichtiger Standort mit einer hoch entwickelten digitalen Wirtschaft in diesen Bemühungen mitwirken kann, braucht es eigene Fähigkeiten und Kapazitäten zur unabhängigen Prüfung von Hardware/Firmware, einschliesslich der rechtlichen und fachlichen Möglichkeiten für Reverse Engineering[11].

Beispielsweise ist für intelligente Strommessgeräte gemäss Art. 8b der Stromversorgungsverordnung (StromVV, SR 734.71) eine Datensicherheitsprüfung vorgeschrieben. Diese Prüfung soll vom Eidgenössischen Institut für Metrologie (METAS) durchgeführt werden, welches mangels eigener Prüfressourcen Dritte mit der Prüfung beauftragt. Aufgrund fehlender akkreditierter Prüflabore in der Schweiz werden die Prüfungen im Ausland durchgeführt.

Darüber hinaus besteht akuter Handlungsbedarf auf der politisch/regulatorischen Seite insbesondere betreffend dem neu zu definierenden bilateralen Abkommen (Mutual Recognition Agreement, MRA) mit der EU (siehe dazu auch Abschnitt 2.3).

1.1.6 Internationale Ausstrahlung

Neben dieser Liste von organisatorischen und strukturellen Defiziten und dem entsprechenden Handlungsbedarf werden auch oft die Chancen einer schweizerischen Prüfinstituts-Initiative betont. Zusätzlich zu den traditionellen

Standortvorteilen wie der hoch entwickelten und international maximal verflochtenen Wirtschaft könnte eine schweizerische Prüfinstitution mit internationaler Ausstrahlung von folgenden Faktoren profitieren:

- der pragmatischen Kultur der Schweiz, die – in der Ausbildung und in den Unternehmen – Theorie und Praxis in anerkannter Weise verbindet,
- den Spitzenrängen der ETH in Informatik (darunter Informationssicherheit, Kryptographie, Machine Learning), Materialkunde usw.,
- der Neutralität der Schweiz in einer re-nationalisierten Weltwirtschaft,
- der Vertretung/Existenz international anerkannter Organisationen (darunter das Labor Spiez, die UNO, das WEF, die WHO, die WTO, die ISO, die IEC, die ITU),
- der Rechtssicherheit und der Tradition der guten Dienste,
- wenig protektionistischen Interessen aufgrund des Fehlens einer eigenen Hardware- und Softwareindustrie.

Die Fähigkeit zur unabhängigen und effektiven Prüfung von digitalen Produkten – inklusive Reverse Engineering von Chips und Firmware – wird in naher Zukunft im weltwirtschaftlichen Kontext wichtiger werden. Durch die Digitalisierung von alltäglichen und kritischen Funktionen wird in der Industrie wie auch bei Behörden, der Polizei und der Armee der Bedarf an dieser Fähigkeit steigen. Um im Cyber-Testing nicht ausschliesslich von externen Partnern abhängig zu sein, sollte in der Schweiz eine entsprechende Prüfinstanz aufgebaut werden.

1.2 Mögliche Ausrichtung eines Cyber-Prüfinstituts

In der oben skizzierten Lagebeurteilung und bezüglich der Wünschbarkeit oder gar Notwendigkeit eines Prüfinstituts herrscht unter den beteiligten Experten weitgehend Konsens. Gleiches gilt für die generelle Aufgabe: Das Prüfinstitut versteht sich als zentrale Anlaufstelle für Schweizer Prüfbegehren mit Fokus auf Schwachstellenfreiheit im informations- und cyberphysischen Sinne. Sie orientiert sich an Bedürfnisse des Schweizer Markts im Sinne der Hersteller und Lieferanten (KMU und Grossunternehmen) sowie der Verbraucher (kritische Infrastruktur, Behörden und Verwaltung, Grossunternehmen, KMU, Private). Für die konkrete Umsetzung dieser Zielsetzungen gibt es jedoch unter den beteiligten Experten unterschiedliche Auffassungen und Stossrichtungen. Dies gilt insbesondere bezüglich der institutionellen Verankerung und der inneren Organisation der neuen Einrichtung.

Im Sinne einer multidimensionalen Liste werden hier die wichtigsten Dimensionen zu den Aufgaben und Funktionen des Prüfinstituts aufgelistet. Diese Anforderungen und Vorgaben schliessen sich nicht aus, sondern überlagern sich. Das Programm der zu schaffenden Institution wird im weiteren Verlauf des Dokuments anhand dieser Achsen eingeordnet und definiert. In Kapitel 3 wird

diskutiert, *wer* Prüfungen auslösen soll (oder muss), in Kapitel 4 wird definiert und eingegrenzt, *was* die zu prüfenden Objekte sind, in Kapitel 5 wird skizziert, *wie* der Prüfprozess aussehen könnte. Kapitel 6 schliesslich listet die möglichen Organisationstypen für ein Prüfinstitut sowie die machbaren Wege dazu auf.

1.2.1 Prüfinstitut – Prüfinstanz – Prüfstelle

Der Begriff Prüf*institut* wird hier generisch und als Oberbegriff verwendet. Er umfasst

- Prüf*instanzen* – also Organisationen, die Prüfungen normieren, spezifizieren, koordinieren, kontrollieren und zertifizieren sowie
- Prüf*stellen* – also Labors und Testeinrichtungen, die mit entsprechender Einrichtung die eigentlichen Prüfungen durchführen.

(Die Begriffe *Prüfstelle* und (*Test-*)*Labor* werden im Folgenden sinnverwandt gebraucht.)

Ob die beiden Funktionen «unter einem Dach» bzw. in einer Institution organisiert werden sollen oder können, ist eine offene Frage. Auf der einen Seite wird ein Labor mit hoch qualifiziertem Personal, einem wissenschaftlichen Stab und einer State-of-the-Art-Ausrüstung als zentraler Bestandsteil der Idee «Prüfinstitut» angesehen. Andererseits betonen anderslautende Stimmen hingegen die klare Trennung zwischen einer quasi hoheitlichen, auf jeden Fall normsetzenden Instanz, die die Prüfstellen bei Prüfverfahren begleitet und überwacht, aber selbst weder personell noch vom Instrumentarium her über alle spezifischen Prüffähigkeiten verfügt. Vielmehr arbeitet sie je nach Aufgabe mit (akkreditierten) Prüfstellen im In- und Ausland zusammen.

1.2.2 Nachfrage im Markt

Ein zentrales Kriterium für die Ausrichtung der Prüfungen ist die Nachfrage nach Prüfungen von Seiten der Industrie sowie staatlicher und internationaler Organisationen. Die Beispiele von Cyber-Prüfinstanzen im benachbarten Ausland, aber auch die Erfahrungen der Normierungsinstanz Electrosuisse zeigen, dass die Nachfrage der Hersteller und Lieferanten wesentlich von entsprechenden staatlichen sowie internationalen Vorschriften abhängt. Inwiefern ein Bedarf auf der Seite der Besteller die Nachfrage der Hersteller ergänzen oder substituieren könnte, bleibt offen. Als normgebender Akteur (und damit indirekter Nachfrager nach Prüfleistungen) wird häufig auch der Versicherungssektor genannt.

1.2.3 Kritische Infrastruktur

Wegen der vermutlich auf lange Sicht grundsätzlich beschränkten Ressourcen für Prüfungen schlagen manche Experten vor, die Prüftätigkeit auf

Unternehmen und Operationen zu beschränken, die von gesamtwirtschaftlicher und/oder sicherheitspolitischer Bedeutung sind. In diesen Sektoren sollten zudem vor allem jene Systeme geprüft werden, die in hohem Masse von Beschaffungen und externen Leistungen (Lieferanten, Betreuung, Cloud) abhängig sind. Innerhalb dieses Kreises würden sich Prüfungen zudem auf die Lieferkette konzentrieren.[12]

1.2.4 Fokus auf gerätespezifische Risiken

Im Gegensatz zur Konzentration auf kritische Infrastrukturen geht es bei der Ausrichtung der Prüfungen auf intelligente und vernetzte Geräte und deren Komponenten nicht nur um die Anfälligkeit, sondern auch um die Verbreitung der Geräte. Im Hinblick auf die rasante Entwicklung von IoT wird von manchen Seiten vorgeschlagen, nicht nur ICT-Komponenten wie Computersysteme und deren Peripherie, Routers, Firewalls usw. in Prüfungen einzubeziehen, sondern auch vernetzte Maschinen in der Industrie, vernetzte Sensoren, Haushaltsgeräte, Consumer Electronics und medizinische Apparate. Ein mögliches Resultat der Prüfungen wäre dabei ein Gütesiegel bzw. Label (im Sinne minimaler Standards), u. U. aber auch für eigentliche Zulassungsprüfungen (mindestens für kritische Infrastrukturen).[13]

1.2.5 Fokus auf marktspezifische Risiken

Einige wenige Hersteller dominieren einzelne Märkte für bestimmte Typen digitaler Produkte oder Subkomponenten (z.B. Prozessoren, WLAN Chips, Adapter usw.). Die Folge ist eine Konzentration von Anreizen für Angreifer. Ein Angriff auf dominierende Hersteller hat weitreichende Konsequenzen.

Die Notwendigkeit gerätespezifischer Prüfungen ergibt sich auch aus dem Umstand, dass die meisten digitalen Infrastrukturen von einer Vielzahl von Lieferanten unterschiedlicher Herkunft bedient werden. Komponenten sowie Subkomponenten werden üblicherweise in einer komplexen Lieferkette gefertigt, welche kaum verständlich und kontrollierbar ist. Die wachsende Komplexität der Lieferkette wird so zur erheblichen Bedrohung für die digitale Gesellschaft.

1.2.6 Schwachstellenprüfungen aus der Sicht potenzieller Angreifer

Die Prüftätigkeit liesse sich ebenso auf spezifische Risiken und Gefährdungen konzentrieren, wie sie sich aus der Art des Angriffs bzw. der Bedrohung ergeben. Zur Identifikation und Beurteilung von Verwundbarkeiten müssen Firmen, Organisationen und Staaten aus der Sicht eines versierten Angreifers betrachtet werden: Wie kann dieser maximalen Einfluss und die grösste Persistenz gewinnen bei gleichzeitig kleinster Detektionswahrscheinlichkeit.[14] Die Kompromittierung digitaler Produkte vor deren Auslieferung, also während des

Designs, der Herstellung oder innerhalb der Lieferkette, erfüllt diese Anforderungen.

Legt man den Fokus auf Hardware/Firmware bzw. die Lieferkette, so sind staatliche Angreifer besonders zu betrachten. Sie verfügen über überdurchschnittliche Ressourcen und den langen Atem, um ein Ziel persistent über mehrere Angriffskanäle und lange Zeiträume unentdeckt zu erreichen. Im Unterschied zu privaten Cyber-Kriminellen und anderen Angreifern können Staaten sich direkten Zugriff auf kritische Teile der Infrastruktur des Internets verschaffen, systematisch und umfangreich den Internetverkehr überwachen und Dienstanbieter oder Hersteller gar per Gesetz zur Überwachung oder Mitarbeit zwingen.[15]

1.2.7 Update-Mechanismen

Ein weiteres Feld für Prüfungen sind die Entwicklung, Implementierung und Dokumentation/Archivierung von sicheren und skalierbaren Update-Mechanismen. Während der gesamten Lebensdauer eines digitalen Produkts werden Security-Updates vom Hersteller benötigt. Viele digitale Produkte haben eine Lebensdauer von Jahrzehnten (z. B. Stromzähler, Kontrollsysteme) und Ersatz ist oft kaum möglich oder zu teuer (z.B. nach Konkurs des Herstellers). Wenn die Möglichkeit der Weiterentwicklung und die Bereitstellung von Updates nicht via Open Source garantiert werden können, könnte die Prüfinstanz die Rolle der «Trusted Third Party» übernehmen und Themen wie «Coordinated Disclosure» für sich beanspruchen. Dafür sind nicht nur technische und juristische Kompetenz nötig, sondern auch Vertrauen der Beteiligten und vor allem Neutralität und öffentliche Glaubwürdigkeit.

2 Bestehende Normierungs-, Prüf- und Zertifizierungslandschaft

2.1 Normierungs- und Prüfungslandschaft in der Schweiz

2.1.1 Aktuelle Situation

Als bestehende Organisationen und Institutionen mit ähnlichen Prüfaufgaben im öffentlichen Interesse werden einerseits die Entwickler bzw. Verwalter des weltweit abgestimmten Common Criteria-Standards (ISO/IEC 15408) genannt und andererseits aber auch Einrichtungen wie das Schweizerische Heilmittelinstitut *swissmedic* sowie Prüfinstanzen im Bereich des Verkehrs und der Luftfahrt. Dass diese Institutionen die Zuständigkeit für Prüfungen im Cyber-Bereich nicht schon längst für sich reklamierten, kann an der Trägheit grosser/traditioneller Organisationen bzw. an mangelndem Wissen über die Auswirkungen von Cyber-Angriffen liegen. Zudem sind Prüfungen im Cyber-Bereich ausserordentlich komplex und ändern sich die Problemstellungen sehr rasch. In verschiedenen Branchen beginnt sich die Situation neuerdings zu bewegen (siehe z.B. Electrosuisse Schweiz). Auch einzelne Firmen lassen ihre vernetzten Geräte vermehrt auf Sicherheitsfragen hin überprüfen, was jedoch bislang auf Eigeninitiative geschieht und wenig Verbreitung findet (als Beispiel seien genannt: Transport- und Beförderungsmittel, die Luftfahrt sowie vernetzte Werkzeuge und Kaffeemaschinen). Auch in der Autoindustrie werden die bestehenden Prüfinstanzen wohl vermehrt ein Auge auf die Cybersicherheit haben und ihre Befunde im Sinne des öffentlichen Interesses veröffentlichen.

Übereinstimmend fordern die Experten eine Anpassung an bestehende Normierungen für Cybersecurity, insbesondere an EU-Standards und die entsprechende Zusammenarbeit mit europäischen Gremien. Die meisten schweizerischen Hersteller verkaufen auch in die EU und viele in der Schweiz angebotene Produkte – insbesondere in den Bereichen Industrie 4.0 und IoT – kommen aus der EU. Die Schweiz tut gut daran, Bestehendes und Erprobtes nicht neu zu erfinden, sondern sich mit den umliegenden Aktivitäten zusammenzuschliessen. Eine europäische Prüfinstanz schliesst eine entsprechende schweizerische Einrichtung nicht aus. Aufgrund der ohnehin knappen personellen Ressourcen im Cyber-Bereich ist auch für die Prüfungen eine Zusammenarbeit sinnvoll, z.B. indem gewisse Geräte im Herstellungsland getestet werden und die Ergebnisse dann von anderen Prüfinstituten übernommen werden. Ein «Swiss-Finish» ist auch in diesem Bereich denkbar, indem die Möglichkeit umgesetzt wird, strengere Vorschriften (z.B. auch für bestimmte Branchen oder kritische Infrastrukturen) einzuführen oder auf für die Schweiz spezifische Prüfdimensionen und Fragestellungen einzugehen, die vom Ausland aufgrund anderslautender Anforderungen nicht berücksichtigt wurden.

Prüfergebnisse von ausländischen Prüfstellen sollten grundsätzlich anerkannt werden, sofern eine anerkannte Akkreditierung existiert oder eine Anerkennung der Prüfqualität gewährleistet werden kann. Die Experten gehen davon aus, dass sich die Schweiz der Europäischen Normierung anpasst, sobald eine solche besteht. Trotzdem gilt es, auf schweizerische Besonderheiten und Interessen – darunter auch zukünftige, heute noch unbekannte – eingehen zu können, sofern diese eine eigene Prüfinstanz rechtfertigen (vgl. z.B. die schweizerischen Label für Nahrungsmittel).

2.1.2 Normierung / Label / Gütesiegel

Seit November 2019 vergibt der «Schweizer Verband für das Cyber-Sicherheitsgütesiegel» ein Cyber-Security-Gütesiegel «cyber-safe» an KMU.[16] Das Gütesiegel soll Anwendern zeigen, dass ein KMU die für ein akzeptables Risiko nötigen Schritte unternimmt und es so einen Wettbewerbsvorteil für das Unternehmen darstellt. Hierbei geht es nicht um die Prüfung von Geräten und Komponenten, sondern um die Unternehmenssicherheit, also um die Mitarbeitenden und die unternehmenseigene IT.

Die Genfer Stiftung «Swiss Digital Initiative» (SDI) propagiert das «Swiss Digital Trust Label» für digitale Dienste wie Apps und Websites, sofern diese vertrauensbildende Kriterien erfüllen.[17] Im Vordergrund der Genfer Initiative steht die Orientierung der Nutzer zu Fragen der Transparenz, dem Umgang mit Daten, der Sicherheit und der Verlässlichkeit. Es geht dabei nicht um die technische Sicherheit im holistischen Sinn, sondern um die Einhaltung ethischer Grundsätze in Software und Dienstleistungen, sowie um die Einhaltung ethischer Verhaltensregeln von Unternehmen mit digitalem Dienstleistungsangebot. Hard- und Firmware sind nicht im Fokus. Am WEF 2020 wurde die Initiative förmlich der Öffentlichkeit vorgestellt.

Der Fachverband Electrosuisse[18] arbeitet an einem Diskussionspapier für eine Regulierung der Cyber-Security in der Schweiz.[19] Ziel ist es, Cyber-Security-Normen für informationstechnische Produkte und Dienste verpflichtend und Risiken für die Anwender transparent zu machen.

Erarbeitet wird nichts weniger als ein umfassendes schweizerisches System mit Gesetzen und Verordnungen und definierten Normen, auf deren Basis Prüfungen und Zertifizierungen durchgeführt und eine entsprechende Ausbildung organisiert werden können. Der Entwurf sieht in diesem Sicherheitssystem für die vernetzte Welt, das mit der Sicherheit im Strassenverkehr oder bei elektrotechnischen Produkten verglichen wird, eine gemeinschaftliche Aufgabe von Bund, Kantonen, Wissenschaft, Wirtschaft und Gesellschaft vor. Vereinzelte Bestimmungen im Bereich Datenschutz, Schutz der Privatsphäre und Kommunikation werden als ungenügend beurteilt. Vielmehr soll mit einer einheitlichen Regelung der Cyber-Sicherheit über alle Anwendungsbereiche der Informations- und

Kommunikationstechnologie verhindert werden, dass in einzelnen Teilbereichen unterschiedliche Regelungen entstehen. Mit dem Diskussionspapier sollen die Grundlagen für die gesetzlichen/regulatorischen Rahmenbedingungen für Cyber-Sicherheit in der Schweiz geschaffen werden. Das Papier will die Anforderungen für eine solche ganzheitliche gesetzliche Grundlage für digitale Sicherheit definieren.

Wie im vorliegenden Bericht zum Cyber-Sicherheits-Prüfinstitut weist das Electrosuisse-Papier darauf hin, dass in der Schweiz mit dem Datenschutzgesetz allein keine hinreichende gesetzliche Grundlage für digitale Sicherheit besteht, während die Europäische Union 2016 mit der Datenschutzgrundverordnung (DSGVO) und der Richtlinie zur Netz- und Informationssicherheit (NIS) sowie 2019 mit dem EU Cybersecurity Act (CSA) entsprechende Grundsteine gelegt hat.

