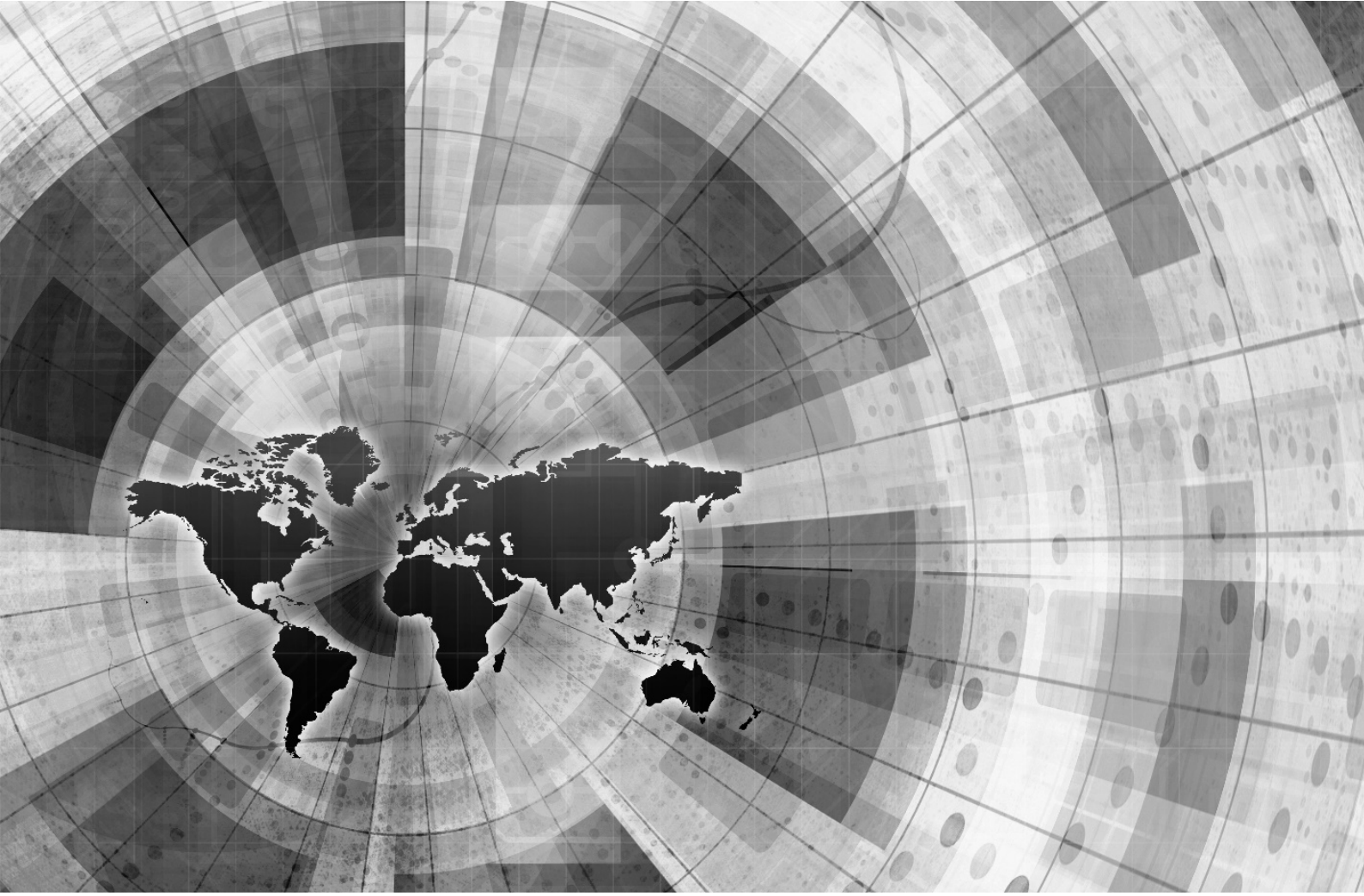


Supply Chain Security

Analyse & Massnahmen zur Sicherung der digitalen Lieferkette

Arbeitsgruppe Supply Chain Security der
Kommission Cybersecurity von ICTswitzerland

September 2019

ICTSWITZERLAND

Impressum

ICTswitzerland
Aarbergergasse 30
CH - 3011 Bern

Autoren:
Dr. Stefan Frei, Christof Jungo[1], Daniel Busch[2], Dr. Raphael Reischuk

Anmerkung:
Der Bericht gibt primär die Auffassung der Begleitgruppe wieder. Jedoch spiegelt der Bericht nicht zwangsläufig die Positionen der Organisationen der Mitglieder wider.

