Risiken und Massnahmen zur Sicherung der digitalen Lieferkette

Ohne effektive Qualitätsprüfung von digitalen Produkten muss davon ausgegangen werden, dass kompromittierte Komponenten und Cyber-Produkte bereits heute in Industrie und Behörden im Einsatz sind. Bis dato fehlen griffige Massnahmen und unabhängige Tests wie beispielsweise in der Automobil- oder Aviatik-Industrie, welche die Integrität von Cyber-Produkten hinreichend sicherstellen. Was kann trotzdem zur Sicherung der digitalen Lieferkette unternommen werden?

Christof Jungo und Stefan Frei

© depositphotos DragonImages

Digitale Produkte können bereits vor ihrer Auslieferung kompromittiert sein.

Das Internet verbindet zunehmend Menschen und Maschinen und hat das Leben bereits nachhaltig verändert. Die Integrität und Sicherheit von Produkten aus traditionellen Branchen wird vor der Marktzulassung verbindlich und systematisch geprüft (z.B. im Bereich Transport, Energie, Lebensmittel, Medikamente usw.). Im Gegensatz dazu bestehen bei digitalen Produkten kaum einheitliche Anforderungen zu Sicherheit, Prüfprozessen und -methoden. In der Folge wird deren Sicherheit weder systematisch noch verbindlich überprüft. Die heutige Sicherheit der Lieferkette (Supply Chain) digitaler Produkte ist oft unzulänglich. Mangels transparenter oder belastbarer Informationen zur Sicherheit ist es nicht möglich, nachhaltige Entscheidungen zu treffen.

Kommen ungeprüfte digitale Produkte zum Einsatz, so können die Konsequenzen aus Cyber-Vorfällen sowohl Unternehmen als auch die Gesellschaft bedrohen. Dieser Artikel analysiert die Sicherheit der digitalen Lieferkette (Supply Chain) und identifiziert notwendige Massnahmen.

Neue Herausforderungen

Trotz stetig wachsender Abhängigkeit und Verbreitung von digitalen Produkten (Hard- wie auch Software) hat ein Käufer heute kaum die Möglichkeit, deren Sicherheit zu beurteilen. Mit der zunehmenden Digitalisierung in Industrie und Gesellschaft steigen die Gefahren, die von verwundbaren oder bereits bei Auslieferung kompromittierten, digitalen Produkten ausgehen. Qualitätsprüfungen oder Anforderungen, wie sie in anderen Industrien längst etabliert sind (Automobil, Aviatik, Lebensmittel, Energie), fehlen in der Cyberwelt weitgehend. Verbindliche Normen sind grösstenteils inexistent. Im Gegensatz zu den traditionellen Risiken sind Cyberrisiken abstrakt und werden dadurch nicht oder erst zu spät (z.B. Vorfall Ruag) wahrgenommen und angegangen. Erst langsam beginnt man zu verstehen, welche Gefahren von umfassend vernetzten Produkten, mitunter in kritischen Funktionen, ausgehen. Sicherheitsmerkmale und Anforderungen, die man in anderen Industrien (z.B.

Automobil) als gegeben voraussetzt, muss die digitale Gesellschaft erst erarbeiten und durchsetzen. Industrie und Behörden sind sich noch uneinig über das Erarbeiten griffiger Grundlagen und Normen zur Sicherung der digitalen Lieferkette (Supply Chain).

Die Industrie scheut die Kosten und befürchtet Wettbewerbsnachteile, welche durch die Umsetzung von Massnahmen zur Sicherung der digitalen Lieferkette entstehen. Die Behörden warten auf Impulse aus der Industrie.

Viele KMU stehen in der Mitte der Wertschöpfungskette. Sie sind gleichzeitig Hersteller oder Integrator und Konsument von digitalen Produkten. Sie sind kaum in der Lage, aus unsicheren digitalen Halbfabrikaten einer komplexen Lieferkette die Sicherheit ihrer Endprodukte zu verstehen oder zu gewährleisten.

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.

Ohne zuverlässige Qualitätsprüfung von digitalen Produkten muss man davon ausgehen, dass kompromittierte Komponenten bereits heute im Einsatz sind. Weitere solche Komponenten werden fortlaufend hinzukommen, mitunter auch in kritischen Funktionen.[1]

Sicherung der Lieferkette für digitale Produkte

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:

- Steigende Komplexität und Anzahl Akteure unterschiedlicher Herkunft (Gesinnung, Kultur, politisches Umfeld)
- Mit der steigenden Komplexität von digitalen Produkten verlagert sich die Bedrohung in Richtung des Designs von Software, Chips und Komponenten.[2]
- Traditionelle nicht vernetzte Produkte ändern sich nach Auslieferung kaum. Integrierte Fehlfunktionen in vernetzten Produkten hingegen können auch nach der Auslieferung aktiviert werden.