Weil Cyber-Sicherheit ein Querschnittsthema ist, konnte nach Auffassung von Electrosuisse in der Schweiz bisher keine Organisation die Führung für das Thema übernehmen. In der Schweiz existiert keine Normenorganisation für Cyber-Sicherheit wie SWISSMEM für die Maschinen- und Metallindustrie, SIA für das Bauwesen, VSS für das Strassen- und Verkehrswesen, FH für die Uhrenindustrie, Electrosuisse für die Elektrotechnik und asut für die Telekommunikation. Das Papier wendet sich – wie auch das erwähnte White Paper der Arbeitsgruppe Supply-Chain der Cybersecurity-Kommission von ICTswitzerland – gegen das Argument, ein Alleingang der Schweiz bezüglich einer Cyber-Regulierung hätte keine Aussicht auf Erfolg und würde die Schweiz womöglich isolieren. Der Autor weist daraufhin, dass in verschiedenen anderen sicherheitsrelevanten Bereichen international harmonisierte technische Normen bestehen, zu denen die Schweiz bislang häufig als Pionier von Sicherheitsstandards beigetragen hat. Eine solche Pionierfunktion könnte sie auch bezüglich Cyber-Sicherheit wahrnehmen (siehe dazu auch die Ausführungen zur SDI).

Ebenso deckt sich das Papier mit der hier mehrfach unterstrichenen Einschätzung, dass mit der raschen Verbreitung von vernetzten, «smarten» IoT-Produkten, bei denen Komfortfunktionen und der Kostendruck zu Lasten der Cyber-Sicherheit gehen, die Angriffsziele für Cybercrime massiv zunehmen. Diese Geräte stellen damit eine bislang stark unterschätzte Bedrohung für alle anderen Netzteilnehmer dar.

Das Electrosuisse-Papier hält die bisherigen Abwehr- und Sicherheitsbemühungen im Cyberbereich für stark ungenügend. Punktuelle Patches und einzelne freiwillige Zertifizierungen nach ungenügend definierten Standards würden ein falsches Gefühl der Sicherheit erzeugen. Auch eine Fokussierung auf Produkte in kritischen Infrastrukturen würde zu kurz greifen. Deshalb werden nichts weniger als ein «Paradigmenwechsel und ein Quantensprung bei der Cyber-Sicherheit» gefordert.

Das Electrosuisse-Papier listet dann eine Reihe von – sehr ambitionierten – Zielen auf, die mit einer geeigneten Regulierung erreicht werden sollen.[20] Im Papier werden dann die aufgeführten Bestimmungen und Verordnungen im Einzelnen erläutert. Der Autor passt dabei nach eigener Angabe verschiedene Elemente aus dem EU Cybersecurity Act und dem Referentenentwurf zu Deutschlands IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) vom 27.03.2019 auf die Schweizer Tradition und Verhältnisse an.

Besonderes Gewicht legt das Electrosuisse-Papier auf die Schaffung eines zweiteiligen Cyber-Security-Labels, das einerseits auf einer obligatorischen Selbstdeklaration der Hersteller und Dienstanbieter und andererseits auf einer freiwilligen Zertifizierung beruht. Dazu würde die Korrektheit der Selbstdeklaration von einer unabhängigen und akkreditierten Prüfstelle beurteilt. Zur Umsetzung wurde ein Vorschlag für die Prüfprozesse und -organisation beschrieben.

Beurteilt bzw. geprüft werden sollen dabei die folgenden Aspekte der Cyber-Sicherheit:

- Security by Design & Default
- Transparenz bezüglich Risiken
- Systemsouveränität für Systemeigner
- Datensouveränität für Benutzer
- Umsetzung von Sicherheitsgrundsätzen
- Normenkonformität
- Schwachstellenfreiheit bezüglich bekannter Schwachstellen
- Sicherstellung des Security-Supports

Entsprechend der geforderten Regulierung schlägt Electrosuisse die Schaffung und Involvierung verschiedener Institutionen vor:

- Eine unabhängige Zertifizierungsstelle, die auf Basis eines Prüfberichts einer akkreditierten Prüfstelle das Zertifikat für ein «Cyber-Security-Label» erteilt.
- Mit der Schweizerischen Akkreditierungsstelle (SAS) besteht in der Schweiz bereits eine Akkreditierungsorganisation zur Akkreditierung von Prüflaboratorien (nach SN EN ISO/IEC 17025 bzw. SN EN ISO 15189) und Inspektionsstellen (nach SN EN ISO/IEC 17020).
- Neu soll eine zentrale Aufsichtsstelle geschaffen werden, die die Konformitätsbewertungsstellen (Prüfstellen, Zertifizierungsstelle usw.) überwacht.

2.2 Bestandsaufnahme ausgewählter Länder

Die Situation der Cyber-Prüfinstanzen in Deutschland, Frankreich, Österreich, UK, den USA und Finnland wird anhand der folgenden Gliederung beschrieben:

- Institutionell/organisatorische Verortung der Einrichtung (Teil eines Ministeriums, eigene Behörde, staatliche oder private oder gemischtwirtschaftliche Organisation).
- Umfang desjenigen Teils der Einrichtung, der sich mit Prüfung bzw. Evaluierung bzw. Zertifizierung von Cyber-Produkten befasst (Personal, Mittel, Kompetenzen).
- Leistungsspektrum: Verhältnis der eigentlichen Instanz zur Prüfstelle bzw. zu den Prüfstellen im engeren Sinne: Welche Leistungen werden von der Prüfstelle erbracht, welche ausgelagert?
- Scope: Was wird alles geprüft/evaluiert/zertifiziert, was sind die Abgrenzungskriterien?

Im Anschluss wird die besondere Rolle der Europäischen Union beschrieben, insbesondere im Hinblick auf den «Cybersecurity Act» in Form der neuen Verordnung (EU) 2019/881.

2.2.1 Deutschland

2.2.1.1 Institutionelle Verortung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist in Deutschland für die IT-Sicherheitszertifizierungen von IT-Produkten und -Systemen zuständig und entwickelt die dafür benötigten Prüfkriterien bzw. Grundlagen. Das BSI ist eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Am Hauptsitz in Bonn arbeiten rund 1000 Mitarbeitende. Das BSI besteht aus 8 Abteilungen, jede beinhaltet 1 bis 3 Fachbereiche. Der Etat des BSI beläuft sich auf € 117,8 Mio. (2018).[21]

Die Abteilung Standards und Zertifizierung (SZ) ist im BSI für dieses Thema verantwortlich. Sie gliedert sich in die beiden Fachbereiche SZ 1 und SZ 2 mit jeweils mehreren untergeordneten Referaten.[22]

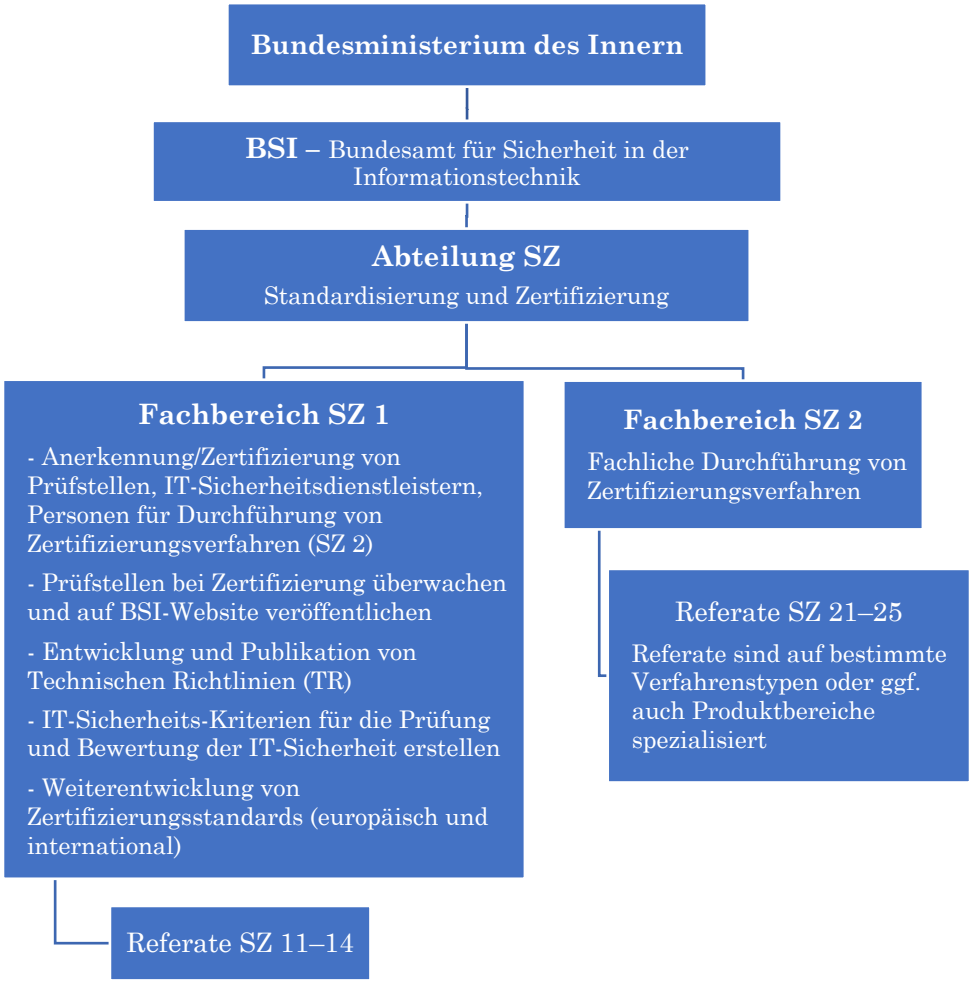


Abbildung 1: Organisation BSI im Bereich Standardisierung und Zertifizierung (eigene Darstellung)

2.2.1.2 Verhältnis Prüfinstanz – Prüfstelle

Die vom BSI verlangten und überwachten Prüfungen werden fast ausschliesslich von kommerziellen Prüfstellen durchgeführt. An einer Produktzertifizierung sind somit folgende Parteien beteiligt:[23]

- Der **Antragsteller** (in der Regel Hersteller) wählt eine Prüfstelle aus und beantragt die Prüfung bei der Zertifizierungsstelle des BSI. Er stellt die erforderlichen Nachweise zum Prüfgegenstand bereit und erhält nach erfolgreichem Abschluss des Verfahrens die Konformitätsurkunde, z.B. das Deutsche IT-Sicherheitszertifikat des BSI. Er entschädigt sowohl die Prüfstelle und entrichtet dem BSI eine Gebühr.
- Die **Prüfstelle** wird von der Anerkennungsstelle des BSI überwacht und auf der BSI-Website gelistet. Die Anerkennung einer Prüfstelle bezieht sich immer auf einen konkreten Anerkennungsbereich, z.B. ein Kriterienwerk (ITSEC oder CC oder ggf. Teile davon), ein spezifisches technisches Gebiet oder eine Technische Richtlinie (TR).[24] Die Prüfstelle prüft und bewertet (im Folgenden: evaluiert) die IT-Produkte gemäss den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien auf Funktionsfähigkeit und potenzielle Schwachstellen. Sie stellt der BSI-Zertifizierungsstelle sowie dem Antragsteller die vollständigen Prüfergebnisse zur Verfügung.
- Die **BSI-Zertifizierungsstelle** berät den Antragsteller in Verfahrensfragen, unterstützt ihn bei der Erarbeitung der Sicherheitsvorgaben und begleitet bzw. überwacht die Evaluierungsaktivitäten der Prüfstelle und nimmt die Prüfberichte der Prüfstellen ab. Insbesondere wird jede Evaluierung durch Mitarbeitende der Zertifizierungsstelle begleitet mit dem Ziel, eine einheitliche Vorgehensweise und Methodik sicherzustellen. Es erfolgt hierbei ein Abgleich der Bewertungen mit denen aus anderen Zertifizierungsverfahren.[25] Die Zertifizierungsstelle erstellt dann den Prüfreport und erteilt mit Prüfabnahme die Konformitätsurkunde. Nach Einvernehmen mit dem Antragsteller veröffentlicht sie den Prüfreport samt Konformitätsurkunde auf der Website des BSI.

Im Zertifizierungsreport sind unter anderem das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht enthalten. Der Zertifizierungsbericht beinhaltet die sicherheitstechnische Beschreibung des zertifizierten Produktes, die Einzelheiten der Bewertung und Hinweise für den Anwender.

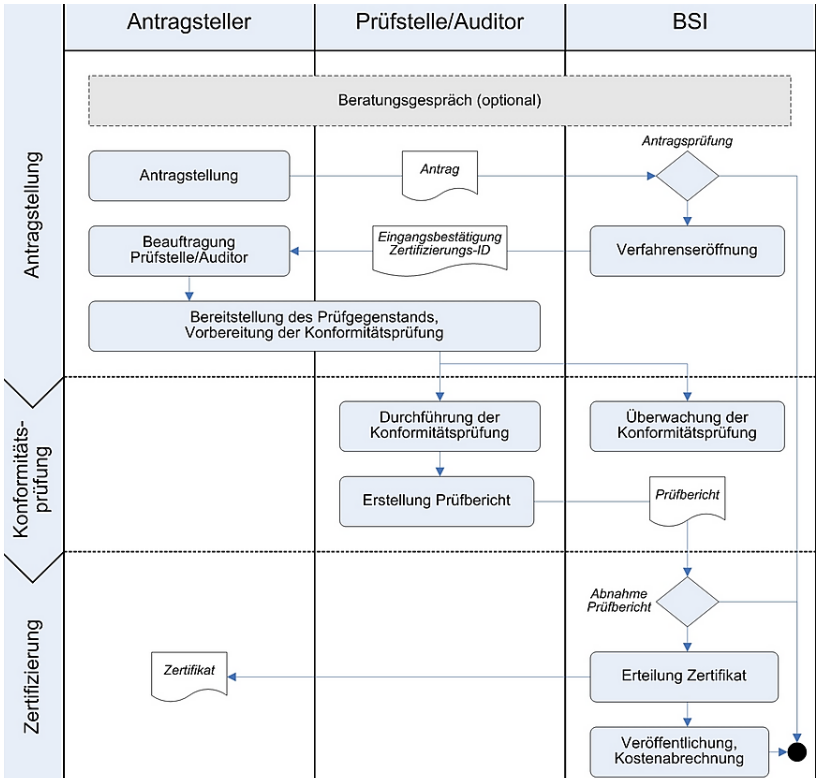


Abbildung 2: Zertifizierung nach technischen Richtlinien (Quelle: https://www.bsi.bund.de/SharedDocs/Bilder/DE/BSI/Themen/Zertifizierung/Verfahrensablauf_Zert-TR.jpg)

2.2.1.3 Was wird wonach geprüft?

Das BSI unterscheidet verschiedene Arten der Zertifizierung:

Im Programm **IT-Sicherheitszertifizierung Common Criteria (CC)** werden IT-Produkte (Software/Hardware) z.B. aus folgenden Produktkategorien zertifiziert:

- Betriebssysteme
- Digitale Signaturen
- Digitale Tachographen
- Gesundheitswesen
- Intelligente Messsysteme
- Netzwerk- und Kommunikationsprodukte
- Serveranwendungen
- Smartcards und ähnliche Produkte

Im Programm **Technische Richtlinien (TR)** werden IT-Produkte zertifiziert, die mit dem Aufbau oder der Absicherung von IT-Systemen zu tun haben, insbesondere IT-Produkte und -systeme, die für den Einsatz in hoheitlichen und

damit sicherheitskritischen Bereichen der Bundesrepublik Deutschland vorgesehen sind, z.B. Produkte aus folgenden Kategorien:

- Beweiswerterhaltende Langzeitspeicherung
- eHealth-Kartenprodukte
- Router
- Kontaktlose Chipkarten und Lesegeräte
- Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme

Seit Oktober 2018 bietet die **Beschleunigte Sicherheitszertifizierung (BSZ)** (als Alternative zur CC-Zertifizierung) die Möglichkeit, die Sicherheitsaussage eines Produktes durch ein Zertifikat bestätigen zu lassen. Die Evaluierung des Produktes erfolgt ebenfalls durch vom BSI anerkannte Prüfstellen. Die BSZ ist weniger flexibel als die Zertifizierung nach CC, bietet dafür besser planbare Evaluierungslaufzeiten und verursacht einen geringeren Dokumentationsaufwand. Die Prüfungen fokussieren auf die sicherheitstechnische Robustheit des Produktes. Explizit vorgedacht ist die Aufrechterhaltung eines Zertifikates bei Produktupdates.[26]

Die gegenseitige Anerkennung von Zertifikaten mit anderen europäischen Zertifizierungsstellen (insbesondere mit dem CSPN-Verfahren der französischen ANSSI) ist ein erklärtes Ziel. Zudem soll die neue beschleunigte Sicherheitszertifizierung (BSZ) in den Cybersecurity Act der EU integriert werden.

Neben den erwähnten drei Zertifizierungsschemen bietet das BDI noch weitere Prüfverfahren an:

Zertifizierung von Standorten

Neben Produkten können auch Entwicklungs- und Produktionsstandorte für IT-Produkte nach Common Criteria separat evaluiert und zertifiziert werden. Ziel einer solchen Standortzertifizierung ist meistens die Wiederverwendung des Ergebnisses in späteren Zertifizierungsverfahren für IT-Produkte, die an diesem Standort entwickelt oder produziert werden.[27]

IT-Sicherheits-Gütesiegel

Ein vom BSI ausgestelltes IT-Sicherheits-Gütesiegel soll Anwendern dabei helfen, das Sicherheitsniveau eines Produktes tatsächlich beurteilen zu können. Ausserdem hofft man, dass mit dem freiwilligen Gütesiegel ein gewisser Druck auf diejenigen Hersteller ausgeübt wird, für die das Siegel aufgrund mangelnder Sicherheit in weiter Ferne ist. Durch mehr Transparenz für die Verbraucher sollen diese animiert werden, zukünftig doch mehr in die Sicherheitseigenschaften ihrer Produkte zu investieren.[28]

2.2.1.4 Zertifizierungspflicht

Grundsätzlich erfolgt die Zertifizierung auf Wunsch eines Herstellers oder Anbieters von IT-Produkten und -Systemen. Es gibt aber auch Verordnungen, die explizit eine Zertifizierung verlangen. Die Forderung nach zertifizierten Produkten wurde in den letzten Jahren in zahlreichen Gesetzen und Verordnungen verankert, sodass Hersteller und Anbieter von IT-Produkten, die neben den kritischen Infrastrukturen von besonderem nationalem Interesse sind, stärker in die Pflicht genommen werden. Das BSI geht davon aus, dass die Zertifizierungspflicht in Zukunft deutlich ausgeweitet wird. Vielfach betrifft dies die Digitalisierungsprojekte der Bundesregierung, z.B. in den Bereichen eHealth, hoheitliche Dokumente und Smart Metering und seit vielen Jahren auch die digitale Signatur. Beispielsweise wird in der seit Mitte 2016 gültigen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-Verordnung (EU) Nr. 910/2014) die Zertifizierung für IT-Produkte zur Erzeugung von digitalen Signaturen verlangt.[29]

2.2.2 Frankreich

2.2.2.1 Institutionelle Verortung

In Frankreich ist die nationale Behörde ANSSI («Agence Nationale de la Sécurité des Systèmes d'Information») für die Beaufsichtigung der Ausstellung von Sicherheitszulassungen (Zertifizierung und Qualifizierung) für vertrauenswürdige Produkte und Dienstleister im Namen des Premierministers zuständig. Der Teil *Zertifizierung* ist ein Unterbereich der Behörde. Die ANSSI ist dem «Secrétariat Général de la Défense et de la Sécurité Nationale» (SGDSN) angegliedert. Das SGDSN unterstützt den Premierminister im Bereich der nationalen Verteidigung und Sicherheit. Die ANSSI verfügt über rund 600 Mitarbeitende und über ein Budget von € 100 Mio. Die Zertifizierung ist in der Sous-Direction Expertise (SDE) in der Division «Produits et Services de Sécurité» angesiedelt.[30]

2.2.2.2 Verhältnis Prüfinstanz – Prüfstelle

Das «Centre de Certification National» der ANSSI ist für den Evaluationsprozess, die Einhaltung der Kriterien und für die Zulassung der privaten Labore, die die Evaluation durchführen, zuständig. Diese Labors werden als «Centre d'Evaluation de la Sécurité des Technologies de l'Information» (CESTI) bezeichnet.[31] Ein CESTI besteht aus einem Team von Fach- und Führungskräften, die meist in ein grösseres Unternehmen integriert sind. Die Akkreditierungskriterien verlangen, dass das CESTI von den anderen Aktivitäten des Unternehmens, dem es angegliedert ist, getrennt und abgegrenzt ist.[32]

Die ANSSI zertifiziert nach CC oder nach der «Certification de Sécurité de Premier Niveau» (CSPN). Für die Evaluation gemäss CC werden die CESTI vom COFRAC (Comité Français d'Accréditation) akkreditiert nach ISO/IEC 17025 und von der ANSSI zugelassen. Für die Evaluation gemäss CSPN werden die Labors von der ANSSI zugelassen. Für die sogenannte *Qualifikation* begleitet ANSSI den gesamten Prozess, die Evaluation wird aber wiederum von einem CESTI durchgeführt.[33]

2.2.2.3 Was wird wonach geprüft?

Die Zertifizierung gemäss CC oder CSPN kann Cyber-Sicherheitslösungen und, allgemeiner gesagt, alle digitalen Lösungen betreffen, die Sicherheitsfunktionen bieten, z.B. VPN- und Firewall-Netzwerkprodukte, Smartcards, HSM, Trusted Execution Environments, Produkte für industrielle Systeme (PLC, SCADA-Server) usw.[34]

Die über die Zertifizierung hinausgehende *Qualifizierung* beinhaltet eine Empfehlung der ANSSI, die die Vertrauenswürdigkeit eines Sicherheitsproduktes und seines Herausgebers attestiert. Von der ANSSI wird seit 2018 zudem das Gütesiegel «Visa de Sécurité» vergeben. Dieses basiert auf einer Zertifizierung

nach CC, CSPN oder einer Qualifikation und unterstützt französische Unternehmen bei ihrer Wahl nach Lösungen.