Begleitung:
Arbeitsgruppe Supply Chain Security der Kommission Cybersecurity von ICTswitzerland

Dr. Stefan Frei	Cyber Security Principal, Accenture Head der Arbeitsgruppe Supply Chain Security von ICTswitzerland
Umberto Annino	Head Security Governance, SIX Group
Markus Bischof	Director Europe Security & Trust Organization, Cisco Systems GmbH
Tobias Ellenberger	Vorstandsmitglied, Swiss Cyber Expert Chief Operating Officer, Oneconsult AG
Dr. Jon Albert Fanzun	Sondergesandter für Cyber-Aussen- & -Sicherheitspolitik, EDA
Christophe Gerber	Head of Defense & CyberSecurity, ELCA Informatique SA
Christian Grasser	Geschäftsführer, asut
Thomas Holderegger	Head of Security IT, UBS AG
Andreas Kaelin	Geschäftsführer, ICTswitzerland
Uwe Kissmann	Managing Director Cyber Security Services EALA, Accenture Präsident, Kommission Cybersecurity von ICTswitzerland
Arié Malz	Referent IKT und Digitalisierung, Stab Generalsekretariat Finanzdepartement
Dr. Raphael Reischuk	Head of Cyber Security Services, Zühlke Engineering AG Vize-Präsident, Kommission Cybersecurity von ICTswitzerland
Gérald Vernez	Delegierter Cyberdefence, VBS
Nicole Wettstein	Leitern Schwerpunktprogramm Cybersecurity, SATW

[1] SecIntel GmbH
[2] Symantec (Deutschland) GmbH

Executive Summary

Das Internet verbindet zunehmend Menschen und Maschinen und hat unser Leben bereits heute nachhaltig verändert. Während die Integrität und Sicherheit von Produkten aus traditionellen Branchen vor der Marktzulassung auf gewisse Fragestellungen hin überprüft werden (z.B. im Bereich Mobilität, Lebensmittel, Medikamente, etc.), werden Qualität und Sicherheit vieler digitaler Produkte oft nicht hinreichend überprüft. Die Gründe dafür sind vielfältig. So ist beispielsweise die heutige Sicherheit der Lieferkette (Supply Chain) digitaler Produkte oft unzulänglich und untergräbt bestehende Sicherheitsvorkehrungen. Auch ist es Entscheidungsträgern mangels fundierter und transparenter Informationen oft nicht möglich, nachhaltige Entscheidungen zu treffen.

Durch die fortschreitende Digitalisierung kann die Unkenntnis über das Sicherheitsniveau der eingesetzten Produkte zu kritischen Bedrohungen führen. Kommen nicht vollständig geprüfte Produkte in kritischen Infrastrukturen zum Einsatz, so sind Bedrohungen unter Umständen flächendeckend und gefährden die Versorgung der Gesellschaft in den Bereichen Elektrizität, Medizin, Mobilität und physischer Schutz. Die einhergehenden Risiken sind oft abstrakt und entwickeln sich schleichend, in der Folge wurden sie lange Zeit kaum wahrgenommen und haben sich bis heute fortwährend kumuliert.

Die Arbeitsgruppe Supply Chain Security analysiert den Umgang mit Technologierisiken in anderen Industrien (Bsp. Strom), darauf aufbauend identifiziert und dokumentiert sie notwendige Massnahmen für eine sichere Digitalisierung. Unter anderem werden folgende Fragestellungen bearbeitet:

- Was sind die grössten Risiken der digitalen Gesellschaft und wo liegen sie?
- Wie sehen kritische Angriffsszenarien aus, wer sind die Angreifer?
- Was können und müssen wir – als Gesellschaft oder Industrie – heute bereits beachten oder einleiten?
- Welche Massnahmen zur Sicherung der digitalen Lieferkette sind notwendig und hilfreich?

Die Gesellschaft ist heute gefordert, bekannte und vermeidbare Fehler zu verhindern, damit die Chancen der Digitalisierung deren Risiken überwiegen.

Inhalt

Ausgangslage: Die Digitale Gesellschaft

Entwicklung & Cyberrisiken

Die vernetzte Gesellschaft wird mit der steigenden Anzahl von neuartigen Interaktionen zwischen Menschen, Maschinen, Diensten und diversen Rückkopplungsprozessen stetig und schnell komplexer. Insbesondere durch Abhängigkeiten von Hard- und Software, sowie beim Einkauf von Leistungen (direkt oder delegiert) entstehen neue Risiken für kritische Infrastrukturen[3]. Sicherheitsvorfälle können durch Fehlfunktionen oder Manipulation von Hard- oder Softwarekomponenten, durch Zufälle aufgrund ungenügender Design- und Entwicklungsqualität der Komponenten, oder durch gezielte Angriffe ausgelöst werden.

Finden digitale Produkte mit Sicherheitsdefekten den Weg in den Markt, können sich diese Schwachstellen über Jahrzehnte auswirken. Davon betroffen sind beispielsweise fest verbaute Geräte in Haus- oder Industriesteuerungen und auch kritische Infrastrukturen sind davon nicht ausgenommen.