Zertifizierung nach CC

Nach CC zertifizierte Produkte gehören zu folgenden Kategorien:[35]

- Cartes à puce (Smart Cards)
- Chronotachygraphe numérique (digitale Fahrtenschreiber)
- Micro-circuits (Mikroschaltkreise)
- Produits réseaux (Netzwerkprodukte)
- Profil de Protection – Ordinateur personnel et serveur (PC und Server)
- Systèmes (IT-Systeme)

Zertifizierung gemäss CSPN

CSPN ist eine von ANSSI geschaffene Zertifizierung, die weniger lang dauert und weniger kostet als die CC-Zertifizierung. Das Ziel ist, diese derzeit rein französische Kennzeichnung in Zukunft auf europäischer Ebene anzuerkennen.[36] Nach CSPN zertifizierte Produkte gehören zu folgenden Kategorien:

- Effacement de données (Datenlöschung)
- Stockage sécurisé (sichere Speicherung)
- Systèmes d'exploitation et de virtualisation (Betriebs- und Virtualisierungssysteme)
- Pare-feu (Firewall)
- Détection d'intrusions (Intrusionsdetektion)
- Anti-virus, protection contre les codes malveillants (Antivirus und Schadsoftwareschutz)
- Administration et supervision de la sécurité (Sicherheitsverwaltung und -überwachung)
- Identification, authentification et contrôle d'accès (Identifizierung, Authentifizierung und Zugriffskontrolle)
- Communication sécurisée (sichere Kommunikation)
- Messagerie sécurisée (sichere Nachrichtenübermittlung)
- Matériel et logiciel embarqué (eingebettete HW und SW)
- Environnement d'exécution sécurisée (sichere Betriebsumgebung)
- Automate programmable industriel (speicherprogrammierbare Steuerung)
- Commutateur industriel (industrieller Schalter)
- SCADA

Qualification

Über die einfache Zertifizierung hinausgehend ist die *Qualification* mit einer Empfehlung der ANSSI verbunden und attestiert die Vertrauenswürdigkeit, die der französische Staat einem Sicherheitsprodukt und seinem Herausgeber

bescheinigt. Sie bescheinigt die Einhaltung der von der ANSSI geförderten regulatorischen, technischen und die Sicherheit betreffenden Anforderungen, indem sie eine Garantie für die Robustheit des Produkts und die Kompetenz des Dienstleisters sowie die Verpflichtung des Lösungsanbieters zur Einhaltung der Vertrauenskriterien bietet. Für die Produkte bestehen drei Qualifikationsniveaus, die jeweils ein Sicherheitsniveau und die Einhaltung der Vertrauenskriterien bescheinigen: elementar, Standard und verstärkt.

Die im Vergleich zur Zertifizierung strengere *Qualification* betrifft alle Produkte und Dienstleistungen im Bereich der Cyber-Sicherheit, insbesondere solche, die in erster Linie von der Verwaltung und von Betreibern kritischer Infrastrukturen verwendet werden.[37]

Sicherheitssiegel «Visa de Sécurité»

Seit Anfang 2018 wird von der ANSSI das «Visa de Sécurité» vergeben, ein Label, das die Sicherheit von Cyber-Security-Produkten und -Dienstleistungen bezeugt und damit Lösungen auszeichnet, die vom französischen Staat nach strengen Tests und einer genauen Analyse als zuverlässig und vertrauenswürdig anerkannt werden. Die Spezifikationen für das Visa de Sécurité werden von der ANSSI festgelegt. Es dient einerseits Nutzern als Orientierungshilfe und gibt andererseits Lieferanten Zugang zu einem spezifischen Markt (z.B. für den Einsatz in kritischen Infrastrukturen). Unterschieden wird zwischen dem strengeren Visa de Sécurité für *qualifizierte* Produkte und jenem für *zertifizierte* Produkte.[38] Die ANSSI stellt einen Entscheidungsbaum zur Verfügung, mit dessen Hilfe Anbieter von IT-Produkten und deren Anwender entscheiden können, in welchem Fall die Zertifizierung und in welchem eine Qualifikation sinnvoll ist.

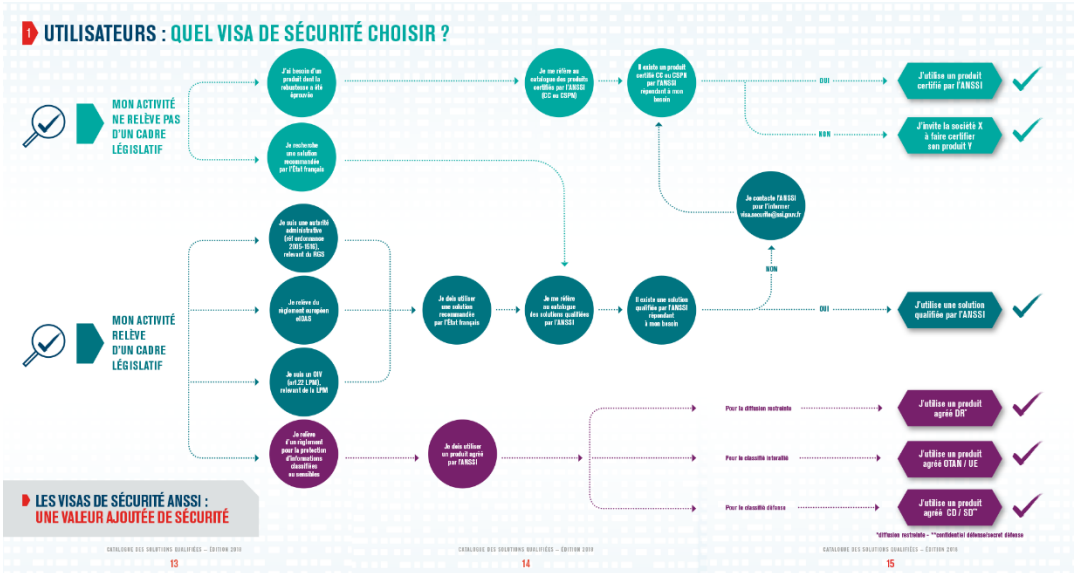


Abbildung 3: Entscheidungsbaum für Visa de Securité (Quelle: https://www.ssi.gouv.fr/uploads/2018/01/visasecu_2017_schema_utilisateurs_p13.png)

2.2.3 Österreich

2.2.3.1 Institutionelle Verortung

In Österreich ist die 2015 vom Bundeskanzleramt ins Leben gerufene «Cyber Security Plattform» (CSP) für Cyber-Security-Fragen zuständig. Die CSP ist als PPP organisiert und stellt eine zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung dar, mit besonderem Fokus auf die kritischen Infrastrukturen. Mit ihren Interessensvertretern aus Verwaltung, Wirtschaft und Wissenschaft erfüllt die CSP folgende Aufgaben:

- Informationsaustausch zu wesentlichen Fragen der Cyber-Sicherheit.
- Initiierung von Kooperationen zwischen den beteiligten Partnern in den Bereichen Sensibilisierung und Ausbildung sowie Forschung und Entwicklung.
- Beratung und Unterstützung der «Cyber-Sicherheit-Steuerungsgruppe».
- Förderung der Errichtung von Sektor-spezifischen Computer Emergency Response Teams (CERT).
- Dachorganisation für bereits bestehende Kooperationsformate (unter anderem: Kuratorium sicheres Österreich, Austrian Trust Circle, Cyber-Sicherheit-Forum, Zentrum für sichere Informationstechnologie Austria (A-SIT), Cyber-Security Austria, CERT-Verbund.[39]

Die CSP setzt sich organisatorisch zusammen aus dem Plenum, den Arbeitsgruppen (AG) und dem Sekretariat der CSP. Sie trifft sich 1- bis 2-mal jährlich im Plenum – bevorzugt im Rahmen von etablierten Veranstaltungen im Bereich der IKT.

In den Umkreis der CSP gehört auch die von der Hochschule St. Pölten betriebene Beschaffungsplattform (www.it-sicher.kaufen). Unter verschiedenen Produktekategorien (z.B. Router, Internet Browser, Antivirus usw.) werden dort vertrauenswürdige Hersteller/Lieferanten aufgelistet.

2.2.3.2 Verhältnis Prüfinstanz – Prüfstelle

Aktuell beschäftigt sich eine Arbeitsgruppe «Standardisierung» mit der Entwicklung von Mindestsicherheitsstandards im Bereich von IKT-Produkten. Die Arbeitsgruppe mit Fachleuten aus Industrie und Forschung hat eine erste **Anforderungsliste** erarbeitet, die Mindeststandards definiert und beispielsweise von Beschaffungs-/Einkaufsabteilungen bei der Ausschreibung von IKT-Produkten verwendet werden kann.

Diese Mindeststandards werden derzeit in eine Arbeitsgruppe der ENISA (Europäische Agentur für Netz- und Informationssicherheit) eingebracht und auf breiter Basis mit anderen Mitgliedsstaaten diskutiert. Man will daraus ein europäisches Rahmenwerk schaffen, welches auch im Rahmen der European Cyber-

Security-Organisation (ECSO) als Basis für zukünftige europäische Standards eingebracht werden soll.

In Österreich ist das **Zentrum für Sichere Informationstechnologie Austria** (A-SIT) seit Dezember 2016 als Konformitätsbewertungsstelle Produktzertifizierungsstelle akkreditiert.[40] A-SIT wurde im Jahr 1999 als gemeinnütziger Verein gegründet und wird privatwirtschaftlich als Kompetenzzentrum für IT-Sicherheit geführt. Hauptaufgabe der Konformitätsbewertungsstelle ist, Anbieter von Vertrauensdiensten (darunter unter anderen auch die Swisscom) anhand der Anforderungen der eIDAS-Verordnung und darauf basierender europäischer Normen zu überprüfen.[41]

Im Juli 2015 wurde die A-SIT Plus GmbH gegründet, die Leistungen zur technischen Informationssicherheit sowohl öffentlichen wie auch privatwirtschaftlichen Organisationen anbietet.

2.2.3.3 Campus Graz

Der Schweizer Warenprüfkonzern SGS gründete zusammen mit der technischen Hochschule Graz einen Cyber-Security Campus. Im Campus Graz sollen Forschung, Ausbildung sowie Produktprüfung und -zertifizierung angesiedelt werden. Geplant ist ein 7000-Quadratmeter-Gebäude für ein Forschungszentrum sowie ein Prüf- und Zertifizierungslabor für Cyber-Security der SGS-Gruppe.[42] Der Start des Campus erfolgt mit 120 Mitarbeitenden, im Vollbetrieb sollen rund 400 Personen in Graz arbeiten.

2.2.4 United Kingdom

2.2.4.1 Institutionelle Verortung

Das «National Cyber-Security Centre» (NCSC) ist für die Zertifizierung von Produkten in UK verantwortlich. Dieses ist dem «Government Communications Headquarters» (GCHQ) angegliedert, der grossen und bedeutenden Nachrichten- und Geheimdienstorganisation, die zum Verantwortungsbereich des Aussenministers, d.h. des «Secretary of State for Foreign and Commonwealth Affairs», gehört.[43]

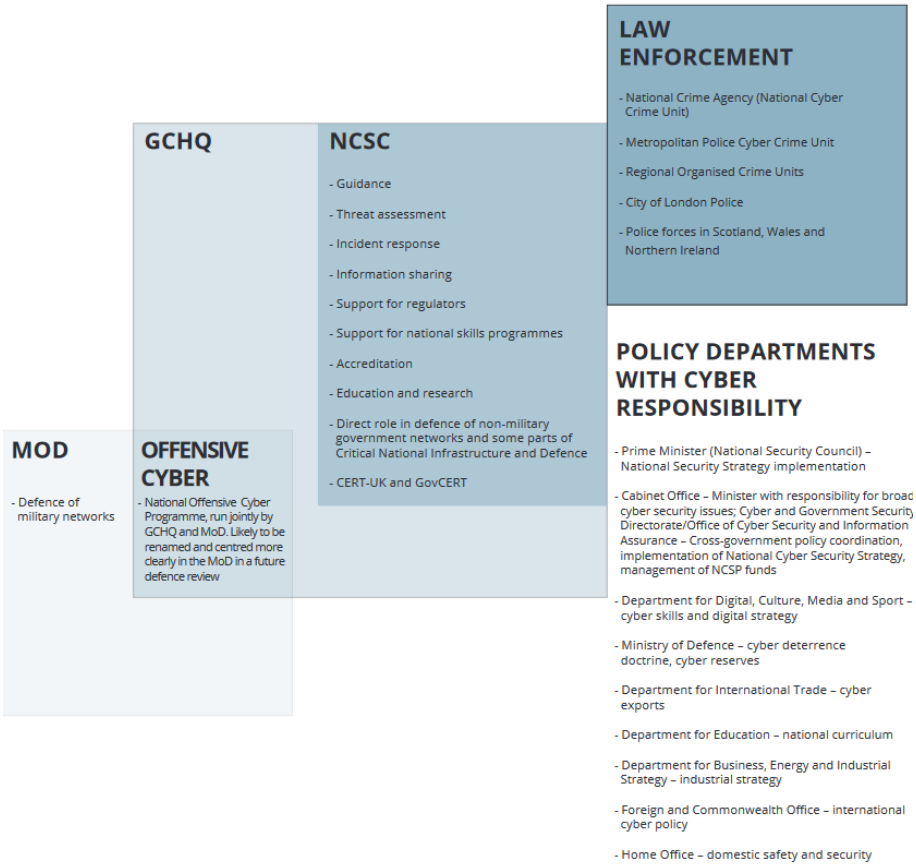


Abbildung 4: Organisation und Verantwortlichkeiten des Cyberbereichs in UK (Quelle: https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf)

2.2.4.2 Verhältnis Prüfinstanz – Prüfstelle

Das NCSC evaluiert die Prüfstellen («Labs») und definiert die Kriterien für die NCSC-Zertifizierung. Die Prüfung der Produkte wird von externen Unternehmen und Labors durchgeführt. Unternehmen können sich als Testlabors bewerben oder auch ihr Produkt beurteilen lassen, um auf der Website aufgeführt zu werden.[44]

2.2.4.3 Was wird wonach geprüft?

Das NCSC stellt eine Liste der geprüften Produkte zur Verfügung. Eine Prüfung kann nach den nachfolgend genannten «Assessment Schemes» erfolgen.

Assisted Products Scheme (CAPS)

Unter diesem Schema werden kryptographische Produkte geprüft, ob sie für den Einsatz in der britischen Regierung die geforderten Standards erfüllen. Es geht um Produkte für den Schutz von als geheim eingestuften Daten der britischen Regierung, z.B. disk encryptors, link and network encryptors, secure radios and access control devices.[45]

Commercial Product Assurance (CPA)

Das CPA betrifft die unabhängige Prüfung kommerzieller Produkte mit sicherheitsrelevanten Funktionen für den öffentlichen Sektor (good for use at OFFICIAL). Mit Hilfe der CPA können Unternehmen nachweisen, dass die Sicherheitsfunktionen ihrer Produkte den NCSC-Standards entsprechen. Die Regierung bzw. der öffentliche Sektor soll so in der Lage sein, diejenigen Produkte zu identifizieren, deren Sicherheit durch unabhängige Tests untermauert wurde. NCSC setzt die Standards fest, die anerkannten Prüfstellen (Labs) nehmen die Prüfungen vor. Der Standard, nach dem getestet wird, nennt sich «Security Characteristics».[46] Der Verkäufer des Produktes muss sich in UK befinden. Das internationale Pendant des CPA ist CC.

CCRA

Per 1. Oktober 2019 hat das NCSC seine Tätigkeit als Zertifikatsproduzent im Rahmen der «Common Criteria Recognition Agreement» (CCRA) eingestellt. Als «Certificate Consuming Participant» wird UK aber weiterhin CCRA-konforme Zertifikate anerkennen, die ein hohes Mass an Vertrauen in die jeweiligen Produkte schaffen.[47]

2.2.5 USA

2.2.5.1 Institutionelle Verortung

In den USA ist die «National Information Assurance Partnership» (NIAP) für die Umsetzung der Common Criteria verantwortlich. Die NIAP ist eine Partnerschaft zwischen dem «National Institute of Standards and Technology» (NIST, Departement of Commerce) und der «National Security Agency» (NSA, Departement of Defence). Sie leitet die Validierungsstelle des NIAP «Common Criteria Evaluation and Validation Scheme» (CCEVS).

2.2.5.2 Verhältnis Prüfinstanz – Prüfstelle

Das CCEVS verwaltet ein nationales Programm zur Entwicklung von «Protection Profiles» (PP), Bewertungsmethoden und Richtlinien, die erreichbare, wiederholbare und prüfbare Anforderungen gewährleisten.

NIAP-Evaluierungen werden von den «Common Criteria Testing Laboratories» (CCTL) durchgeführt. Diese Labors werden im Rahmen des NVLAP-Programms («National Voluntary Laboratory Accreditation Program») von NIAP akkreditiert. Auf der Website der NIAP werden per April 2020 nur 7 solche Labs aufgeführt. Ein Produktanbieter wählt ein zugelassenes Labor, um die Produktbewertung anhand der geltenden PP vorzunehmen.[48]

Die NIAP arbeitet mit der NATO und internationalen Normungsgremien (ISO) zusammen, um Erfahrungen mit der Bewertung nach CC auszutauschen und Doppelarbeit zu vermeiden. Da NIAP ein Mitglied des CCRA («Common Criteria Recognition Arrangement») ist, sind NIAP-Evaluationen gegenseitig in allen CCRA-Mitgliedsstaaten anerkannt.

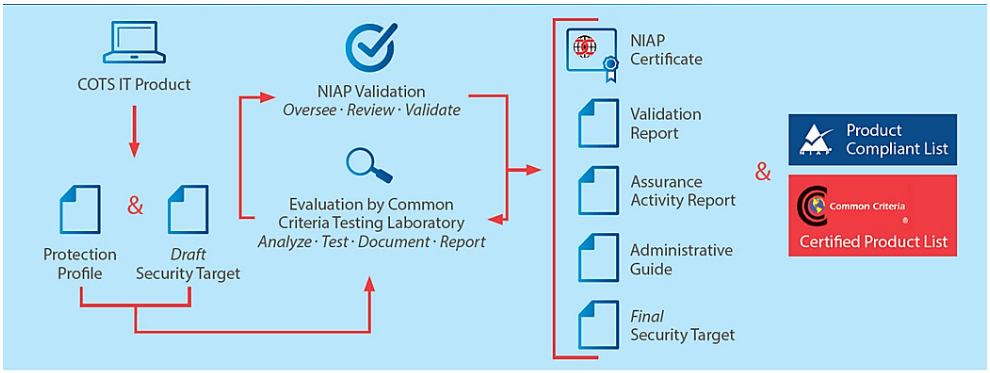
2.2.5.3 Was wird wonach geprüft?

Wenn ein Produkt für den Einsatz in nationalen Sicherheitssystemen vorgesehen ist, ist eine Bewertung durch die CNSS-Richtlinie #11 («Committee on National Security Systems») vorgeschrieben. Die Verwendung eines bewerteten Produkts ermöglicht schnelle Beschaffungs- und Akkreditierungsprozesse.

Eine NIAP-Zertifizierung stellt sicher, dass das Produkt die Bewertung erfolgreich abgeschlossen hat. Der Zweck der Evaluierung ist, die IT-Sicherheit der Produkte anhand eines ausgewählten, anwendbaren PP zu bewerten. Es gibt jedoch keine Garantie dafür, dass ein Produkt grundsätzlich frei von Mängeln ist. Bedingt durch die Anforderung in den USA, im öffentlichen Bereich nur noch Produkte mit CC-Zertifikat zu akzeptieren, werden Hersteller von IT-Produkten weltweit gezwungen, sich einem Zertifizierungsverfahren zu unterziehen, wenn sie auf dem amerikanischen Markt in diesem Sektor mitbieten möchten.[49]

Der Evaluierungsprozess beinhaltet die folgenden Schritte:

- Zu Beginn des Evaluierungsprozesses wählt ein Produktanbieter ein zugelassenes CCTL aus, welches die Produktevaluierung anhand eines zutreffenden, von der NIAP genehmigten PP durchführt. Hersteller werden ermutigt, sich an mehrere CCTL zu wenden, um Fachwissen, Erfahrung und Kosten zu vergleichen. Alle CCTL bieten Beratungsleistungen an, die dem Anbieter helfen, die Anforderungen zu ermitteln, bevor dieser formell in den Bewertungsprozess eintritt.[50]
- Der Hersteller, eventuell mit Unterstützung des Labors, erstellt die Sicherheitsvorgaben und stellt das zugehörige Prüfobjekt dem CCTL zur Verfügung.
- Das CCTL schlägt der NIAP eine neue Evaluierung vor. Nach der Eingabe der Evaluierung bewertet das CCTL das Produkt unter der Aufsicht durch die NIAP, welche die Prüfung validiert und endgültig genehmigt. Der Evaluierungsprozess dauert zwischen 90 Tagen und bis zu sechs Monaten.



Documents:

- **Protection Profile:** An implementation independent set of security requirements for a category of IT products that meet specific consumer needs.
- **Security Target:** Specification of the security functions against which the IT product, i.e., the Target of Evaluation (TOE), will be evaluated and as a description relating the product to the environment in which it will operate.
- **Administrative Guidance:** Instructions to users on how to configure the product so that it is consistent with the evaluated configuration.
- **Assurance Activity Report:** Summarized assurance activities of the product evaluation.
- **Validation Report:** A publicly available document issued by the NIAP validation body that summarizes the evaluation results and confirms the overall results are acceptable.

Abbildung 5: NIAP-Validierungsprozess (Quelle: https://www.niap-ccevs.org/Ref/Evals.cfm)

Die Kosten einer Prüfung werden zwischen dem Lieferanten und dem CCTL ausgehandelt, die NIAP ist nicht an den Bewertungskosten beteiligt.[51]

Die NIAP überwacht nur die Evaluation von «**Commercial**-off-the-shelf»-(COTS)-IT-Produkten von akkreditierten CC-Testing Labs (CCTL). Eine andere Kategorie sind die so genannten «**Government** off-the-shelf»-(GOTS)-Produkte. Für Produkte, die der nationalen Sicherheit dienen, muss das CNSS Nr. 11 erfüllt sein, sie werden aber nicht vom NIAP überwacht.

Analog zum englischen CAPS gibt es in den USA zudem noch den «Federal Information Processing Standards??» FIPS 140, der die Anforderungen an

Kryptomodule definiert. Die Anforderungen werden von den US (und kanadischen) Behörden vorgegeben. Diese beziehen sich sowohl auf Soft- als auch Hardware, die von den Departementen und Agenturen der USA genutzt werden. IT-Hersteller, die Produkte mit Verschlüsselungskomponenten in den USA vertreiben wollen, benötigen in der Regel eine Zertifizierung nach FIPS 140-2. Für diesen Standard verantwortlich ist das NIST, welches die Zulassung für die Testlabors herausgibt.[52]

2.2.6 Finnland

Die finnische Transport- und Kommunikationsagentur Traficom hat Ende November 2019 auf Basis der ETSI EN 303 645 ein finnisches Cyber-Security-Label eingeführt. Die Etikette garantiert den Verbrauchern, dass die gekennzeichneten Geräte grundlegende Informationssicherheitsmerkmale aufweisen. Mit dem Label möchte Traficom das Bewusstsein der Konsumenten für Informationssicherheit und die sichere Nutzung von vernetzten Geräten fördern. Finnland ist das erste Land in Europa, das ein solches Sicherheitslabel für Smart Devices lancierte und so IoT-Produkte fördert, die «secure-by-default» sind.

Das Cyber-Security-Label wurde in einem Pilotprojekt unter der Leitung des «National Cyber Security Centre» (NCSC-FI) in Zusammenarbeit mit den Unternehmen Cozify Oy, DNA Plc und Polar Electro Oy entwickelt. NCSC-FI entwickelte den Zertifizierungsprozess, legte die Kriterien fest und prüft deren Einhaltung.

Die ersten Cyber-Security-Labels wurden für die Produkte der genannten Unternehmen vergeben. Das Label wurde an den Cozify Hub für Smart Homes, das Wattinen Smart Heating System von DNA und die Polar Ignite Fitness-Smartwatch verliehen.

Das Cyber-Security-Label wird auch in einer Kampagne unter dem Motto «buy smart, not blind» gefördert. Ziel ist, das Etikett den Verbrauchern vertraut zu machen und sie zu motovieren, bei der Auswahl von Produkten und Dienstleistungen aktiv danach zu suchen. Gleichzeitig soll das Label zur besseren Verfügbarkeit von sicheren Geräten auf dem Markt beitragen. Längerfristig möchte man möglichst viele Hersteller animieren, ihre Produkte zertifizieren zu lassen, so dass in einigen Jahren die meisten Heimelektronik-Produkte mit dem Cyber-Security-Label ausgezeichnet sein werden.[53]

2.3 Europäische Union

2.3.1 Gemeinsamer Rahmen für die Zertifizierung der Cyber-Sicherheit

Die in der «Senior Official Group Information Systems Security» (SOG-IS, https://www.sogis.org) organisierten Mitgliedsstaaten bilden einen Verbund, um einen von öffentlichen Stellen unterstützten Vertrauenswürdigkeitsnachweis für IT-Sicherheitsprodukte zu fördern.[54] Das Abkommen zur internationalen Anerkennung (MRA) von IT-Sicherheitszertifikaten in Europa wird in Kürze abgelöst durch ein CC-ähnliches Zertifizierungsschema unter dem europäischen «Cybersecurity Act».

Dieser Rechtsakt zur Cyber-Sicherheit trat am 27. Juni 2019 als unmittelbar in der EU geltende «Verordnung (EU) 2019/881» in Kraft.[55,56] Die für Prüfung und Zertifizierung relevanten Artikel (insbesondere die Artikel 58, 60, 61, 63) gelten ab dem 28. Juni 2021. Die Verordnung besteht grundlegend aus zwei Teilen: Einerseits stärkt sie die Rolle der Agentur der Europäischen Union für Cyber-Sicherheit (ENISA) und stattet diese mit einem dauerhaften Mandat aus. Andererseits führt die Verordnung einen europäischen Zertifizierungsrahmen für Cyber-Sicherheit ein.

Mithilfe der europäischen Cyber-Sicherheits-Zertifikate will die EU sicherstellen, dass die Cybersicherheitsstandards bei in den EU-Ländern vermarkteten Produkten und Dienstleistungen eingehalten werden. Der neue Zertifizierungsrahmen soll die Transparenz der Sicherheitseigenschaften von Produkten und Dienstleistungen für Konsumenten erhöhen und so das Vertrauen in den digitalen Binnenmarkt der EU stärken. Nicht zuletzt soll für europäische Anbieter, die das wachsende Kundenbedürfnis nach sicheren digitalen Lösungen bedienen, ein Wettbewerbsvorteil entstehen. Die von der ENISA entwickelten Schemata für Zertifizierungen enthalten zu diesem Zweck u.a. Listen der IKT-Produkte, -Dienste und -Prozesse und Kategorien, die von der Aufnahme in ein europäisches System für Cyber-Sicherheits-Zertifizierung profitieren können.

Auf Antrag der Europäischen Kommission hat die ENISA gemäss Artikel 48.2 des Cybersecurity Acts eine Ad-hoc-Arbeitsgruppe eingerichtet, um die Vorbereitung eines Kandidaten für ein EU-Zertifizierungssystem für Cybersicherheit als Nachfolger der bestehenden SOG-IS MRA Systeme zu unterstützen. Dieses wurde als EUCC-Schema («Common Criteria based European candidate cybersecurity certification scheme») bezeichnet und befasst sich mit der Zertifizierung der Cybersicherheit von IKT-Produkten auf der Grundlage der «Common Criteria», der «Common Methodology for Information Technology Security Evaluation» und der entsprechenden Normen ISO/IEC 15408 und ISO/IEC 18045. Am 2. Juli 2020 wurde die Vernehmlassung eines durch die Arbeitsgruppe erarbeiteten ersten Entwurfs des EUCC-Schemas initiiert.[57]

Kapitel 22 («Mututal recognition with third countries») des EUCC-Schemas behandelt gemäss Artikel 54.1 (t) des Cybersecurity Acts die Vorbedingungen für die gegenseitige Anerkennung von Zertifikaten von Drittländern und für die Begutachtung durch Fachkollegen. Der Abschluss eines Abkommens über gegenseitige Anerkennung (MRA) zwischen den Teilnehmern soll die gegenseitige Anerkennung von Zertifizierungen mit Drittländern unterstützen.

2.3.2 Konsequenzen für Standards und Zertifizierungen in der Schweiz

Die Standards und Zertifizierungen, welche die Schweiz in Umsetzung der NCS einführen würde, wären aller Voraussicht nach mit den Anforderungen der EU kompatibel. Allerdings ist noch unklar, wie die EU in Zukunft mit ITK-Produkten aus dem Ausland umgehen wird, welche die Cyber-Sicherheits-Standards von in den EU-Ländern vermarkteten Produkten und Dienstleistungen einhalten, aber nicht formell nach ENISA geprüft bzw. zertifiziert worden sind.

Es stellen sich mindestens die folgenden Fragen:

- Welche Cyber-Sicherheits-Produkte und -Dienstleistungen aus dem EU-Ausland können ein entsprechendes Zertifikat der ENISA erhalten?
- Welches sind die Bedingungen dafür?
- Wird die EU die Äquivalenz der Schweizer Cyber-Sicherheits-Standards anerkennen und auf dem EU-Binnenmarkt zulassen?
- Welche Institution in der Schweiz würde ein bilaterales Abkommen (MRA) mit der EU organisatorisch und inhaltlich vorantreiben, damit Cyber-Sicherheitsprodukte und -dienstleistungen einen Zugang zum EU-Binnenmarkt erhalten?

3 WER lässt prüfen bzw. sollte prüfen lassen?

Die folgenden Kapitel beschreiben eine mögliche Ausrichtung eines Schweizer Prüfinstitutes für vernetzte Geräte. Die Strukturierung erfolgt gemäss der folgenden Übersicht.

- Kapitel 3 («WER») betrachtet die beteiligten Akteure.
- Kapitel 4 («WAS») klassifiziert die zu prüfenden Objekte.
- Kapitel 5 («WIE») beschreibt Methoden und Spezifikationen.
- Kapitel 6 zeigt mögliche Organisationsformen auf.

3.1 Wünschbarkeit von Prüfungen vs. Nachfrage im Markt

Der Expertenbefund über einen Mangel an Cyber-Sicherheits-Prüfungen und entsprechenden Institutionen (siehe Kapitel 1) kann auch als Fehlen einer entsprechenden Nachfrage im Markt interpretiert werden. Die gesellschaftlichen und politischen Forderungen nach einer Durchsetzung von Cyber-Sicherheits-Standards bei Geräten und Anwendungen (und entsprechenden Vorschriften/Vorgaben) stossen bis dato offenbar nicht auf ein entsprechendes Bedürfnis im Markt. Weder bei den Herstellern (bzw. Lieferanten, bzw. Importeuren) noch bei den geschäftlichen Beschaffern von Cyber-Produkten noch bei den Haushalten (Haushaltsgeräte, Consumer Electronics) scheint heute eine konkrete Nachfrage nach Prüfungen mit einer entsprechenden Zahlungsbereitschaft zu bestehen.[58]

Der Ruf nach Cyber-Security-Prüfungen, -Zertifikaten und allenfalls sogar einem entsprechenden Label kann somit nicht ohne weiteres mit der Situation im Lebensmittel- und Energiebereich verglichen werden. Dort werden Qualitäts- bzw. Sicherheitslabels (EG-BE, CE, Grüner Punkt, Agroscope Labels usw.) sowohl von Konsumenten verlangt als auch von Hersteller- bzw. Lieferantenseite als Marketing-Instrument eingesetzt. Allerdings zeigt gerade die Geschichte der Energieverbrauch-Labels, dass es Vorschriften bzw. Gesetze braucht, damit sich ein Label und entsprechende Prüfungen durchsetzen. Ohne Prüfkapazitäten lassen sich Vorschriften und Gesetze weder durchsetzen noch sinnvoll anwenden.

Gegen solche Vorgaben könnte eingewendet werden, dass es in der Form von Produkte-Bewertungen in Foren und Netzwerken (darunter die Open Source Communities, zahlreiche White Hat Hacker, aber auch Geräte-spezifisch ausdifferenzierte User-Communities) schon eine Art «Selbstkontrolle» des Marktes existiert. Auch liegt es sicher im Interesse von Herstellern und Anbietern, Reputationsverlusten vorzubeugen. Trotzdem müssen die Prüfergebnisse der Hersteller oder jene aus der Community durch eine unabhängige Instanz überprüft werden können. Nur so kann dokumentiert werden, was von wem auf der Basis welcher Normen mit welchem Know-how und in welcher Tiefe getestet wurde. Dass informelle Communities nicht immer funktionieren, zeigt die noch immer

hohe Zahl an Sicherheitslücken in Open-Source-Produkten auf.[59, 60] Obwohl immer wieder Schwachstellen öffentlich bekannt gemacht werden, fühlen sich weder Hersteller noch Konsumenten grundsätzlich zu Änderungen verpflichtet.[61] Trotz Bekenntnissen zur Bedeutung der Sicherheitsfrage sehen internationale Produzenten bzw. Anbieter in Prüfungen primär zusätzliche Regulierungen und Kosten. Die Mehrheit der Experten stimmt deshalb überein, dass ohne gesetzliche Vorgaben oder entsprechende verbindliche Richtlinien keine Normierungs- oder Prüfungsinstanzen existieren können. Konsequenterweise wird im Hinblick auf das angestrebte Prüfinstitut auch der Gesetzgeber gefordert sein.

Auch wenn gesetzliche Vorschriften (oder Handels- und Marktzugangsabkommen) als Voraussetzung für einen Prüfungsmarkt scheinen, so zeigt das Beispiel des TÜV Süd, dass Prüfstellen bis zu einem gewissen Grad auch freiwillig genutzt werden. Die Prüfung von Cyber-Produkten kann via internationale Standards wie z.B. ISA induziert werden. Verschiedene Branchen und zunehmend auch die öffentliche Hand verlangen eine Zertifizierung nach ISO.[62] Ein wichtiger Weg zur Ausweitung von Cyber-Sicherheits-Prüfungen sind Spezialgesetzgebungen, z.B. im Gesundheitswesen und im Energiebereich. Aus der Sicht des deutschen BSI haben solche Vorschriften den Reputationsgewinn als Motivation für Prüfungen abgelöst.

3.2 Grundsätzliche Verantwortung der Hersteller

Unabhängig von der Frage spezieller Vorgaben ist gemäss den Prinzipien der Haftpflicht grundsätzlich der «Inverkehrbringer» (Hersteller, Lieferant) von Geräten für die Prüfungen zuständig, wie dies bei vielen anderen Sicherheitsprüfungen (Autos, Flugzeuge, elektrische Anlagen usw.) der Fall ist. Aus den Länderbeschrieben (Kapitel 2) geht hervor, dass es durchgehend die Hersteller und Lieferanten sind, die Prüfungen beantragen und diese dann bei einer Prüfstelle durchführen lassen.

Parallel zum Aufbau der Prüfinstanz wären verschiedene gesetzgeberische Massnahmen und privatrechtliche Regelungen nötig. Der erste Komplex solch regulatorischer Schritte betrifft die Verantwortlichkeit von Herstellern und Lieferanten für die Sicherheit und Qualität ihrer digitalen Produkte und Dienste. Es sollten sektorspezifische Vertragsvorlagen (Security Appendices) entwickelt werden, welche die relevanten Sicherheitskriterien dokumentieren. Die Sicherheitsanliegen erhalten auf diese Weise mehr Gewicht als durch individuelle Absprachen zwischen Kunde und Hersteller.

Wichtige Minimalforderungen in solchen «Security Appendices» wären:

- Der Hersteller verpflichtet sich zu Coordinated Disclosure (ISO 29147) zur Handhabung von gemeldeten Schwachstellen. Er dokumentiert die Umsetzung des Prozesses, die Ansprechpartner und die Bearbeitungsdauer.

- Der Hersteller verpflichtet sich, gängige Sicherheitsstandards bei der Entwicklung einzuhalten (wie beispielsweise den Verzicht auf hardcodierte Passwörter und Standardpasswörter).
- Der Hersteller verpflichtet sich zur vollständigen und abschliessenden Dokumentation aller im Produkt eingebauten Sicherheitsobjekte (wie beispielsweise Zugangsdaten, Default Accounts, Passwörter, Keys/Schlüssel usw.).
- Der Hersteller räumt dem Kunden das Recht ein, die Hard- und Software des Produktes auf Integrität und Sicherheit zu prüfen (Reverse Engineering), ohne damit die Intellectual Property Rights (IPR) zu verletzen.