Die Eigenschaften eines komplexen, vernetzten Systems, lassen sich nicht mehr aus der isolierten Analyse des Verhaltens einzelner Komponenten ableiten. Es entstehen neue, mitunter überraschende Systemeigenschaften, wie Selbstorganisation oder Emergenz[4]. Eine kleine lokale Störung — ausgelöst durch einen Zufall oder eine Fehlfunktion — kann unvorhersehbare und räumlich entfernte Auswirkungen zur Folge haben.

Beispiele:

- Massenbeeinflussung von ganzen Gesellschaften durch Social Media[5].
- Fitness Tracker Apps führen zur Identifikation geheimer Militärbasen[6].

Cyberkriminelle & Staatliche Akteure

Die Digitalisierung wird von Angreifern aller Art aktiv verfolgt und ausgenutzt. In jüngster Vergangenheit verzeichnen sich vermehrt Angriffe zur Durchsetzung einer politischen Agenda unter Ausnutzung von Verwundbarkeiten der digitalen Gesellschaft. Aus der Geschichte ist bekannt, dass sich Geheimdienste sowie Kriminelle jeweils sehr schnell neue Technologien aneignen. Seit jeher betätigen sich Staaten und Geheimdienste in der

[3] «Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.» (Bsp. Strom- & Wasserversorgung)
Definition des BABS: https://www.babs.admin.ch/de/aufgabenbabs/ski.html
[4] Komplex Adaptives System
https://de.wikipedia.org/wiki/Komplexes_adaptives_System
[5] Wie die Sozialen Netzwerke die Gesellschaft durchdringen
https://www.nzz.ch/feuilleton/medien/wie-die-sozialen-netzwerke-die-gesellschaft-praegen-ld.1380183
[6] Fitness tracking app Strava gives away location of secret US army bases
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Spionage und Sabotage und in militärische Verteidigungs- und Angriffsstrategien werden diese Taktiken zunehmend eingeplant[7].

Abbildung 1: Bedrohungen im komplexen System der digitalen Gesellschaft – ausgelöst durch Zufälle oder gezielte Angriffe von Akteuren.

Zur Beurteilung kritischer Verwundbarkeiten muss die Digitalisierung der Gesellschaft aus der Sicht eines Angreifers betrachtet werden. Folgende Fragen helfen dabei, die richtige Perspektive einzunehmen:

- Wie kann ein versierter Angreifer den maximalen Einfluss und die grösste Persistenz gewinnen, bei gleichzeitig kleinster Detektionswahrscheinlichkeit?
- Wie geht ein Angreifer vor, wenn sein Primärziel sehr gut gesichert ist?

Die Kriminal- und Militärgeschichte zeigt, dass erfolgreiche Angreifer oft den schwächsten Punkt identifizierten. Der Angriff erfolgt dort, wo die Verteidiger ihn am wenigsten erwarten. Die Kompromittierung digitaler Produkte vor deren Auslieferung, also während des Designs, der Herstellung oder in der Lieferkette, erfüllt genau dieses Angriffskriterium.

Etliche Staaten bauen derzeit ihre offensiven und defensiven Cyberfähigkeiten aus. Im Unterschied zu Cyberkriminellen und anderen Angreifern können Staaten . . .

- . . . sich direkten Zugriff auf kritische Teile der Infrastruktur des Internets verschaffen («Internet Backbone»).
- . . . Dienstanbieter oder Hersteller per Gesetz zur Überwachung oder Mitarbeit zwingen.
- . . . systematisch und umfangreich den Internetverkehr überwachen.

[7] Luiijf, E., Besseling, K. and de Graaf, P. (2013) 'Nineteen national cyber security strategies', Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, pp.3–31.

Staatliche Angreifer verfügen über überdurchschnittliche Ressourcen und den langen Atem, um ein Ziel persistent über mehrere Angriffskanäle und lange Zeiträume unentdeckt zu erreichen. Persistenz und Zugriffsmöglichkeit im Bedarfsfall sind die obersten Ziele. Die Tätigkeiten der Angreifer beinhalten das versteckte Einbringen von Malware und Backdoors in Hardware und Software der Zielsysteme anderer Länder (oder Konkurrenten).

Cybersecurity sollte sich nicht auf Software und Netzwerksicherheit beschränken, sondern die Integrität und Sicherheit der Hardware und ihrer Bestandteile ebenso wie den Faktor Mensch miteinbeziehen. Schlussendlich werden die meisten Komponenten von Menschen installiert, konfiguriert und bedient.

Beispiele:

- Israeli und Amerikaner sollen den Computerwurm Stuxnet, der grosse Teile der iranischen Atomanlagen lahmgelegt hat, gemeinsam entwickelt haben[8].
- Nach Kompromittierung vom System des Computerherstellers ASUS, verteilt sich eine Malware über die automatische Update-Funktion auf Systeme von ASUS Kunden [9].
- Liste von Signifikanten Cyberangriffen auf Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen[10].