Bei allfälligen späteren Entdeckungen von Schwachstellen oder Backdoors kann der Hersteller so als Urheber in die Pflicht genommen werden (keine «Plausible Deniability») und der Kunde hat die Möglichkeit, bei Sicherheitsvorfällen der Ursache auf den Grund zu gehen (Forensik, Reverse Engineering). Vertrauen und Transparenz werden erhöht, der Hersteller trägt seinen Teil der Verantwortung. Fehlverhalten kann Konsequenzen haben und schlimmstenfalls den Ausschluss vom Markt zur Folge haben (vergleiche dazu die Situationen in Deutschland und Grossbritannien).[63]

3.3 Subsidiäre Auftraggeber von Prüfaufträgen

Angesichts fehlender Vorgaben für Cyber-Sicherheits-Prüfungen und entsprechend geringer «Motivation» der Hersteller und Lieferanten werden subsidiär auch besonders betroffene Besteller bzw. Anwender als Auftraggeber bzw. Initianten von Prüfungen ins Auge gefasst.

Ein besonderes Interesse an Prüfungen wird bei Betreibern von kritischen Infrastrukturen und Anbietern von Service-Public-Funktionen erwartet. In einer anfänglichen Phase ist deshalb denkbar, dass die Betreiber kritischer Infrastrukturen erste Prüfungen definieren. Bei diesen Firmen und Institutionen kann man schon heute von einer öffentlichen Pflicht zur Erfüllung minimaler Sicherheitsstandards sprechen (z.B. bei Smart Meters). Wenn sich das Prüfinstitut (mindestens in der Anfangsphase) auf kritische Infrastrukturen konzentrieren würde, könnte sowohl mit einer politischen Unterstützung als auch mit Prüfungsaufträgen aus dem Umfeld der Stromproduzenten und -vertreiber, der Verkehrsbetreiber, der Gesundheitsversorgung und auch der Finanzindustrie gerechnet werden.

Eine Nachfrage wird zudem auch bei Endbenutzern von besonders exponierten und/oder lebenswichtigen Geräten antizipiert, z.B. bei medizinischen Apparaten, die im Alltag, d.h. ausserhalb der kontrollierten bzw. geschützten Spitalumgebung, eingesetzt werden (z.B. Herzschrittmacher).

Ebenfalls denkbar ist, dass Branchenverbände oder der Bund regelmässige Prüfungen beauftragen. Als weiterer Auslöser oder sogar Besteller von Prüfungen wird auch immer wieder die Versicherungsindustrie genannt.

Schliesslich soll zudem das Prüfinstitut selbst eigene Prüfungen definieren und in Auftrag geben können oder, wenn es über ein eigenes Labor verfügt, diese selbst durchführen. Derartige Prüfaufträge können sein:

- Prüfungen zum Zweck der Sensibilisierung von Schweizer KMU und der Gesellschaft, insbesondere im Hinblick auf wenig bekannte Schwachstellen und Komponenten.
- Prüfungen aufgrund einer besonderen (Gefährdungs)lage mit Auswirkung auf grosse Teile der Bevölkerung.[64]
- Prüfungen im Hinblick auf die Publikation von wissenschaftlichen Studien zur internationalen Positionierung des Instituts.
- Wiederholungen von im Ausland erfolgten Prüfungen zu Zwecken der Qualitätssicherung und der internationalen Vergleichbarkeit.

3.4 Finanzierung des Prüfaufwands

Aus der Verantwortung bzw. Verpflichtung der Hersteller und Lieferanten ergibt sich auch deren Pflicht zur Übernahme der Aufwände für die Prüfungen. (In den Prüfmodellen im benachbarten Ausland bezahlen Hersteller und Lieferant als Aufraggeber der Prüfungen die Kosten für die Prüfstelle sowie eine Gebühr an die Prüfinstanz.[65])

Es wird oft argumentiert, dass sich die Prüfinstanz zuerst etablieren muss, bevor sich eine Nachfrage herausbilden kann. Die Prüfinstanz sollte deshalb in einer ersten Phase durch die öffentliche Hand (Bund, Kantone) finanziert werden. In einem zweiten Schritt könnte die öffentliche Finanzierung durch eine gemischtwirtschaftliche Trägerschaft (z.B. in Form eines Vereins oder einer Stiftung analog z.B. zu Electrosuisse) übernommen werden.

4 WAS soll geprüft werden?

Dieses Kapitel beschreibt Priorisierungen im Hinblick auf die Frage der zu prüfenden Komponenten und Systeme («Prüflinge»).

4.1 Eingrenzung der Klassen von Prüflingen

Aus der Sicht des Prüfinstitutes ist das zu prüfende Universum zunächst unendlich. Wenn alle Hersteller (oder sogar zusätzlich alle Betreiber) von netzwerkfähigen Geräten als potenzielle Kunden betrachtet werden, kommt es zu Tausenden von wichtigen Device-Typen (mit mehreren Generationen) sowie zu Zehntausenden weiterer Device-Typen (mit mehreren Generationen), die grundsätzlich zu prüfen wären – idealerweise über den gesamten Lifecycle.

Angesichts der unterschiedlichen Erwartungen und Risikoeinschätzungen der potenziellen Nachfrager von Prüfungen muss der Eingrenzung der Prüflinge (genauer: der Festlegung des Scopes der Prüfinstanz) eine möglichst «objektive» Risiko-Einschätzung und -Bewertung vorausgehen, z.B. abgestützt auf die vom Bundesamt für Bevölkerungsschutz (BABS) entwickelten Methoden. Aufgrund der beschränkten Ressourcen einer neuen Institution und der wachsenden Zahl an prüfbaren Geräten ist eine eingrenzende und priorisierende Analyse unerlässlich.

Wenn die Prüfinstanz fast ausschliesslich auf Antrag der Hersteller und Lieferanten tätig wird (allenfalls ergänzt durch aktuelle sicherheitspolitisch relevante Einzelprüfungen), relativiert sich allerdings die Bedeutung dieser (theoretischen) A-priori-Begrenzungen der Prüfungen. Trotzdem gibt es unter den Experten einen gewissen Konsens, nach welchen Kriterien eine Priorisierung der Prüflinge vorgenommen werden könnte oder sollte.

Unabhängig von solchen Priorisierungen wird ferner davon ausgegangen, dass es auch im Bereich der Cyber-Sicherheit europäische und internationale Vereinbarungen zur gegenseitigen Anerkennung von Prüfungen bzw. Zertifikaten geben wird. Geräte, die von anerkannten Instanzen im Ausland (bzw. von den von diesen anerkannten Prüfstellen) geprüft wurden, würden deshalb nur in Ausnahmefällen in der Schweiz nochmals einen vollständigen Prüfprozess durchlaufen.

4.2 Differenzierung zwischen Hard- und Software?

Grundsätzlich hat das angestrebte Prüfinstitut vernetzte Geräte aller Art im Fokus. Eine Unterscheidung zwischen Hard- und Software-Produkten ist nicht zielführend, da sich insbesondere im Zusammenspiel (z.B. in der Firmware) Sicherheitslücken ergeben können. Auch eine Unterscheidung zwischen IoT, IIoT

und anderen Geräten scheint wenig sinnvoll, da der Trend in die Richtung einer allgemeinen Vernetzung geht. Es müssen also grundsätzlich Prüfungen für Hardware, Firmware und Software durchführbar sein.

Bei Cyber-Bedrohungen über die Lieferkette können Komponenten während oder bereits vor der Lieferung manipuliert werden. Im Falle staatlicher Bedrohungen kann die Manipulation bereits bei der Entwicklung von Chips, bei der Herstellung oder Integration von Komponenten oder während des Transports zum Endabnehmer geschehen.[66] Integrierte Fehlfunktionen oder Backdoors in vernetzten Produkten können auch erst nach der Auslieferung aktiviert werden, z.B. durch ein Update. Mit der steigenden Komplexität von Prozessoren und Chips verlagert sich die Bedrohung in Richtung des Designs dieser Komponenten.[67]

4.3 Kritikalität

Die Kritikalität bemisst sich grundsätzlich am erwarteten Schaden bei Manipulation oder Ausfall des Prüfobjekts am vorgesehenen, späteren Einsatzort. Fällt eine relevante Systemkomponente einer Anlage der kritischen Infrastruktur aus, so ist der Schaden grösser als beim Ausfall einer Komponente im Bereich der Unterhaltungselektronik. Von verschiedener Seite wird deshalb vorgeschlagen, den Umfang der Prüfungen auf Komponenten zu beschränken, die in kritischen Infrastrukturen zum Einsatz kommen, etwa im Mobilfunk sowie in der Energie- und Wasserversorgung. Bei einer Konzentration (oder sogar Beschränkung) der Tätigkeit des Prüfinstituts auf Aufträge von Betreibern kritischer Infrastrukturen ergäbe sich automatisch eine Einschränkung der zu betrachtenden Komponenten/Systeme.

Gegen eine solche Priorisierung wird allerdings eingewendet, dass auch unkritische Komponenten dazu missbraucht werden können, kritische Komponenten anzugreifen.[8] Weiter wird die Kritikalität eines Prüfobjekts massgeblich durch den Grad seiner Verbreitung im Feld beeinflusst. Dies gilt insbesondere auch für vernetzte Geräte im Haushalt und in der Industrie. So gelten beispielsweise Smart Meters als Elemente kritischer Infrastrukturen.

Neben der Prüfung einzelner Komponenten ist die Prüfung ganzer Systeme (also der Verbund von Komponenten inkl. Leitstellen und entsprechender Prozesse) zu betrachten. Insbesondere im Hinblick auf kritische Infrastrukturen ist die Prüfung des Zusammenspiels von Komponenten über wohldefinierte Schnittstellen im Sinne der Systemzertifizierung von Bedeutung.[68]

4.4 Differenzierung nach Machbarkeit

Auch die Machbarkeit von Prüfungen (als Verhältnis von potenziellem Prüfaufwand zu potenziellem Risiko) wäre ein Kriterium für die Definition des Scopes der Prüfinstanz. So könnten beispielsweise Produkte, die den CC-Standard nicht erfüllen, von vornherein als nicht zertifizierungswürdig und somit als nicht einsetzbar bewertet werden. Diese Eingrenzungen sollten aber in regelmässigen Abständen überprüft werden, um raschen Risikoveränderungen und neuen Angriffsszenarien Rechnung zu tragen.

4.5 Differenzierung nach «Herkunftsort»

Aufgeworfen wird auch die Frage, ob Geräte aufgrund des Herkunftsorts für eine Prüfung ausgewählt (oder ausgeschlossen) werden sollten. Diese Überlegung resultiert einerseits aus vermuteten Qualitätsmängeln, eher aber noch aus sicherheitspolitischer Perspektive (vgl. Huawei und Crypto AG). Qualitätsmängel werden von den Experten grundsätzlich als negatives Selektionskriterium gesehen: Wurde eine CC-Zertifizierung abgelehnt, fällt das zu prüfende Produkt ohnehin ausser Betracht. Liegt eine bestehende Zertifizierung einer vertrauenswürdigen, d.h. akkreditierten Prüfstelle vor, wären weitere Prüfungen überflüssig.[69]

5 WIE soll geprüft werden?

Dieses Kapitel listet die Anforderungen an das Prüfverfahren auf, meist in Form minimaler Anforderungen. Es ist an dieser Stelle unerheblich, ob die technische Prüfung von einem Labor durchgeführt wird, das selbst Teil des Prüfinstituts ist, oder durch eine in angemessener Weise vom Prüfinstitut anerkannte, überwachte und begleitete Prüfstelle (siehe auch Kapitel 6).

5.1 Wohldefinierter Prozess

Prüfvorgänge müssen einem wohl definierten Prozess folgen und unterliegen einer Dokumentationspflicht. Die zu jedem Prüfauftrag erforderliche Prüfspezifikation regelt individuell, welche Fragestellungen Bestandteil der Prüfung sind. In dieser Spezifikation ist unter anderem geregelt, ob die Existenz bekannter Schwachstellen überprüft wird oder ob die Prüfobjekte auf grundlegende Auffälligkeiten hin untersucht werden sollen. Zu den grundlegenden Fragestellungen zählt unter anderem die Einhaltung von Security-by-Design und Security-by-Default. Ein Verweis auf existierende Standards ist möglich.

5.2 Anforderungen – Testtiefe

Die Spanne der Prüfungen reicht von grundlegenden Prüfungen, die sich idealerweise automatisieren lassen, bis hin zu hochspezialisierten Prüfungen, die oft forschungsnah sind und aufwendige Geräte, spezialisierten Materialeinsatz und Spezialwissen erfordern. Die Tests der Prüfinstanz sollten typischerweise zumindest folgende Punkte beinhalten:

- Review von Source Code (sofern verfügbar)
- Review von Konfigurationen und Einstellungen (sofern sichtbar)
- Analyse von Soft-, Firm- und Hardware (falls nötig durch Reverse Engineering)

Damit geprüft werden kann, muss der Quellcode frei verfügbar sein (Open Source) oder bei einer unabhängigen Stelle deponiert werden (Code Escrow). Der zu prüfende Code muss ausserdem eindeutig gekennzeichnet sein, sodass sichergestellt werden kann, dass tatsächlich der geprüfte Code zur Ausführung kommt.[70]

5.3 Prüfungen von Mustern/Stichproben

Es liegt auf der Hand, dass aus Skalengründen in der Regel nur einzelne Muster der Geräte geprüft werden. Um eine Repräsentativität für grosse Bestände (allenfalls Gesamtheiten oder zumindest Serien) zu gewährleisten, werden die zu prüfenden Objekte zufällig und nicht vorhersehbar aus einer Menge gleicher

Prüfobjekte ausgewählt. Die geprüften Geräte werden mit eindeutiger Seriennummer erfasst und in einem Prüfpfad («Audit Trail») inklusive Prüfspezifikation für 10 Jahre durch die Prüfinstanz abgelegt. Anhand der Historie des Prüfpfads lässt sich die Entwicklung einer Produktserie sowie des Herstellers feststellen.

5.4 Prüfobjekt im Einsatzumfeld

Die Frage, ob Geräte isoliert in einem Labor oder konnektiert in ihrem späteren Einsatzumfeld geprüft werden, muss in der Prüfspezifikation geklärt werden. Es ist davon auszugehen, dass in der Mehrheit der Fälle Systemkomponenten im Labor geprüft werden. In ihrer beratenden Rolle kann die Prüfinstanz den Auftraggebern (und der Prüfstelle) empfehlen, wo und in welcher Umgebung geprüft werden soll. Es muss allerdings berücksichtigt werden, dass Interaktionen mit den umgebenden Systemen nicht vorhersehbar sind. Sowohl die Systemumgebung als auch Parametrisierung und Konfiguration des zu prüfenden Systems bzw. Geräts kann jederzeit angepasst werden. Diese Dynamik ist durch die Prüfinstanz weder prognostizierbar noch kontrollierbar. Folglich kann nur getestet werden, ob ein System einer technischen Spezifikation folgt (sofern diese vorhanden ist) und ob es frei von offensichtlichen Schwachstellen ist (z.B. ungeschützte Speicherung von Zugangsdaten für Umsysteme, Exponierung sensitiver Daten auf ungeschützten Kanälen usw.).

5.5 Prüfobjekt vs. Deklaration/Patch-Management

Grundsätzlich liegt der Prüfinstanz nur das zu prüfende Objekt selbst vor. Eine begleitende Dokumentation hat keinen verbindlichen Charakter und wird nur als Hilfestellung für die Tester verstanden. Insbesondere sind die Entwicklungsprozesse des Prüfobjekts sowie die Prozesse innerhalb der Organisation des Herstellers nicht Bestandteil der Prüfung. Ebenso wenig werden vertragliche Bestimmungen zwischen Hersteller, Lieferant und Anwender durch die Prüfinstanz auf juristische Fragestellungen hin validiert oder geprüft. Vom Prüfumfang ausgeschlossen sind Verpflichtungen und Absichtserklärungen der Hersteller, regelmässig Patches und Updates zu liefern. Der Grund dafür ist, dass sich die spätere Einhaltung von Zusicherungen dieser Art technisch nicht am Prüfobjekt feststellen lässt.

Eingeschlossen in die Prüfungen sind jedoch all jene Prozesse, die das Prüfobjekt zum Einsatzzeitpunkt direkt betreffen. Diese lassen sich typischerweise am Prüfobjekt durch das Vorhandensein technischer Massnahmen feststellen. Lediglich als Beispiel sind hier zu nennen:

- Vulnerability- und Patch-Management: Technische Vorkehrungen für das Aufspielen von Patches und die Beseitigung von Schwachstellen durch den Hersteller, Vorhandensein von Auto-Update-Mechanismen.
- Backup-/Restore-Funktionalität: Sind Backups von Konfigurationen und Daten möglich? Lassen sich Konfigurationen und Daten aus vorhandenen
- Backups wieder aufspielen?
- Zugangskontrolle: Lässt sich die Zugangskontrolle anpassen? Lassen sich Passwörter anpassen? Sind Mehrfaktorauthentisierungen aktivierbar?
- Secure Reset/Erasure: Lassen sich Daten und Konfigurationen sicher aus dem Gerät entfernen, z.B. bei Ausserbetriebnahme.

5.6 Umgang mit Updates

Als weitläufig akzeptiert gilt, dass netzwerkfähige Produkte über einen robusten und sicheren Mechanismus verfügen sollten, um Sicherheits-Updates zeitnah und skalierbar einzuspielen. Damit wird die Möglichkeit zum Schutz kritischer Produkte während der gesamten Lebensdauer sichergestellt, auch nach einem allfälligen Untergang des Herstellers. Für die Prüfung von netzwerkfähigen Produkten ergeben sich dadurch besondere Herausforderungen.

Werden Prüfobjekte nach erfolgter Prüfung überarbeitet, so decken erfolgte Prüfungen die aktualisierten Objektversionen nicht notwendigerweise ab. Aus diesen Gründen sind zurückliegende Prüfergebnisse nur mit eingeschränkter Aussagekraft gültig. Insbesondere sind Prüfergebnisse nur für eine Versionsnummer des Prüfobjekts und grundsätzlich nur bis zu einem definierten Ablaufdatum gültig. Das Ablaufdatum richtet sich insbesondere nach dem Typ des Prüfobjekts. Eine Nachprüfung erfolgt nicht automatisch, sondern muss durch einen Auftraggeber erneut initiiert werden. Die Prüfinstanz verfolgt die Versionsgeschichte aller jemals geprüften Prüfobjekte nicht. Die Prüfprotokolle hingegen werden durch die Prüfinstanz sicher verwahrt.

Die Aussagekraft der Prüfung von Apps mit kurzen Releasezyklen kann nur durch wiederholte Prüfungen in kurzen Zyklen erhöht werden. Der Hersteller kann den Prozess massgeblich vereinfachen, indem er einen Nachweis über die Änderungen in den jeweiligen Releases bereitstellt, idealerweise als technischen Beschrieb, z.B. am Source-Code oder in Form dedizierter Update Labels.[71]

5.7 Problem Prüfstandmodus

Anders als in der Autoindustrie lässt sich keine universelle Detektion eines Prüfstandmodus realisieren. Gezieltes Reverse-Engineering und Source-Code-Analysen erhöhen zwar die Detektionschancen verbauter Weichen zur Umschaltung in unerwünschte Betriebsmodi, jedoch existieren insbesondere bei Closed-Source-Komponenten zahlreiche Methoden, um Hintertüren gezielt zu

aktivieren.[72] Bei Open-Source-Komponenten besteht zudem das Problem der Abweichungen zwischen veröffentlichtem und tatsächlich ausgeliefertem Code.[60]

5.8 Zusätzliche Voraussetzungen für Prüfungen

Die im Folgenden aufgeführten Anforderungen sollen aussagekräftige und öffentlich nachvollziehbare Prüfergebnisse ermöglichen.