Digitaler Blindflug

Angriffe in der Lieferkette können grundsätzlich weder ausgeschlossen noch vollständig verhindert werden. Ein effektiver Schutz gegen solche Bedrohungen der Digitalisierung ist heute noch so gut wie inexistent. Die Eintrittsbarriere für jede Art von Angriff ist unnötig tief, solange folgende Punkte weiterhin gelten:

- Die Kompromittierung eines Produktes lässt sich nicht detektieren.
- Minimale Qualitätsmerkmale vom Hersteller (und dessen Zulieferanten) lassen sich nicht einfordern.
- Der Unterhalt der Infrastruktur ist nicht sichergestellt, da Sicherheits-Updates nicht zuverlässig eingespielt werden.

Diese Situation ist in Anbetracht der steigenden Abhängigkeit von digitalen Produkten nicht länger hinnehmbar. Aufgrund ungenügender Detektionsmöglichkeiten muss davon

[8] Israel und die USA sollen hinter Computer-Angriff stecken https://www.nzz.ch/iran_israel_usa_stuxnet-1.9110811
[9] Hunderttausende Asus-Computer mit Virus infiziert https://www.tagesanzeiger.ch/digital/computer/hunderttausende-von-asuscomputern-mit-virus-infiziert/story/19690172
[10] Significant Cyber Incidents Since 2006 https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

ausgegangen werden, dass bereits heute Teile der kritischen Infrastruktur der Schweiz kompromittiert sind.

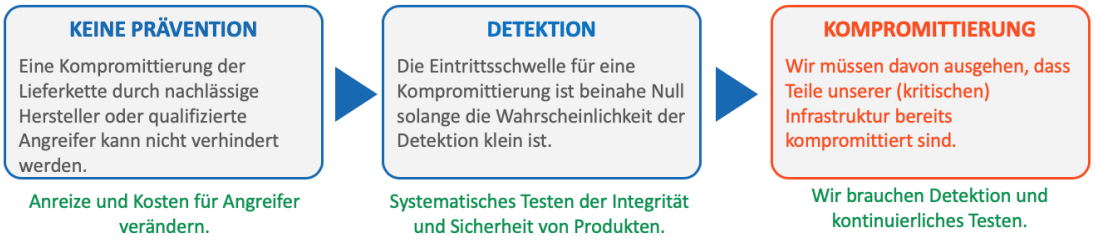


Abbildung 2: Wird die Qualität und Sicherheit von digitalen Produkten weder eingefordert noch überprüft, müssen wir von einer grossen Zahl an kompromittierten Produkten, auch in kritischen Funktionen, ausgehen.

Folgende Beispiele aus dem Bereich der Lieferkette zeigen die Folge der Kompromittierung aufgrund ungenügender Detektion:

- **IBM Schreibmaschinen | Sowjetunion 1970**
  Die Sowjetunion kompromittiert IBM Schreibmaschinen vor der Lieferung an die US Botschaft in Moskau. Während ca. 8 Jahren konnten die Sowjets die maschinengeschriebenen Texte der US Botschaft mitlesen[11].

- **Bezahlterminal (POS) | Cyberkriminelle 2008**
  Kompromittierte Bezahlterminals in Europa exfiltrieren Kreditkarteninformationen und Passwörter per GSM Implantat direkt an Cyberkriminelle im Ausland[12].

- **Werkzeugkasten der NSA | USA 2013**
  Schadsoftware- und Hardware-Implantate für Rechner von Cisco, Dell, Juniper, Hewlett-Packard (HP) und Huawei werden durch den U.S. Geheimdienst NSA installiert[13].

- **BlackIOT, High Wattage Botnet | 2018**
  Ein Botnetz mit kompromittierten IoT Klimageräten und Heizungen kann die Stromversorgung einer Region bedrohen[14].

[11] Operation GUNMAN https://www.cryptomuseum.com/covert/bugs/selectric/
[12] Chip and pin scam 'has netted millions from British shoppers'
https://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html
[13] Der geheime Werkzeugkasten der NSA
https://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html
[14] BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid
https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

Auch wenn absolute Sicherheit nicht existiert (weder in der digitalen noch in der realen Welt), sind geeignete Massnahmen zu ergreifen, welche . . .

- . . . die Eintrittsbarriere, Komplexität und die Kosten für Angreifer erhöhen.
- . . . die Erfolgsaussicht von Angriffen reduzieren.
- . . . die Detektion von Angriffen und die Identifikation der Angreifenden ermöglichen.
- . . . die Hersteller und Betreiber der Produkte bzgl. Qualität und Sicherheit in die Pflicht nehmen.

In anderen Worten heisst dies einerseits, ein Angreifer darf nicht länger in der Lage sein ohne erhebliches Eigenrisiko die Sicherheit der Digitalisierung zu gefährden. Andererseits müssen Hersteller die Verantwortung für die Sicherheit ihrer digitalen Produkte übernehmen.

Die Lieferkette digitaler Produkte (Supply Chain)

Wie oben erwähnt, ist die Sicherung der Lieferkette von besonderer Wichtigkeit und wird daher im Folgenden genau betrachtet.

Abbildung 3: Lieferkette von digitalen Produkten und Komponenten vom Design der Hardware über Integration und Versand bis zum Einsatz beim Endabnehmer.

Herkunft und Hersteller

Die meisten digitalen Infrastrukturen stammen von einer Vielzahl von Lieferanten unterschiedlicher Herkunft. Komponenten sowie Subkomponenten werden üblicherweise in einer komplexen Lieferkette gefertigt, welche aufgrund eben dieser Komplexität kaum verständlich und nicht kontrollierbar ist. Mit der steigenden Verbreitung digitaler Produkte stellt die wachsende Komplexität der Lieferkette eine erhebliche Bedrohung für die digitale Gesellschaft dar.

Traditionelle vs. digitale Lieferkette

Der traditionelle Ansatz zur Sicherung der Lieferkette basiert auf der Annahme, dass die grösste Bedrohung in der Herstellung liegt. Dieser Ansatz muss für digitale Produkte erweitert 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 mit ein.

- Traditionelle nicht-vernetzte Produkte ändern sich nach Auslieferung kaum. Integrierte Fehlfunktionen in vernetzten Produkten hingegen, können auch nach der Auslieferung aktiviert werden. Eine Fehlfunktion oder Backdoor kann ebenso durch ein Update ausgelöst werden.

- Im Unterschied zu nicht-vernetzten Produkten werden Security Updates vom Hersteller benötigt. Dies gilt nicht zuletzt während der gesamten Lebensdauer des digitalen Produkts.

- Traditionelle Produkte sind meistens per visueller Inspektion überprüfbar. Die Integrität digitaler Produkte kann oft nur durch aufwendige Testverfahren beurteilt werden.

- Traditionelle Produkte lassen sich aufgrund der fehlenden Vernetzbarkeit kaum individuell manipulieren. Alle Produkte einer Serie sind gleich. Vernetzte Produkte hingegen lassen sich individuell aus der Ferne manipulieren. Testverfahren sind entsprechend aufwendiger.

- Einige wenige Hersteller dominieren den Markt bestimmter digitaler Produktarten oder Subkomponenten (z.B. Prozessoren, WLAN Chips, Adapter, etc.). Die Folge ist eine Konzentration von Anreizen für Angreifer. Ein Angriff auf dominierende Hersteller hat weitreichende Konsequenzen.

Integrität der Lieferkette

Bei einem Angriff über die Lieferkette werden Komponenten bereits vor der Lieferung an den Endabnehmer kompromittiert oder manipuliert. Dies kann bereits im Design und bei der Entwicklung von Chips, bei der Herstellung oder Integration von Komponenten oder während dem Transport zum Endabnehmer geschehen. Die Manipulation während des Betriebs, z.B. durch Lieferung einer kompromittierten Firmware, muss ebenfalls berücksichtigt werden. Die Integrität digitaler Lieferobjekte ist insbesondere durch nicht dokumentierte Zugänge und Backdoors oder implantierte Fehlfunktionen gefährdet.

Wir unterscheiden in erster Näherung folgende Arten von Bedrohungen:

(A) Gezielter Angriff	(B) Opportunistischer Angriff
Ein einzelnes kompromittiertes Produkt hat kritische Auswirkungen auf die Zielorganisation. Die gezielte Kompromittierung ausgewählter Produkte einer Organisation oder Industrie erlaubt Zugriff und Einflussnahme in einem genau spezifizierten Umfeld.	**Erst eine grosse Verbreitung der kompromittierten Produkte wird kritisch.** Die Kompromittierung von allgemein zugänglichen digitalen Gebrauchsgütern für Private und/oder die Industrie ermöglicht die Einflussnahme über eine grosse Population des Produkts.
	
• Spezielle Netzausrüstung (ISP, GSM, etc.) • Industriekontrollsysteme (ICS) • Industrial Internet of Things (IIoT) • Industriespezifische Produkte (Militär, Energie, Medizin)	• Computer / Computerperipherie • Smart Meter, Toaster, TV, Waschmaschine • Home Control Systems • IoT, Sensoren • zB. Mirai Botnet DDoS Attacke

Die Grenzen zwischen diesen Bedrohungsarten sind fliessend.

Sabotage & Spionage

Geheimdienste treffen vermehrt Massnahmen wie z.B. sogenannte Kill Switches (Notausschalter), um eine Sabotage von fremden Systemen für den Bedarfsfall 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. Somit ist eine klare Beweislage für die Sabotage beinahe unmöglich.

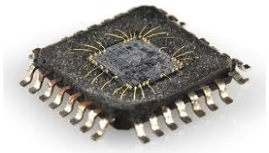
Kompromittierte Hardware

Auch Hardware kann mit versteckten Funktionen versehen und ausgeliefert werden, welche bei Bedarf aus der Ferne aktiviert werden. Digitale Produkte ohne Eingabegeräte (Maus,

Bildschirm, etc.) wirken oft nicht wie vernetzte Computer (bspw. IoT Geräte wie Smart Toaster). Dabei sind genau diese digitalen Produkte oft mit unzureichend gesicherter Hard- und Software in einem meist ungeschützten Netzwerk im Einsatz. Angriffe auf die Firmware wie auch auf die Hardware digitaler Produkte sind möglich und für Angreifer sehr attraktiv.