Definition der Prüfspezifikation: Eine hinreichend detaillierte Prüfspezifikation ist zwischen Prüferstelle und Auftraggeber vereinbart. Neben individuellen Spezifikationen sind auch Verweise auf bestehende Normen denkbar, sofern der Testumfang und die Testtiefe ausreichend dokumentiert sind.

Einwilligung des Herstellers bzw. Urhebers: Sofern kein übergeordnetes staatliches Sicherheitsinteresse an einer Prüfung des Prüfobjekts besteht, muss eine Einwilligung des Urhebers des Prüfobjekts vorliegen. Wird die Einwilligung nicht erteilt, sollte dies öffentlich einsehbar dokumentiert werden.

Verarbeitung und Schutz der Prüfergebnisse (responsible disclosure): Es muss sichergestellt werden, dass der Hersteller bzw. Urheber als Auftraggeber und die Prüfinstanz (sowie natürlich die Prüfstelle) sich über die weitere Verarbeitung der Prüfergebnisse einig sind. Eine Veröffentlichung bedarf in der Regel der Einwilligung des Urhebers. Sofern gefundene Schwachstellen eine Auswirkung auf die Stabilität und den sicheren Betrieb von kritischen Infrastrukturen oder Sicherheitsorganisationen wie der Armee haben, ist die Prüfinstanz verpflichtet, die Behörden (z.B. das Nationale Zentrum für Cyber-Sicherheit NCSC) über die Befunde zu informieren.

Einhaltung von Rahmenbedingungen und Rechtsgrundlagen: Die Prüfanfragen dürfen nicht gegen geltendes Recht einschliesslich Embargobestimmungen und internationale Sanktionen verstossen.

5.9 Resultate der Prüfverfahren

Von jeder durchgeführten Prüfung entsteht ein Prüfprotokoll mit den ausgeführten Schritten und den festgestellten Ergebnissen. Es beinhaltet die zugehörige Prüfspezifikation sowie eine von der Prüfinstanz festgelegte eindeutige Referenz. Das Prüfprotokoll wird manipulationssicher und vertraulich in der Prüfinstanz verwahrt (z.B. für 10 Jahre). Sofern in der Prüfspezifikation angegeben, kann diese Frist anders festgelegt werden. Die Prüfspezifikation ist grundsätzlich öffentlich zugänglich, ausser es wird explizit Anderslautendes vereinbart.

Nach erfolgter Prüfung wird eine Prüfbestätigung mit Angaben zum Prüfobjekt[73], den Prüfergebnissen und spezifischen Bemerkungen (Auffälligkeiten,

Abweichungen vom Prüfprozess, Vergleich mit ähnlichen Prüfobjekten) erstellt. Ausgehend von der Prüfbestätigung können die Prüfergebnisse im Nachgang in ein leicht verständliches Klassifikationssystem (Label) überführt werden. Eine Definition einzelner Stufen eines solchen Systems wird durch die Prüfinstanz erarbeitet.

6 Organisation

In den Diskussionen, wer als Auftraggeber von Prüfungen auftritt (Kapitel 3) und was und wie geprüft werden soll (Kapitel 4 und 5), blieben zwei Punkte offen.

Zum einen wird mehrheitlich die Auffassung vertreten, dass die Hersteller nur mit verbindlichen Vorschriften bzw. gesetzlichen Vorgaben Prüfungen beantragen werden. Nur so entsteht die für ein Prüfinstitut notwendige Nachfrage im Markt. Ob diese auch durch subsidiäre Auftraggeber auf der Besteller- bzw. Anwenderseite geschaffen werden könnte, bleibt offen. Ein bestellerseitiges Interesse an Prüfungen (mit entsprechender Zahlungsbereitschaft) wird am ehesten bei den Betreibern von kritischen Infrastrukturen vermutet, insbesondere bei den staatsnahen Energieversorgern und Verkehrsbetrieben. Zudem ist auch zu vermuten, dass die Schaffung eines Prüfinstitutes die entsprechende Regulierung beschleunigen könnte.

Der zweite offene Punkt betrifft den Umfang der Prüfungen. Die Aufzählung der zu prüfenden Objekte erscheint als geradezu unendlich. Dies beginnt schon bei einer unübersehbaren Menge an vernetzten Geräten und deren Komponenten, hinzu kommen die Interaktionen von Hardware, Firmware und Software, die rasche technologische Entwicklung und die Problematik relativ kurzer Update-Zyklen. Selbst bei grossen Prüfkapazitäten, deren Aufbau realistische Budgets sprengen würde, müsste sehr selektiv geprüft werden. Häufig wird deshalb die Kritikalität von Geräten als Kriterium für Prüfungen genannt. Die Kritikalität bezieht sich entweder auf den Einsatz der Geräte in sicherheitskritischen Infrastrukturen oder aber auf deren grossflächige Verbreitung im Alltag (z.B. in Haushalten).

6.1 Grundsatzentscheidungen für das Prüfinstitut

Weder die zukünftige Nachfrage nach Prüfungen noch der mögliche Umfang der Prüfungen können zum jetzigen Zeitpunkt des Projektes scharf bestimmt werden. Entsprechend schwierig ist es, konkrete institutionelle und personell-organisatorische Anforderungen an das Institut zu definieren. Deshalb wird versucht, die neue Einrichtung direkt zu beschreiben, wobei zwei Grundsatzentscheidungen eine zentrale Rolle spielen. Zum einen geht es dabei um die mögliche Einbindung in die bestehende institutionelle Landschaft und zum anderen um die Frage, ob das Prüfinstitut auch als Prüfstelle agieren, d.h. über eigene Laborkapazitäten verfügen soll.

6.1.1 Differenzierung A: Prüfinstitut vs. Prüfstelle

Die neue Organisation (und auch deren Einbindung in die existierende institutionelle Landschaft) kann nicht ohne Klärung des Verhältnisses von Prüf*institut*

und Prüf*stelle* beschrieben werden (vgl. die Definitionen in Abschnitt 1.2.1). Die Vorstösse zur Schaffung eines Prüfinstituts standen unter der Prämisse, dass diese Institution keine blosse Compliance-Überprüfungsstelle sein würde. Vielmehr sollte sie über ein substanzielles Testlabor verfügen, d.h. selbst in der Lage sein, durch unabhängige und glaubwürdige Tests die Integrität und Sicherheit von digitalen Produkten zu analysieren und zu beurteilen.[74]

Dieses Labor orientierte Prüfinstitut würde Prüfpläne ausarbeiten und Testmethoden und -prozesse festlegen. Das Prüfinstitut würde Einfluss auf die Ausarbeitung von Security Labels nehmen und gleichzeitig Normen und Empfehlungen von normgebenden Institutionen (Schweizer Akkreditierungsstelle SAS, Electrosuisse) übernehmen und die eigenen Tests gegebenenfalls entsprechend anpassen. Mit dem NCSC würde das Prüfinstitut Informationen austauschen, sodass Tests neue Angriffsmuster berücksichtigen können und auf der anderen Seite Warnungen betreffend Schwachstellen und Befunde zurückgespielt werden können. Auch mit der ENISA würde ein internationaler Austausch bezüglich Standards (EUCC) erfolgen.

Die Situation in relevanten Vergleichsländern und auch die Sicherheits-Regulierungen in anderen Technikbereichen legen nun aber das Modell einer organisatorisch-institutionellen Differenzierung von Prüfinstitut und Prüfstelle nahe. Das Institut funktioniert dabei als – in vielen Fällen hoheitliche – Instanz, welche Prüfungen organisiert und autorisiert und dabei mit verschiedenen (von ihm oder von einer Akkreditierungsstelle anerkannten) Prüfstellen bzw. Labors zusammenarbeitet. In diesem Modell, das jenem des BSI oder der ANSSI, aber auch den Verhältnissen in den USA entspricht (vgl. Kapitel 2), ist das Prüfinstitut nicht primär eine wissenschaftlich-technische (Forschungs-)Einrichtung, sondern eine zwar inhaltlich kompetente, aber normativ ausgerichtete Audit- und Controlling-Stelle.

Demnach ergibt sich die Arbeitsteilung zwischen dem normgebenden, kontrollierenden und zertifizierenden Prüfinstitut und einer Reihe akkreditierter Labors bzw. Prüfstellen. Das normative Prüfinstitut würde

- zusammen mit der Industrie und den Hochschulen Zertifizierungsschemata und Standards definieren und weiterentwickeln und sich darum kümmern, dass diese richtig angewandt und bekannt gemacht werden sowie im Einklang mit internationalen Standards stehen. Dazu sollte das Prüfinstitut die Führung einer entsprechenden Workgroup übernehmen.
- zusammen mit der Workgroup das Zertifizierungsschema, die Security Levels, den Umfang von Tests sowie die Prozesse und Methoden bestimmen.
- die Akkreditierungen von externen Labors durchführen (nach Kriterien wie physische Sicherheit, Datensicherheit sowie Erfahrung und technische Möglichkeiten).

- eine Liste der akkreditierten Labors führen und Auftraggeber beraten, welches Labor für eine bestimmte Prüfung geeignet ist.

Das Prüfinstitut als Instanz müsste mit der SAS zusammenarbeiten: Akkreditierungen, die vom Prüfinstitut vergeben werden, sollten auch von der SAS anerkannt sein. Ebenso wichtig ist eine enge Zusammenarbeit mit dem NCSC. Auf der privaten Seite würden eine Reihe von Unternehmen für die Durchführung von Prüfungen benötigt, wie beispielsweise Compass Security (CH, DE), EDSI Security (FR), Frauenhofer SIT (DE), GoSecurity (CH), InfoGuard (CH), Kudelski Security (CH), Oneconsult AG (CH, DE), CertX (CH)[75], SySS GmbH (DE), TÜV (DE, AT).

Um die Idee der technisch/wissenschaftlichen Kompetenz (plus der entsprechenden Ausstrahlung und Legitimation) des Prüfinstituts zu bewahren, wurde von verschiedener Seite auch eine Art Zweiteilung der Organisation vorgeschlagen. Neben der Kapazität für die Abwicklung von Prüfaufgaben (in der Regel unter Zuhilfenahme von externen Labors) sollte der Organisation auch eine «Innovationsabteilung» oder eine andere auf wissenschaftliche Forschung ausgerichtete Gruppe zur Organisation angehören. Die erwähnten Institutionen aus Deutschland und Frankreich verfügen (auch als Teile grösserer Organisationen) über die wissenschaftlich-technischen Kompetenzen für anforderungsreiche Prüfungen, nehmen aber solche in aller Regel kaum selbst vor.

6.1.2 Differenzierung B: Neue Institution vs. Anbindung/Integration in bestehende Organisation

Die zweite Diskussion unter den Experten betrifft die Selbstständigkeit der neuen Einrichtung bzw. deren Anbindung oder gar Integration in bestehende Strukturen. Wegen der Gefahr von Doppelspurigkeit und dem akuten Mangel an Experten wird dabei für eine Integration in (oder eine Anbindung an) vorhandene Kompetenzen argumentiert.

Für eine neue Einrichtung spricht demgegenüber die Trägheit der bestehenden Strukturen, nicht zuletzt in der Bundesverwaltung. Im Wissenschaftsbereich und erst recht in der Privatwirtschaft ist es hingegen möglich, sehr rasch neue und relativ unabhängige Kompetenzzentren zu schaffen. Beim Entscheid für eine Einbindung bestehen verschiedene Möglichkeiten für Trägerschaften, Partnerschaften und Legitimierungsinstanzen, aber auch unterschiedliche Vorgaben für Umfang und Qualifikation der Organisation und deren Ausstattung. Höchste Priorität hat jedoch die Unabhängigkeit des Prüfinstituts. Dies schliesst Partnerschaften mit dem Bund, mit Verbänden, Think Tanks und grossen Tech-Firmen keineswegs aus. Aus Gründen der Glaubwürdigkeit liesse sich das Prüfinstitut als Stiftung institutionalisieren, wobei der Bund (und interessierte Kantone wie Zug) Stifter werden sollten.

6.2 Mögliche Gestaltungen des Prüfinstituts

Aus den genannten Differenzierungen ergibt sich folgender Entscheidungsbaum für Varianten des Prüfinstituts entlang pragmatischer Prioritäten:

Differenzierung A

- Prüfinstitut mit eigener Prüfkapazität (was die Zusammenarbeit mit spezialisierten Prüfstellen je nach Fragestellung nicht ausschliesst) oder
- Prüfinstitut als Instanz (Herr des Verfahrens mit Vermittlung/Überwachung von Prüfungen, die ausschliesslich von externen Prüfstellen bzw. Labors durchgeführt werden).

Differenzierung B

- Prüfinstitut als neue, selbstständige und unabhängige Organisation mit einer eigenen Trägerschaft (präferenziell eine Form von PPP). In diesem Fall stellen sich zusätzlich die Fragen nach:
    - Rechtsform und Trägerschaft
    - Aufträge/Partnerschaften
    - Personal [= Kombination der Listen]

  oder
- Prüfinstitut als Teil, Ausbau oder Ergänzung einer bestehenden Organisation. In diesem Falle stellt sich die Frage nach dem geeigneten institutionellen Gefäss bzw. einer möglichen Mutter- oder Partnerorganisation. Genannt werden in diesem Zusammenhang:
    - NCSC, also Einbettung in die Bundesverwaltung
    - Electrosuisse, also ein Prüfinstitut als zusätzlicher Geschäftsbereich
    - EMPA
    - Prüf- und Sicherheitsfirmen wie SGS, Kudelski usw.

Resultierende Kombinationen

Die Varianten lassen sich in folgender Tabelle zusammenfassen:

	A1: Institut *mit* Prüfstelle/Testlabor	**A2: Instanz *ohne* Prüfstelle/Testlabor**
B1: Eingebunden	(Siehe Abschnitt 6.2.1) - Abteilung von EMPA - Anstalt, Institut oder Zentrum im ETH-Bereich - Aufgaben übernommen von Armasuisse W+T - Einbindung in private Trägerfirma (SGS, Kudelski usw.	(Siehe Abschnitt 6.2.3) - Zuordnung zu NSCS - Neue Gruppe/Abteilung von Electrosuisse - Trägerschaft durch Verband/Verein (ICTswitzerland, asut, Swiss Cyber Experts usw. - Aufgabe übernommen von Comcom, EDÖB usw. (Kommission, Beauftragter)
B2: Selbstständig	(Siehe Abschnitt 6.2.2) - Neue Institution mit eigener Trägerschaft - PPP (Stiftung) - Privat (Firma, Verein)	(Siehe Abschnitt 6.2.4) - Neue Instanz - Nach Modell Comcom, Elcom oder EDÖB - Konstituierung als eigene (internationale) Organisation (wie Rotes Kreuz, Swiss Digital Initiative)

Die Frage der Anbindung oder Unabhängigkeit des Prüfinstituts und die mögliche Verbindung mit anderen Organisationen ist vom Charakter des Prüfinstituts (Instanz oder Testlabor) nicht unabhängig. Auch wenn Optionen für alle vier Kombinationen angegeben werden können, sind diese nicht gleich gewichtig.

Innerhalb der vier Felder sind jeweils mehrere mögliche Ausgestaltungen des Prüfinstituts aufgelistet, und zwar in der Reihenfolge der geschätzten Machbarkeit. Diese Einschätzung wird im Folgenden für die vier Kombinationen erläutert. Die Konzentration auf näher liegende bzw. «realistischere» Verbindungen zu einzelnen Institutionen schliesst selbstverständlich eine breite Zusammenarbeit des Prüfinstitut mit anderen Einrichtungen nicht aus.

6.2.1 Eingebundenes Institut mit Labor/Prüfstelle (A1/B1)

Einige Fachexperten und Vertreter der Politik verfolgten bisher die Idee einer neuen ETH-Anstalt. Auch über ein ausgelagertes ETH-Kompetenzzentrum (à la Campus in Sitten) wurde diskutiert. Nicht im Sinne einer Ein- oder Angliederung, aber als Modell wird auch häufig das «Labor Spiez» genannt (welches als völlig unabhängiges und forschungsorientiertes Prüfinstitut wahrgenommen wird, aber organisatorisch und rechtlich ein Geschäftsbereich des Bundesamtes für Bevölkerungsschutz ist und damit zum VBS gehört).

Eine Angliederung des Prüfinstitutes mit einem gewichtigen und innovativen Labor kann nur an eine Institution erfolgen, die selbst in der industriell-

technischen Forschung tätig ist. Das ist in der Schweiz der ETH-Bereich. Nach zahlreichen Vorstössen und ETH internen Abklärungen wird eine solche Einrichtung von den ETH-Gremien jedoch ausgeschlossen.

Eine Anbindung an Armasuisse W+T wäre von den dort vorhandenen Cyber-Kompetenzen her interessant. Wahrscheinlich würde sich aber die Frage der gesetzlichen Voraussetzungen stellen. Es scheint zumindest fraglich, ob ein PPP-Modell, wie es Armasuisse W+T für andere Projekte betreibt, als Grundlage für eine solche Ausweitung der Aufgaben und des Kundenkreises genügen würde.

Schliesslich ist eine Delegation der Kompetenzen an eine private Trägerfirma denkbar. Aufgrund Bedenken betreffend Unabhängigkeit und Neutralität wurde dieser Ansatz für die Schweiz nicht weiterverfolgt.

6.2.2 Selbstständiges Institut mit Labor/Prüfstelle (A1/B2)

Die Vorstellung einer neuen, unabhängigen und umfassenden Institution war und ist die Motivation für die AG Prüfinstitut und deren Vorläuferin, der Arbeitsgruppe Supply Chain der Cybersecurity-Kommission von ICTswitzerland. Besonderes Gewicht wird dabei auf die Unabhängigkeit gelegt, da die Beschaffer bzw. Kunden als mögliche Kunden/Auftraggeber der Prüfinstanz in den komplexen Lieferketten immer auch als Hersteller auftreten können. Zur Wahrung der Unabhängigkeit gegenüber dem Markt erscheint daher eine zumindest teilweise öffentliche Finanzierung des Prüfinstituts im Sinne eines Service Public angemessen.

Wie oben erwähnt, würde sich dieses unabhängige Institut in zwei Kernbereiche gliedern:

- Der *kontrollierende und ausführende Bereich* nimmt Prüfaufträge auf nationaler (und internationaler) Ebene entgegen, koordiniert die Zusammenarbeit und Weiterleitung an geeignete Prüfstellen bzw. -labore, nimmt von diesen die Ergebnisse entgegen, berät Unternehmen, Behörden und Betreiber kritischer Infrastruktur in Prüfangelegenheiten, koordiniert die internationale Zusammenarbeit und fungiert als nationaler Ansprechpartner in der Schweiz.
- Der *Innovations- und Forschungsbereich* – im Idealfall eine unkonventionelle Forschungsgruppe von internationalen Cyberexperten aus den Bereichen Defence und Forensik – würde das Ziel verfolgen, die Bedürfnisse des Schweizer Markts zu antizipieren, das Sicherheitsniveau in der Schweiz ganzheitlich zu verbessern und die Reputation des Prüfinstituts international zu festigen.[76]

6.2.3 Eingebundenes Institut ohne Labor/Prüfstelle (A2/B1)

Wenn das Prüfinstitut sich auf die Definition, Organisation und Kontrolle der Prüfungen konzentriert, also nicht selbst ein Labor betreibt bzw. forscht, stellt sich die Frage nach der organisatorischen Anbindung anders als im Falle des Instituts mit Labor. Die Mutter- bzw. Partnerorganisation muss nicht primär ein wissenschaftlich-technisches, sondern muss ein vom Markt anerkanntes und kompetentes regulatives Umfeld bieten, in welchem erprobte Prozeduren und Zuständigkeiten bestehen. Im Fall der Sicherheit der vernetzten Geräte bieten sich hier zwei Pfade an:

- das NCSC als zentrale Kompetenz für Cyber-Security-Fragen bzw. als Quasi-Ersatz für die zuständigen Ämter in Deutschland und Frankreich. Einige Stimmen schlagen im Sinne einer Konzentration der Kompetenzen sogar eine «Unterstellung» des Prüfinstituts unter das NCSC vor. In der Praxis würde es sich bei dieser Umsetzung wohl um einen zusätzlichen Auftrag für das NCSC handeln, wobei die dafür notwendige Kapazitätserweiterung eine hohe Hürde darstellt.
- der private Fachverband Electrosuisse als Sicherheits-Überprüfungsorganisation, national mandatiert (Starkstrominspektorat) und international vernetzt. Electrosuisse arbeitet an einer Norm für Cyber-Sicherheit mit dem Ziel, eine entsprechende Zertifizierung für kritische Infrastrukturen und ein Label (oder eine «Unbedenklichkeitserklärung») für weit verbreitete vernetzte Geräte zu entwickeln.