Weltweit werden pro Jahr in unzähligen Firmen mit hunderttausenden von Ingenieuren über 5'000 neue Chips entwickelt. Statistisch betrachtet gibt es folglich genügend Mitarbeiter mit den Fähigkeiten und dem notwendigen Zugang, um Chips bereits auf Stufe Design zu kompromittieren. Dies kann aus eigenem Antrieb oder durch Erpressung eines Mitarbeiters erfolgen[15].

Kompromittierte Hardware erlaubt u.a.:



- Exfiltration sensitiver Daten, z.B. über «Covert Channels» (verdeckte Kanäle)
- Fernzugriff und Kontrolle von Systemen
- Funktionsmanipulation, z.B. die Erzeugung inkorrekter Resultate
- Einspielen kompromittierter Software und erzwungene Verwendung unsicherer Algorithmen
- Physische Zerstörung auf Befehl (Kill Switch)

Die Abwehr und Beseitigung von unsicherer Hardware kann sehr aufwändig und teuer werden, ein Software Update genügt in vielen Fällen nicht (z.B. Ersatz aller Smartmeter in einer Stadt oder gar Region).

Ohne zuverlässige Qualitätsprüfung von digitalen Produkten müssen wir davon ausgehen, dass kompromittierte Komponenten bereits heute im Einsatz sind. Weitere kompromittierte Komponenten werden fortlaufend dazukommen, mitunter in kritischen Funktionen.

General Michael Hayden, ehem. Leiter der CIA und NSA hat diese Problematik wie folgt ausgedrückt: *«Frankly, it's not a problem that can be solved, this is a condition that you have to manage.»* [15]

[15] Compromised By Design?
https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf

Technologie & Innovationsgeschichte

Gibt es Lehren aus der Geschichte, welche uns helfen, die Entwicklung der Cybersicherheit der digitalen Gesellschaft besser zu verstehen oder gar voranzutreiben?

Die Einführung disruptiver Innovation

Bei der Einführung einer Innovation (z.B. Automobil, Aviatik) ist die Sicherheit sekundär, Erfahrungen und Sicherheitsnormen fehlen noch. Mit steigender Verbreitung mehren sich die Vorfälle und die Gesellschaft beginnt die fehlende Sicherheit zu hinterfragen. Forderungen nach verbindlichen Sicherheitsnormen werden von den betroffenen Industrien oft heftig und mit den folgenden Argumenten bekämpft:

- Das Produkt gilt als sicher, Unfälle werden dem Benutzer zugeschrieben.
- Sicherheitsnormen gelten als nicht notwendig, sie würden die Industrie wirtschaftlich ruinieren.
- Sicherheitsnormen würden Innovation verunmöglichen.

Ralph Naders Buch «Unsafe at any Speed» von 1965 veranschaulicht diesen Konflikt. Die Publikation des Buches führte — nach Auseinandersetzungen mit der Automobilindustrie — zur Einführung von Sicherheitsgurten, Crashtests sowie zum Rückruf von ganzen Produktserien[16]. Die Flugzeugindustrie bekämpfte in den Anfangszeiten die Tests von Flugmotoren. Als diese doch eingeführt wurden, bestanden über die Hälfte der Motoren die ersten Tests nicht[17].

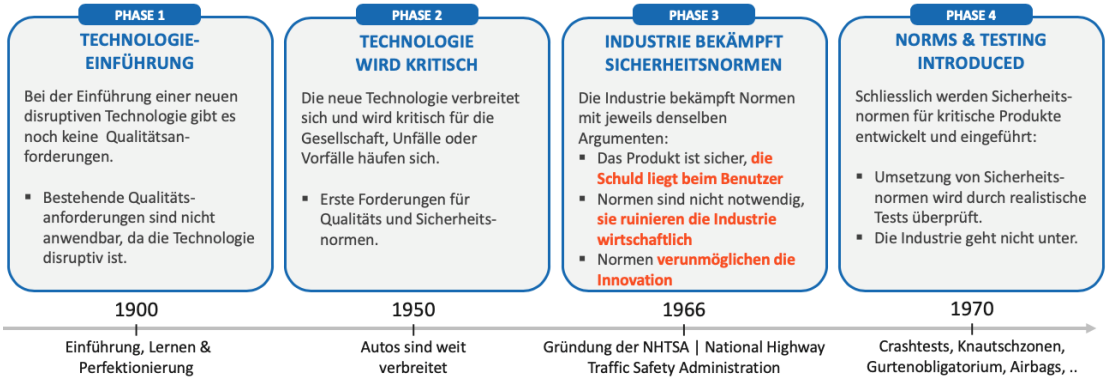


Abbildung 4: Die Einführung von Qualitätsnormen wurden von der Automobil- und Luftfahrtindustrie zuerst bekämpft. Heute ist ein Fehlen solcher Normen und Tests nicht mehr vorstellbar.