Zwei weitere Varianten einer institutionellen Verankerung sind in der Schweiz bekannte Modelle für die Bewältigung spezieller Herausforderungen. Im ersten Fall würden die betroffenen Branchen via die Verbände die Trägerschaft für die neue Institution übernehmen – quasi im Sinne einer Selbstkontrolle. Angesichts der grossen Aufwendungen für das Prüfinstitut und der Zurückhaltung der Hersteller/Lieferanten erscheint die Verbandsträgerschaft als wenig aussichtsreich. Zudem würde wohl argumentiert, dass mit dem Fachverband Electrosuisse schon eine zumindest verbandsnahe Rahmenträgerschaft zur Verfügung stehen würde. Im anderen Fall könnte das Mandat einer bestehenden Regulierungsbehörde ausgeweitet werden. In Frage käme hier die Comcom oder allenfalls auch der Eidgenössische Datenschützer. Die Beurteilung der Sicherheit von vernetzten Geräten ist allerdings eine so umfassende und komplexe Aufgabe, dass die bestehenden Regulierer personell massiv erweitert bzw. komplett umgebaut werden müssten.

6.2.4 Selbstständiges Institut ohne Labor/Prüfstelle (A2/B2)

Auch wenn einer Integration des Prüfinstituts ohne Labor in bestehende Regulierungsorganisationen wenig Chancen eingeräumt werden, könnten diese als Modell dienen. Sowohl Comcom als auch Elcom (sowie im ökonomischen Bereich auch die Wettbewerbskommission) sind klassische Miliz-Organisationen, bei

denen der Staat auf privates Fachwissen und Erfahrungen in der Wirtschaft zurückgreift. Diese Formel, die auch im NCS-Umsetzungsplan 2018/22 mehrfach beschworen wird, liesse sich auch für die Regulierung der Cyber-Sicherheit von Geräten anwenden. Dazu müsste eine Gruppe von Experten aus den Branchen und Fachkreisen berufen und mit einem behördlichen Mandat ausgestattet werden. Infrage dafür kämen u.a. Mitglieder des Public Private Partnerships «Swiss Cyber Experts»[77], die in der Vergangenheit von Bundesstellen wiederholt ad personam für Problemlösungen beigezogen wurden. Dieser Kreis könnte als Ausgangspunkt für eine Prüfinstanz via befugte Experten dienen. Allerdings müsste dann – ähnlich wie bei Comcom und Elcom oder beim Eidgenössischen Preisüberwacher – eine gesetzliche Voraussetzung geschaffen werden.

Eine weitere Möglichkeit einer Zusammenarbeit von Staat und privaten Akteuren wäre auch im Falle des selbstständigen Instituts ohne Labor eine Stiftung, in der private Firmen und staatliche Akteure (Bund, Kantone) vertreten wären. Eine solche unabhängige Prüfinstanz könnte als Geräte orientierte Schwesterorganisation der Swiss Digital Trust Stiftung bzw. als deren Ergänzung konzipiert werden.

6.3 Aufbau und Rekrutierung von Personal

6.3.1 Team für die Betriebsaufnahme

Die Anregungen aus der Arbeitsgruppe beziehen sich sowohl auf ein Prüfinstitut ohne als auch auf ein solches mit Labor. Ein Team von fünf bis acht Personen zur Lancierung des Instituts wird vorgeschlagen. Neben einer Leitungsperson mit sehr guten Beziehungen zu den Hochschulen und zur Industrie und einer erfahrenen administrativ-organisatorischen Kraft würden rund fünf technisch qualifizierte Mitarbeitende zur Start-Belegschaft gehören. Im Falle eines Instituts mit Labor würde dieses Team auch Tester und Researcher umfassen. Die Leitungsfunktionen könnten u.U. auch von zwei Personen abgedeckt werden, wobei sich die eine auf Stakeholder in Verwaltung und Wirtschaft, die andere auf den Kontakt zu den Hochschulen und zur Forschung konzentrieren würde.

6.3.2 Profile

Die Mitarbeitenden sollten einen Fach- oder Hochschulabschluss in Elektrotechnik, Informatik, Physik usw. sowie einige Jahre praktische Erfahrung in Cyber-Security mitbringen. Im Falle der Tester oder Testkoordinatoren wird von einer mindestens fünfjährigen Erfahrung ausgegangen; bei den Forschenden, die weltweit Untersuchungen zu neuen Technologien, Methoden und Angriffsszenarien durchführen sollen, von mindestens 10 Jahren. Erforderlich sind fachliche Kenntnisse u.a. in den Disziplinen Informationssicherheit, IT-Sicherheit, Pentesting, Coding und Reverse Engineering. Je nach Qualifikation und Erfahrung

werden die Gehälter auf 80K bis 200K CHF geschätzt. Es ergibt sich so eine jährliche Lohnsumme inklusive Sozialversicherung usw. von nicht ganz 2 Mio. CHF.

6.3.3 Spezifische Anreize

Der Mangel an Experten im ICT-Bereich im Allgemeinen und im Feld der Cyber-Sicherheit im Speziellen ist notorisch. Ebenso wird immer wieder auf das Lohngefälle zwischen Stellen im öffentlichen Bereich bzw. an den Hochschulen und jenen bei grossen Tech-Firmen hingewiesen. Es liegt deshalb auf der Hand, dass eine Rekrutierung für das Prüfinstitut nur über intrinsische Anreize Erfolg haben kann.

Um die Erwartungen der hochqualifizierten Mitarbeitenden zu befriedigen, müssten

- eine Lern- und Interessenskultur geschaffen werden,
- eine enge Zusammenarbeit mit Hochschulen und thematisch passenden Studiengängen angestrebt werden, einschliesslich der Betreuung von Dissertationen und Abschlussarbeiten sowie die Finanzierung von Lehrstühlen und Forschungsprojekten,
- umfangreiche Weiterentwicklungs- und -bildungsmöglichkeiten angeboten werden,
- hohe ethische Standards in Bezug auf die Neutralität gegenüber den beteiligten Akteuren verfolgt werden.

6.3.4 Flexibler Einsatz von Ressourcen

Bei knappen personellen Ressourcen wird es – nicht nur in der Startphase – Situationen geben, in denen Prüfaufträge oder -erwartungen nicht erfüllt werden können. Aufgrund der Schnelllebigkeit und der Produktinnovation in der digitalen Welt lassen sich derartige Situationen kaum vermeiden. Kann die Prüfinstanz einen Auftrag aufgrund hoher Anforderungen an Vertraulichkeit oder technische Tiefe nicht an eine Prüfstelle delegieren, werden die entsprechenden Anforderungen in die thematische und personelle Ausrichtung der Prüfinstanz einfliessen, um künftige, ähnlich gelagerte Anfragen beantworten zu können.

Ohnehin braucht es einen kontinuierlichen Prozess zur Früherkennung sowie Partnerschaften mit anderen Wissensträgern. Beispielsweise könnten Forschungsaufträge an Hochschulen vergeben werden. Ebenso könnten bestehende Prüflabors zu gemeinsamen Aktionen motiviert werden, wie z.B. Hackathons, Bug-Bounty-Programme usw. Weiter liessen sich Netzwerke und Partnerschaften mit Herstellern aufbauen, um frühzeitig in die Produkteentwicklung involviert zu werden. Zusätzlich könnte das Prüfinstitut den Bund und die Kantone

im Bereich der Sicherheit beraten und öffentliche Intrusion-Tests organisieren, durchführen und begleiten.[64]

6.4 Anforderungen an die physische Infrastruktur

Diese hängen in hohem Ausmass vom letztlich gewählten Modell des Prüfinstituts ab. Wenn man vom Labor absieht, ergeben sich aus der skizzierten Personalstruktur grobe Anforderungen an den Bürobedarf (inklusive 2–3 Sitzungszimmer plus einem Seminarraum) von ca. 150–200 qm.

Laborräumlichkeiten müssten mit der ISO-Norm für Prüflabors kompatibel sein, vgl. dazu z.B. Akkreditierungs-Anforderungen des BSI. Eine Ausrüstung für Reverse Engineering wäre abhängig davon, was primär geprüft werden soll. Auf jeden Fall müssten partnerschaftliche Lösungen mit Institutionen gesucht werden, wo entsprechende Gerätschaften bereits vorhanden sind. Die Schätzungen für entsprechende Investitionen gehen auseinander. Für die Prüfung von Smart-Home-Komponenten käme man nach einer Schätzung mit einer relativ günstigen Ausrüstung (ca. 100K CHF) in einem ersten Schritt schon weit. Gleichzeitigt warnt der Vertreter einer internationalen Prüffirma vor sehr hohen Aufwendungen für ein Prüflabor. Ein zweistelliger Millionenbetrag sei schnell erreicht. Vielmehr sollten externe Labors oder die Infrastruktur von Hochschulen in Anspruch genommen werden.

7 Fazit und nächste Schritte

Unter den in Kapitel 6 beschriebenen Möglichkeiten für die Lancierung eines Prüfinstituts kommen in einer Gesamtschau und unter realistischen schweizerischen politischen und rechtlichen Bedingungen nur wenige Pfade in Frage. Das Folgende ist der Versuch einer solchen selektiven Einschätzung, verbunden mit Vorschlägen für konkrete Schritte.

Ein unabhängiges Institut mit einem gewichtigen, ja identitätsbestimmenden Labor (siehe Abschnitt 6.2.2) könnte in vernünftiger Frist nur aus dem Bereich der Hochschulen heraus geschaffen werden, was nach zahlreichen Vorstössen und ETH internen Abklärungen von den ETH-Gremien ausgeschlossen wurde.

Gegen andere Pfade zu einem Institut mit Labor sprechen die Verhältnisse in wichtigen Referenzländern und auch die Regulierungen in anderen technischen Feldern, in erster Linie im Elektrobereich. Das vorherrschende regulatorische Modell ist die Trennung zwischen Normierungs- und Zertifizierungsinstanzen (mit teilweise hoheitlichen Mandaten und in Verknüpfung mit der Expertise in den Industrien) und den privat organisierten Labors und Prüfstellen einschliesslich zahlreicher Firmen, die Penetrationstests und andere Prüfungen anbieten.

Wenn man sich also aufgrund des bisher gezeigten Desinteresses der ETH und der normativen Landschaft im In- und Ausland auf das Prüfinstitut ohne Labor, also auf das Prüfinstitut als kompetente, normsetzende kontrollierende und koordinierende Prüfinstanz konzentriert, so gehen die Vertreter der Lösung «Prüfinstitut als Prüfinstanz» davon aus, dass die Prüfaufgabe für vernetzte Geräte in der Schweiz ähnlich organisiert sein sollte wie in anderen Ländern (siehe Kapitel 2). Folglich ergibt sich die Arbeitsteilung zwischen dem normgebenden, kontrollierenden und zertifizierenden Prüfinstitut und einer Reihe akkreditierter Labors bzw. Prüfstellen, wie in Abschnitt 6.1.1 beschrieben. In der institutionellen Landschaft der Schweiz verbleiben nur zwei plausible Pfade für die Umsetzung bzw. die Verankerung der neuen Einrichtung:

- Die erste wäre die Konzentration der Expertise und der Ressourcen durch eine Anbindung bzw. «Unterstellung» der bisherigen Initianten und Interessierten unter das NCSC.
- Die andere Umsetzung wäre die Fortsetzung, Intensivierung und der Ausbau der Initiative im Schosse von Verbänden bzw. Branchenorganisationen, beispielsweise ICTswitzerland oder Electrosuisse.

Die Lancierung einer komplett neuen Struktur, die dennoch einer hoheitlichen Legitimation und einer internationalen Verankerung bedarf, erscheint angesichts der heute schon verzettelten Kräfte mehr als hürdenreich.

Welche der beiden Lösungen priorisiert wird, sollte pragmatisch entschieden werden. Angesichts der lang andauernden Diskussionen in der

Bundesverwaltung über die Zuständigkeit für Cyber-Sicherheit und der vielen Koordinationsgremien ist eine verwaltungsorganisatorische oder staatspolitische Diskussion über die «richtige» Lösung nicht zielführend. Allerdings dürfte der Rahmen von ICTswitzerland und Electrosuisse eine etwas grössere Flexibilität für den Einbezug privater und vielleicht auch kantonaler und kommunaler Mitträger bieten.

Der prioritäre Vorschlag geht also dahin, das Prüfinstitut institutionell im Umfeld der Branchenorganisationen anzusiedeln. Dazu sollten von den bisherigen Initianten (ICTswitzerland AG Supply Chain, Zuger Initiative AG Prüfinstitut, Regierungsrat Zug) rasch Verhandlungen mit den Organisationen aufgenommen werden, allenfalls unter Einbezug des UVEK und des WBF/SECO.

Unter den Branchenorganisationen scheint Electrosuisse als unabhängiger Fachverband für Elektro-, Energie- und Informationstechnik mit Dienstleistungsangeboten zu Normung, Inspektion, Prüfung, Zertifizierung, Beratung und Weiterbildung geeignet, ein neues Prüfinstitut in Zusammenarbeit mit weiteren Branchenorganisationen aufzubauen.[18] Electrosuisse beheimatet bereits das Elektrotechnische Komitee (CES), die Normenorganisation im Bereich der Elektrotechnik in der Schweiz, und führt das Eidgenössische Starkstrominspektorat (ESTI) als besondere Dienststelle im Auftrag des Bundes, weswegen die oft geforderte Verankerung beim Bund mit vernünftigem Aufwand realisierbar scheint.

Eine gemischtwirtschaftliche Finanzierung im Sinne eines Public-Private-Partnerships scheint angesichts der vielen interessierten Kreise durchführbar.

In welcher rechtlichen Form dies geschieht, muss nicht sofort festgelegt werden. Von mehreren Initianten wird die Gründung einer Stiftung vorgeschlagen, nicht zuletzt wegen der damit demonstrierten Unabhängigkeit und Glaubwürdigkeit. Der Bund (und interessierte Kantone wie Zug), aber auch mögliche Partner wie die Hochschulen, grosse Tech-Firmen, die SAS, das NCSC, armasuisse W+T sowie der EDÖB sollten als Stifter gewonnen werden. Unter Umständen sind auf dem gegenwärtigen Stand der Abklärungen Lösungen mit einem Verein oder sogar einer einfachen Gesellschaft ebenfalls naheliegend.

Eine wesentlich grössere Hürde für das Prüfinstitut als die juristische Form ist die notwendige gesetzliche Grundlage. Electrosuisse bzw. das ESTI stützt sich auf die Verordnung über das Eidgenössische Starkstrominspektorat (ESTI-Verordnung), die ihre Grundlage im Elektrizitätsgesetz von 24.6.1902 hat.[78] Als Ansatzpunkte für die Cyberprüfungen werden das Produktehaftpflichtgesetz (insbesondere die Paragraphen 3 und 4) und das Produktesicherheitsgesetz (PrSG) diskutiert.

Endnoten

[1] Die Details finden sich im Bericht, welcher unter Link heruntergeladen werden kann.

Kapitel 1

[2] Vergl. Benjamin C. Dean: *An Exploration of Strict Products Liability and the Internet of Things*. Center for Democracy & Technology, April 2018.

[3] Artikel «Ripple20 erschüttert das Internet der Dinge» vom 17.06.2020: «Eine Reihe von teils kritischen Sicherheitslücken in einer TCP/IP-Implementierung gefährdet Geräte in Haushalten, Krankenhäusern und Industrieanlagen. Wenn ein paar Netzwerkpakete dazu führen können, dass auf einem Gerät beliebige Befehle ausgeführt werden, bedeutet das allerhöchste Alarmstufe. Genau die ist für viele Geräte aus dem Internet der Dinge jetzt angebracht: Ein Forscherteam hat reihenweise Sicherheitslücken in einer schlanken TCP/IP-Implementierung der Firma Treck entdeckt. Und die nutzen vernetzte Steckdosen, medizinische Geräte, Sensoren industrieller Steuerungen und vieles mehr. Der TCP/IP-Stack ist die verwundbarste Stelle von Netzwerkgeräten, da er als erste Instanz alle Netzwerkdaten verarbeiten muss – auch die bösartigen eines Angreifers. Ein Programmierfehler an dieser Stelle führt sehr häufig zu kritischen Sicherheitslücken. Der TCP/IP-Stack von Treck ist für Embedded Geräte optimiert und wird etwa von Firmen wie HP, Intel, Schneider Electric, Rockwell Automation und vielen anderen genutzt.» Siehe https://www.heise.de/security/meldung/Ripple20-erschuettert-das-Internet-der-Dinge-4786249.html

[4] Vgl. Präsentation von L. Dobszay, electrosuisse.

[5] Für das autonome Fahren wird die Vernetzung via 5G und anderen Technologien zur essenziellen Bedingung. Die Sicherstellung der Sicherheit der gesamten Lieferkette ist gemäss Strassenverkehrsordnung Art 31 (Beherrschen des Fahrzeugs) und Art. 29 (Betriebssicherheit des Fahrzeugs) implizit vorgeschrieben. Allfällige Haftungsfragen können im Falle von autonom fahrenden Fahrzeugen nur mit technischer Expertise beantwortet werden. Dazu zählen die Beweisführung, die Unfallaufnahme, die Unfallrekonstruktion usw.

[6] So wurden heimlich Mikrochips in Hauptplatinen implantiert, die in China hergestellt und von dem in den USA ansässigen Unternehmen Supermicro verkauft wurden. Siehe

- H.M. Micah Lee, *Everybody does it: the messy truth about infiltrating computer supply chains*, https://theintercept.com/2019/01/24/computer-supply-chain-attacks/, 24.01.2019;
- J. Robertson und M. Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, 04.10.2018
- J. Robertson und M. Riley, *New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom*, 09.10.2018.

Zudem war der Flugzeughersteller Airbus von einer Reihe von Cyberangriffen betroffen, die auf die Computersysteme seiner Hauptzulieferer abzielten, und zwar im Rahmen einer vermutlich koordinierten Kampagne von Hackern, siehe

- D. Riley, *Airbus hit by cyberattack that targeted key suppliers*, https://silicon-angle.com/2019/09/26/airbus-hit-cyberattacks-targeted-key-suppliers/, 26.09.2019.

[7] Erschwerend kommt hinzu, dass die Kosten für Angriffe auf die Beschaffungskette oft sehr gering sind, siehe

- A. Greenberg, *Planting Tiny Spy Chips in Hardware Can Cost as Little as $200,* https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/, 10.10.2019.