[16] Unsafe at Any Speed: The Designed-In Dangers of The American Automobile
https://en.wikipedia.org/wiki/Unsafe_at_Any_Speed
[17] A History of Aviation Safety: Featuring the U.S. Airline System
https://www.amazon.com/History-Aviation-Safety-Featuring-Airline/dp/144900797X

Heute sind fehlende Sicherheitsnormen und Tests in diesen Industrien unvorstellbar. Sowohl die Automobil- als auch die Aviatikindustrie bestehen noch und gelten als massgebliche Innovatoren.

In allen kritischen Industriesektoren sind Qualitätsprüfungen durch unabhängige Stellen Teil der Produktezulassung, wie z.B. in der Automobilindustrie, Luftfahrt, Medizinaltechnik, Energie, Nahrungsmittelindustrie, etc. Einzig der ICT-Sektor verfügt kaum über verbindliche Normen, welche die Sicherheit oder die Integrität der Produkte gewährleisten. Es gibt keine Produktehaftung für Software; Sicherheitsupdates sind als Rückrufaktionen fehlerhafter Software zulasten des Kunden zu betrachten.

Lehren für die digitale Gesellschaft

Wie oben erwähnt, hat die Gesellschaft bei kritischen Technologien oder hohem Schadenspotenzial (z.B. in der Lebensmittelindustrie, Pharmazie, Transportindustrie, Energieindustrie, Bauwesen etc.), jeweils Normen zur Sicherstellung von Qualität und Sicherheit eingeführt. Diese werden durch realistische Tests gestützt und überprüft. Das Fehlen von Normen und Tests für digitale Produkte ist angesichts der wachsenden Bedeutung dieser Produkte als kritisch zu beurteilen.

Die Technologiegeschichte legt den Schluss nahe, dass die Gesellschaft, auch für digitale Produkte, verbindliche Qualitätsnormen entwickeln und einführen wird. Dazu gehören Überprüfungen durch realistische Test- und Analyseverfahren. Gemäss Erfahrungen, wird die Einführung von verbindlichen Qualitätsnormen nicht zum Untergang der betroffenen Industrie führen. Es ist unumgänglich, dass Gesellschaft, Industrie und Politik gemeinsam die folgenden Fragen diskutieren und die entsprechenden Themen entwickeln:

- Was sind Minimalanforderungen an die Integrität und Sicherheit von digitalen Produkten und Diensten?
- Welche Minimalanforderungen gelten für welche Art von digitalen Produkten, Diensten, Anwendungsbereichen oder Industriesektoren?
- Wie überprüfen wir die Einhaltung der Minimalanforderungen, nicht nur bei der Zulassung, sondern auch während dem gesamten Lebenszyklus?

Diese verbindlichen Qualitätsnormen entsprechen in der Automobilindustrie den uns vertrauten aktiven und passiven Sicherheitsvorkehrungen wie Sicherheitsglas, Mehrkreisbremsanlagen, Airbags, Crashtests, periodischen Motorfahrzeugkontrollen, etc.

Ausblick und Massnahmen

Zur Sicherung der Lieferkette sind Massnahmen auf unterschiedlichen Ebenen einzuführen.

Verantwortlichkeit Hersteller und Lieferant

Hersteller und Lieferanten müssen für Sicherheit und Qualität der digitalen Produkte oder Dienste sowie deren Herstellung zur Verantwortung gezogen werden. Es müssen sektorspezifische Vertragsvorlagen (Security Appendix) entwickelt werden, welche die relevanten Sicherheitskriterien dokumentieren. Somit erhalten Sicherheitsanliegen mehr Gewicht als individuelle Absprachen zwischen Kunde und Hersteller.

Wichtige Minimalforderungen in einem Security Appendix sind unter anderem:

- Der Hersteller verpflichtet sich zu Coordinated Disclosure (ISO 29147) zur Handhabung von gemeldeten Schwachstellen. Er dokumentiert die Umsetzung des Prozesses, die Ansprechpartner und Bearbeitungsdauer[18].

- Der Hersteller verpflichtet sich zur vollständigen und abschliessenden Dokumentation aller im Produkt eingebauten «Default Accounts», Passwörter, Zertifikate und Keys/Schlüssel.

- Der Hersteller räumt dem Kunden das Recht ein, die Hard- und Software des Produktes auf Integrität und Sicherheit zu prüfen (Reverse Engineering) ohne die Verletzung der Intellectual Property Rights (IPR).

Bei allfälligen späteren Entdeckungen (z.B. Schwachstellen oder Backdoors) kann der Hersteller nun 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.

Produkteanforderungen

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 kaum möglich oder zu teuer (z.B. nach Konkurs des Herstellers).