[8] Ein Botnetz mit kompromittierten IoT-Klimageräten und -Heizungen kann beispielsweise die Stromversorgung einer ganzen Region bedrohen. Siehe

- S. Soltan, P. Mittal und H. V. Poor, *BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid,* https://www.usenix.org/conference/usenixsecurity18/presentation/soltan, 15.08.2018.

[9] Darunter fällt die Nichtverfügbarkeit von Dienstleistungen (beispielsweise im Gesundheitswesen) und Angeboten (beispielsweise der Ausfall von Zügen).

[10] Siehe J. FitzPatrick: *Hardware Implants,* https://securinghardware.com/articles/hardware-implants/, 04.10.2018.

[11] Reverse Engineering bezeichnet den Vorgang, die Konstruktionselemente aus einem bestehenden System durch Untersuchung der Strukturen, Zustände und Verhaltensweisen zu extrahieren. Für Softwaresysteme liegt das Ziel insbesondere in der Beschreibung vom Quellcode oder einer vergleichbaren Beschreibung sowie der Beschreibung eines Kommunikationsprotokolls aus der Beobachtung der Kommunikation.

[12] Bei einem Angriff über die Lieferkette können Komponenten während oder bereits vor der Lieferung an den Endabnehmer manipuliert werden. Dies kann im Falle staatlicher Angriffe bereits bei der Entwicklung von Chips, bei der Herstellung oder Integration von Komponenten oder während des Transports zum Endabnehmen geschehen, siehe

- Süddeutsche Zeitung: *Netztechnik nur noch von „vertrauenswürdigen Lieferanten",* https://www.sueddeutsche.de/wirtschaft/telekommunikation-netztechnik-nur-noch-von-vertrauenswuerdigen-lieferanten-dpa.urn-newsml-dpa-com-20090101-190307-99-283834, 07.03.2019, sowie:
- A. LaSota: *The Present and Potential Future of Mac Hardware Impl*ants, https://osf.io/enup4, 19.03.2019.

Im Unterschied zu traditionellen d.h. nicht vernetzten Produkten müssten dabei insbesondere folgende Risiken untersucht werden:

- Mit der steigenden Komplexität von Prozessoren und Chips verlagert sich die Bedrohung in Richtung des Designs von Chips und Komponenten. Dies schliesst die Entwicklungsumgebungen samt Software und Tools zum Design von Chips (auch der Lieferanten) mit ein [siehe oben 2].
- Integrierte Fehlfunktionen oder Backdoors in vernetzten Produkten können auch nach der Auslieferung aktiviert werden, z.B. durch ein Update.
- Vernetzte Produkte benötigen Security Updates vom Hersteller, und zwar während der gesamten Lebensdauer (die jene des Herstellers und v.a. jene des Lieferanten oft übertrifft).
- Vernetzte Produkte lassen sich individuell aus der Ferne manipulieren. Testverfahren sind entsprechend aufwändiger.

[13] Vergleiche dazu: Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, Hanan Hibshi: *Ask the Experts: What Should Be on an IoT Privacy and Security Label?* 2020 IEEE Symposium on Security and Privacy (SP). https://www.computer.org/csdl/proceedings-article/sp/2020/349700a771/1j2LfTRYbNC

[14] Die Kriminal- und Militärgeschichte zeigt, dass erfolgreiche Angreifer oft dort angreifen, wo die Verteidiger dies am wenigsten erwarten.

[15] Die Tätigkeiten der Angreifer beinhalten das versteckte Einbringen von Malware und Backdoors in Hardware und Software der Zielsysteme. Geheimdienste treffen vermehrt Massnahmen wie z.B. sogenannte «Kill Switches» (Notausschalter), um eine Sabotage von fremden Systemen vorzubereiten. Solche Funktionalitäten können sich z.B. in Software-Schwachstellen oder fest eingebauten Zugriffskonten für vermeintliche Wartungszwecke manifestieren. Die angegriffene Partei kann derartige Defekte kaum eindeutig einer gezielten Massnahme des Gegners zuordnen.

Die gezielte Kompromittierung ausgewählter Produkte einer Organisation oder Industrie erlaubt Zugriff und Einflussnahme in einem genau spezifizierten Umfeld wie spezieller Netzausrüstung (ISP, GSM usw.), Industrie-Kontrollsysteme (ICS), Industrial Internet of Things (IIoT) und speziell kritische Industrieprodukte (Militär, Energie, Medizin).

Kapitel 2

[16] Schweizer Verband für das Cyber-Sicherheitsgütesiegel https://www.cyber-safe.ch/de/schweizer-label-der-cyber-sicherheit/

[17] Swiss Digital Initiative:
- https://www.efd.admin.ch/efd/de/home/themen/Digitalisierung/swiss-digital-initiative.html
- https://digitalswitzerland.com/sdi/

[18] Electrosuisse ist ein Fachverband (für Elektro-, Energie- und Informationstechnik) mit Dienstleistungsangeboten zu Normung, Inspektion/Prüfung, Zertifizierung, Beratung und Weiterbildung. Der Verband besteht seit 1889 und engagiert sich seit über 130 Jahren für die sichere Erzeugung und Anwendung von Elektrizität. Electrosuisse verfügt über langjährige Erfahrung in der Erarbeitung und Anwendung von Sicherheitsvorschriften und technischen Normen und ist im Bereich der Elektrotechnik in den internationalen Normungs- und Zertifizierungsgremien gut vernetzt. Rechtlich ist Electrosuisse ein Verein.

Die Normenorganisation im Bereich der Elektrotechnik ist das Comité Électrotechnique Suisse (CES). Diese ist bei Electrosuisse beheimatet, d.h. Electrosuisse führt das Sekretariat, und der CES-Generalsekretär ist bei Electrosuisse angestellt. Der Vorstand des CES setzt sich aus Personen von Electrosuisse-Firmen- und institutionellen Mitgliedern zusammen. Die Mitarbeit in den technischen Komitees des CES setzt eine Mitgliedschaft bei Electrosuisse voraus. Siehe auch https://www.electrosuisse.ch/de/normung/ces/

Das Eidgenössische Starkstrominspektorat (ESTI) ist ein eigenständiger Bereich von Electrosuisse mit hoheitlichen/öffentlich-rechtlichen Aufgaben und wird als besondere Dienststelle im Auftrag des Bundes von Electrosuisse geführt. Siehe auch https://www.esti.admin.ch/de/das-esti/organisation-uebersicht/organisation/

Bis 2017 betrieb Electrosuisse das erste akkreditierte elektrotechnische Prüflabor der Schweiz, das vom international tätigen Konzern Eurofins-Scientific übernommen wurde. Seit 2018 erweitert Electrosuisse ihr Engagement auch auf das Thema Cyber-Security.

[19] Diskussionspapier Cyber-Security-Regulierung, Version 0.9, Electrosuisse (Levente J. Dobszay)

[20] Ein Auszug:

1. Herstellung, Inverkehrbringung, Wartung, Betrieb und Entsorgung von informationstechnischen Systemen sollen über ihren ganzen Lebenszyklus sicher nach den anerkannten Regeln der Technik erfolgen.
2. Bezüglich des Verkehrs von schützenswerten und insbesondere personenbezogenen Daten, den implementierten Funktionen, den verwendeten Komponenten und den damit verbundenen Sicherheitsrisiken soll mehr Transparenz geschaffen werden.
3. Die Souveränität über ein informationstechnisches System soll allein dem Systemeigner gehören.
4. Für die Teilnahme am vernetzten Datenverkehr soll ein Fähigkeitsnachweis («Internetführerschein») zum sicheren Betrieb von vernetzten informationstechnischen Systemen nach den anerkannten Regeln der Technik vorausgesetzt werden.
5. Verstösse gegen Mindestsicherheitsstandards, welche eine Gefährdung der Cyber-Sicherheit für Dritte darstellen, sollen wirksam sanktioniert werden.
6. Nicht den zwingenden Sicherheitsvorschriften entsprechende informationstechnische Systeme müssen identifiziert und ausser Betrieb gesetzt beziehungsweise vom Markt genommen werden. Die dafür nötige Transparenz und Rückverfolgbarkeit muss sichergestellt werden.

[21] https://www.bsi.bund.de/DE/Presse/BSI-Kurzprofil/kurzprofil_node.html

[22] https://www.bsi.bund.de/DE/DasBSI/Aufgaben/AbteilungSZ/AbteilungSZ_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/Organisationsplan_IFG_pdf.pdf?__blob=publicationFile&v=13

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Stellen.pdf?__blob=publicationFile&v=12

[23] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Produkte.pdf?__blob=publicationFile&v=12

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Zertifizierte-IT-Sicherheit.pdf?__blob=publicationFile&v=9, S. 11

[24] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/ITSEC_CC/CC_Liste/CC_Liste_node.html, abgerufen am 23.12.2019

[25] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/zertifizierungnachcc_node.html, abgerufen am 23.12.2019

[26] https://www.secuvera.de/bsi-pruefstelle/beschleunigte-sicherheitszertifizierung-bsz/

[27] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/Standortzertifizierung/Standortzertifizierung_node.html

[28] https://www.lancom-systems.de/blog/mehr-sicherheit-im-netz-bsi-veroeffentlicht-technische-richtlinie-fuer-breitband-router/

[29] http://docs.dpaq.de/14069-bsi_lagebericht_2018.pdf, S. 68

[30] https://www.ssi.gouv.fr/en/organisation/executive-office/

[31] https://www.ssi.gouv.fr/entreprise/produits-certifies/certification-faq/

[32] https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/les-centres-devaluation/

[33] https://www.ssi.gouv.fr/uploads/2018/01/catalogue_solutions_qualifiees_anssi.pdf, S. 8

[34] https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-cer-p-01-certification-de-produits_v3.2.pdf

[35] https://www.ssi.gouv.fr/entreprise/produits-certifies/

[36] https://www.ssi.gouv.fr/en/certification/common-criteria-certification/

[37] https://www.stormshield.com/de/news/qualifizierte-sicherheitslosungen-die-entscheidung-fur-eine-vertrauenswurdige-losung/

https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/

[38] https://www.ssi.gouv.fr/administration/visa-de-securite/

[39] https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment/cyber-sicherheit-plattform

[40] https://www.a-sit.at/ueber-a-sit/

Die Durchführung der Konformitätsbewertungen muss anhand der durch die internationale Norm EN ISO/IEC 1706 vorgegebenen Qualitätssicherungsmassnahmen erfolgen, das eigene Qualitätsmanagement der Konformitätsbewertungsstelle hat daher einen dementsprechend hohen Stellenwert.

[41] ASIT: Die eIDAS-Verordnung regelt im Wesentlichen zwei Themenkreise:

- Vertrauensdienste, d.h. elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, Zustellung elektronischer Einschreiben, Website-Authentifizierung und Validierungs- sowie Bewahrungsdienste.
- Elektronische Identifizierung: Dabei werden Bedingungen für die Anerkennung von elektronischen Identifizierungsmitteln für natürliche und juristische Personen definiert, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen.

Seit der Akkreditierung wird A-SIT laufend von Anbietern von elektronischen Ausweisen, Unterschriften usw. für deren wiederkehrend notwendige Bewertungen herangezogen.

[42] https://www.inside-it.ch/articles/53619 und https://steiermark.orf.at/stories/3013646/

[43] Robert Hannigan, der erste Chef des NSCS, hat über den Aufbau und die Organisation dieser neuen Behörde ein interessantes Papier verfasst: Organising a Government for Cyber. The Creation of the UK's National Cyber Security Centre.

[44] https://www.ncsc.gov.uk/section/products-services/Introduction#section_1

[45] https://www.ncsc.gov.uk/information/products-cesg-assisted-products-service

[46] Inhalt Security Characteristics: https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa-security-characteristics

[47] Für Technologien, die für das Vereinigte Königreich von Interesse sind, wird UK zudem mit der Common-Criteria-Gemeinschaft an der Entwicklung relevanter CPP (und deren Begleitdokumenten) weiter zusammenarbeiten. Siehe auch: https://www.commoncriteriaportal.org/news/

[48] https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs/NIAP_NCSC_factsheet.pdf

https://www.niap-cevs.org/Documents_and_Guidance/cctls.cfm

[49] http://2014.kes.info/archiv/heft/abonnent/03-3/03-3-039.htm

[50] https://www.niap-ccevs.org/Ref/FAQ.cfm

https://www.nsa.gov/news-features/press-room/Article/1638898/niap-approves-first-private-industry-testing-labs-for-common-criteria-evaluatio/

[51] Liste der evaluierten Produkte: https://www.niap-ccevs.org/Product/

[52] https://www.tuvit.de/de/leistungen/hardware-software-evaluierung/fips-140-2/

[53]https://www.wko.at/service/aussenwirtschaft/innovation-aus-finnland-cybersecurity-label.html

https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label

https://portswigger.net/daily-swig/finland-launches-cybersecurity-label-for-iot-devices

[54] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3

[55] Verordnung (EU) 2019/881 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0881

[56] European Commission, Press Corner, Daily News, 12.03.2019, https://ec.europa.eu/commission/presscorner/detail/en/MEX_19_1653

[57] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

Kapitel 3

[58] Die Gründe dafür sind vielfältig. Neben den Entwicklungskosten steigen auch die Einführungszeit und somit die Einführungskosten der Produkte vor Markteintritt. Nach Inbetriebnahme stattfindende Überprüfungen verursachen weitere Prüf- und Nachbesserungsaufwände. In kritischen Bereichen (beispielsweise im Medizinalbereich) finden bereits punktuelle Sicherheitsprüfungen statt, die eigenverantwortlich organisiert sind und entsprechend zu Lasten der Betreiber (nicht der Hersteller oder Lieferanten) gehen.

[59] Die Firma für Anwendungssicherheit Veracode hat anhand 85'000 Anwendungen und 351'000 verwendeten Bibliotheken untersucht, wie viele Schwachstellen in Open-Source-Bibliotheken enthalten sind. https://nakedsecurity.sophos.com/2020/05/27/open-source-libraries-a-big-source-of-application-security-flaws/, 27.05.2020

[60] Open Source kann die Sicherheit nur dann erhöhen, wenn die veröffentlichten Teile des Programmcodes auch tatsächlich in den Paketmanagern zur Ausführung kommen. Dieser trivial lautende Umstand wird bis anhin nicht flächendeckend überprüft und mancherorts bereits ausgenutzt. Vergleiche https://medium.com/hackernoon/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5.

[61] Die fehlende Verpflichtung zu Änderungen und Nachbesserungen lässt sich anhand zahlreicher Beispiele belegen, so zum Beispiel in der Hotellerie (Marriot wurde über mehrere Jahre mehrfach Opfer von Cyberattacken). Auch zeigt der Fakt, dass für Cyberangriffe in den meisten Fällen seit

langem bekannte Schwachstellen ausgenutzt werden, da Anbieter und Betreiber von Diensten ihren Sorgfaltspflichten oft nicht nachkommen.

[62] Somit besteht ein Ansatzpunkt für Cyber-Sicherheits-Prüfungen, indem z.B. für IoT-Geräte in bestimmten Ländern etwas weitergehende Vorschriften gelten als von der ISO vorgegeben.

[63] Siehe Süddeutsche Zeitung, *Netztechnik nur noch von „vertrauenswürdigen Lieferanten",* https://www.sueddeutsche.de/wirtschaft/telekommunikation-netztechnik-nur-noch-von-vertrauenswuerdigen-lieferanten-dpa.urn-newsml-dpa-com-20090101-190307-99-283834, 07.03.2019.

[64] Besondere Situationen in der unmittelbaren Vergangenheit waren beispielhaft die Diskussionen um E-Voting und Covid-19 Tracing.

[65] Nach Auskunft des BSI beläuft sich diese Gebühr auf ca. 10% der Aufwendungen für die eigentliche Prüfung.

Kapitel 4

[66] Siehe auch Endnoten 2 bis 5.

[67] Dies schliesst die Entwicklungsumgebungen samt Software und Tools zum Design von Chips (auch der Lieferanten) mit ein.

[68] Vergleiche dazu BSI-Gesetz vom 17. Juli 2015, §8a und §8b.

[69] Eine Quantifizierung der Fälle, in denen ein CC-Label vorliegt, die betreffenden Geräte aber weder in Deutschland, Frankreich, UK noch USA geprüft worden sind, liegt nicht vor.

Kapitel 5

[70] Nicht immer beinhalten öffentliche Coderepositories (z.B. auf Github) den tatsächlich in Paketen enthaltenen und später ausgeführten Code. https://medium.com/hackernoon/im-harvesting-credit-card-numbers-and-passwords-from-your-site-here-s-how-9a8cb347c5b5

[71] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, Zinaida Benenson: *Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products*. 2020 IEEE Symposium on Security and Privacy (SP). https://www.computer.org/csdl/proceedings-article/sp/2020/349700a346/1j2LfHnkRPy

[72] Als Beispiel seien hier Techniken wie Port Knocking und Single Packet Authorization genannt. Im Unterschied zu Verbrennungsmotoren lassen sich Hintertüren zu gezielten Zeitpunkten punktuell aus der Ferne aktivieren und kurz darauf wieder deaktivieren, weswegen solche Zugänge auch bei Prüfungen im Feld kaum detektierbar sind**.**

[73] Die Angaben zu einem Prüfvorgang beinhalten neben den Prüfergebnissen und spezifischen Bemerkungen mindestens folgende grundlegende Informationen: eine eindeutige Beschreibung des Prüfobjekts (Typ-, Serien-, Stamm-, Versionsnummer), eine eindeutige Referenz der zugrundeliegenden Prüfspezifikation, das Prüfdatum, den Prüfort (Labor) und Informationen über den Prüfer (Name, Qualifikation).

Kapitel 6

[74] Vgl. dazu auch das White Paper der Supply-Chain-Arbeitsgruppe der Cyber-Security-Kommission von ICTswitzerland. https://ictswitzerland.ch/en/publikationen/mm-white-paper-supply-chain-security/

[75] CertX ist nach eigenen Angaben die erste schweizerische Zertifizierungsstelle, die auf internationaler Ebene (nach ISO17065) akkreditiert ist und Bewertungs- und Zertifizierungsdienste nach

industriellen Cyber-Sicherheitsstandards anbietet, typischerweise nach IEC62443, die in kritischen Infrastrukturen in verschiedenen Branchen wie Energie, Fertigung, Eisenbahn, Gesundheitswesen usw. angewandt werden. Siehe auch https://certx.com

[76] Von verschiedener Seite wird empfohlen, dass das unabhängige Prüfinstitut mit Prüflabor als Public-Private-Partnership (PPP) aufgestellt werden sollte, am besten in Form einer Stiftung. Angeregt wurde auch eine mögliche Trennung zwischen dem ausführenden Bereich in Form einer AG und dem Innovationsbereich (mit dem Labor) in Form der Stiftung. Diese Klärung muss auf eine spätere Phase des Projektes verschoben werden. Da das (aufwändige) Labor wahrscheinlich auch Dienstleistungen für Dritte erbringen könnte, d.h. als Prüfstelle gegen aussen auftreten würde, müsste u.U. eher dieser Teil als AG organisiert werden als der Instanz-Teil, der ja quasi-hoheitliche Aufgaben erfüllt.

[77] Swiss Cyber Experts, https://www.swiss-cyber-experts.ch/

[78] Die aktuelle Fassung des Bundesgesetzes betreffend die elektrischen Schwach- und Starkstromanlagen (Elektrizitätsgesetz, EleG) datiert vom 01.06.2020. Beschlossen wurde es am 24.06.1902 und ist am 01.02.1903 inkraftgetreten. Siehe auch https://www.admin.ch/opc/de/classified-compilation/19020010/index.html