[18] ISO/IEC 29147:2014 Vulnerability Disclosure https://www.iso.org/standard/45170.html

Vor dem Einsatz von kritischen Produkten muss mindestens eine der folgenden Vorkehrungen gegeben sein:

- Der Quellcode ist frei verfügbar (Open Source).
- Vor der Anschaffung wird der Quellcode der aktuellsten Version bei einer unabhängigen Stelle deponiert, bei Konkurs des Herstellers geht der Quellcode zum Kunden über.

Auf jeden Fall müssen relevante netzwerkfähige Produkte über einen robusten und sicheren Mechanismus verfügen, um Sicherheits-Updates zeitnah und skalierbar einzuspielen. Damit wird die Möglichkeit zum Schutz kritischer Produkte während der gesamten Lebensdauer sichergestellt, auch nach Ausscheiden des Herstellers.

Unabhängiges Cybertesting Lab

Die vernetzte Gesellschaft muss in der Lage sein, durch unabhängige und glaubwürdige Tests die Integrität und Sicherheit von digitalen Produkten zu analysieren und zu beurteilen.

Solche Tests beinhalten mindestens die folgenden Punkte:

- Review von Source Code (sofern verfügbar), Konfiguration und Einstellungen.
- Analyse von Software und Hardware durch Reverse Engineering, falls notwendig.
- Risikobeurteilung der Resultate, Koordination der Kommunikation mit Auftraggeber und Hersteller (Coordinated Disclosure).
- Publikation der Resultate.

Der Aufbau der entsprechenden Fähigkeiten benötigt Zeit und bedingt ein Testing Lab mit entsprechender High-Tech Ausrüstung sowie ausgebildete Spezialisten und enge Kontakte zu Industrie, Akademie und der Security Community. Ein internationaler Austausch ist langfristig notwendig.

Vision Digitale Schweiz

Die Fähigkeit zur unabhängigen und effektiven Prüfung von digitalen Produkten — inklusive Reverse Engineering von Chips und Firmware — wird in naher Zukunft an Wichtigkeit zunehmen. Durch die steigende 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. Es ist voraussehbar, dass sich Cyber Testing bald als zentrale, nationale Aufgabe entwickeln wird.

Die Fähigkeit, effektive Software- und Hardware-Tests durchzuführen, ist als eine Kernkompetenz der digitalen Gesellschaft zu betrachten.

Um in Zukunft in dieser Kernkompetenz nicht ausschliesslich von externen Partnern abhängig zu sein, sollte die Schweiz ähnlich dem Modell des Chemielabors Spiez[19] zügig ein Cybertesting Lab in Partnerschaft mit Industrie, Akademie und Behörden aufbauen. Das Cybertesting Lab dient der Durchführung und Koordination von Tests im Auftrag der Industrie, des Landes oder internationaler Organisationen.

Als neutrale Nation mit einer stabilen Rechtsprechung und einer langen Tradition als Standort von internationalen Diensten, ist die Schweiz als Kompetenzzentrum und Betreiber eines unabhängigen Cybertesting Labs prädestiniert.

[19] Labor Spiez https://www.labor-spiez.ch/de/lab/ubu/index.htm

Konklusion

Die digitale Gesellschaft läuft derzeit Gefahr, durch den vorschnellen Einsatz und die teils unkontrollierte Beschaffung und Verbreitung digitaler Produkte, Sicherheitsprobleme zu schaffen, welche sich erst langfristig manifestieren und nur mit grösstem Aufwand zu korrigieren sind.

- Das Fehlen von Qualitäts- und Sicherheitsnormen und den entsprechenden Tests für digitale Produkte ist angesichts der steigenden Bedeutung als kritisch zu beurteilen.
- Ohne glaubwürdige Qualitätsprüfung von digitalen Produkten muss davon ausgegangen werden, dass kompromittierte Komponenten bereits heute im Einsatz sind. Durch glaubwürdige und unabhängige Tests ist die Sicherheit digitaler Produkte zu überprüfen.
- Um im Cybertesting nicht ausschliesslich von externen Partnern abhängig zu sein, sollte die Schweiz ähnlich dem Modell des Chemielabors Spiez zügig ein Cybertesting Lab in Partnerschaft mit Industrie, Akademie und Behörden aufbauen.
- Verbindliche Minimalanforderungen für die Sicherheit von digitalen Produkten müssen gemeinsam mit den Partnern (Industrie, Akademie, Behörden) erarbeitet werden.
- Cybersecurity darf sich dabei nicht auf Software, Netzwerksicherheit und den Faktor Mensch beschränken, die Integrität und Sicherheit der Hardware ist miteinzubeziehen.

Die Fähigkeit, effektive Software- und Hardware Tests durchzuführen, ist als eine Kernkompetenz der digitalen Gesellschaft zu betrachten. Die digitale Gesellschaft ist gefordert, das Thema Supply Chain Security zu adressieren und entsprechende Voraussetzungen zu schaffen (Ressourcen, Rechtsrahmen, Ausbildung, etc.) um bekannte und vermeidbare Fehler zu verhindern. Nur so werden die Chancen der Digitalisierung auch in Zukunft deren Risiken überwiegen.