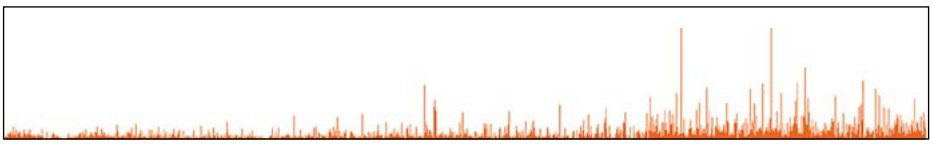

Abbildung 2 zeigt die Anzahl publizierter Schwachstellen pro Woche in den letzten 20 Jahren. (Quelle: NVD National Vulnerability Database)

- Eine visuelle Inspektion genügt nicht zur Beurteilung der Sicherheit digitaler Produkte (abstrakte Risiken). Effektive Testverfahren sind notwendig.
- Software hat Schwachstellen, welche kontinuierlich durch Sicherheitsupdates behoben werden müssen, auch nach Auslieferung.

Einige wenige Hersteller dominieren den Markt bestimmter digitaler Produktarten, Subkomponenten oder Services (z.B. Prozessoren, Cloud). Vorzeitiges Beenden benötigter Dienste und Updates degradiert die Sicherheit dieser Produkte vor ihrem eigentlichen Ende des Lebenszyklus.

«Durch glaubwürdige und unabhängige Tests ist die Sicherheit digitaler Produkte zu überprüfen.»

Software eats the world

Trotz grosser Investitionen schafft es die Industrie nicht, sichere Software zu erstellen. Deshalb muss man sich mit Sicherheitsschwachstellen auseinandersetzen, neu auch in Bereichen ausserhalb der traditionellen Softwareindustrie (siehe auch Abb. 2). Das unabhängige Entdecken und Publizieren von Schwachstellen kann nicht verhindert werden. Entdecker von Schwachstellen wurden früher ignoriert oder mit Rechtsmitteln an der Publikation gehindert.

Viele Schwachstellen wurden daher nie oder nur mit grosser Verzögerung repariert, trotz der Risiken. Über die Zeit hat sich der Coordinated-Disclosure-Prozess etabliert: Ethische Entdecker melden die Schwachstelle unter Geheimhaltung zuerst dem Hersteller und geben ihm eine vernünftige Frist zur Entwicklung eines Sicherheitsupdates, bevor die Information publiziert wird[3].

Durch das Internet of Things (IoT) werden nun viele softwareferne Industrien und deren Produkte vernetzt, wobei die Erkenntnisse der Softwareindustrie (sichere Entwicklung, Coordinated Disclosure) oft ignoriert werden. Meldungen über Sicherheitsdefekte in digitalen Stromzählern, Überwachungskameras oder Thermostaten häufen sich.

Anforderungen für sichere digitale Produkte

Die Sicherung der Lieferkette wird in Zukunft zu einem entscheidenden Erfolgsfaktor für das Vertrauen in digitale Produkte und deren Hersteller. Heute muss der Kunde noch blind annehmen, dass sich die digitalen Produkte auf dem Markt für den vernetzten Einsatz eignen. Ohne Normen oder Qualitätslabel ist Sicherheit nicht transparent und somit kein Einkaufskriterium. Dies hemmt Investitionen der Hersteller in die Sicherheit digitaler Produkte.

Von der Entwicklung bis zur Auslieferung des Produkts ist primär der Hersteller in der Verantwortung. Danach erfolgt eine Verschiebung der Verantwortung zum Kunden (oder Betreiber) des Produkts. Dessen Sicherheit degradiert durch unsachgemässen Betrieb in unsicherem Kontext oder durch unsichere Konfiguration (z.B. Betrieb eines sicheren Autos mit abgefahrenen Reifen).

Tabelle 1 zeigt die wesentlichen Anforderungen zur Sicherheit in Entwicklung, Herstellung und Betrieb von digitalen Produkten.

Es ist unumgänglich, dass Gesellschaft, Industrie und Politik gemeinsam die folgenden Fragen diskutieren und die entsprechenden Themen entwickeln:

- Welches sind Minimalanforderungen an die Integrität und Sicherheit von digitalen Produkten und Diensten?
- Welche Minimalanforderungen gelten für welche Art von digitalen Produk-

	Cyberanforderungen	Vergleich mit Automobilindustrie
1	Etablierte Sicherheits- und Qualitäts-anforderungen für digitale Produkte	Gesetzliche Normen und Industriestandards
2	Belastbare Deklaration und Nachweis des Herstellers zu Sicherheitsaspekten des Produkts	– Deklarationen im Rahmen des Zulassungs-verfahrens – Tauglichkeitsnachweis durch Crashtest
3	Transparenz und Überprüfbarkeit der Sicherheit des Produkts	Externe unabhängige Tests (z.B. TÜV, National Transportation Safety Board)
4	Sichere Grundeinstellungen und Erstkon-figuration bei Inbetriebnahme. Automati-scher Update-Mechanismus des Produkts	Aktive und passive Sicherheit wie redundan-te Bremskreise, Airbag, Sicherheitsgurten, Sicherheitsglas sowie Knautschzonen
5	Zeitnahes Bereitstellen von Sicherheitsup-dates über den vereinbarten Lebenszyklus	– Garantieleistungen und Rückrufaktionen bei Defekten (zulasten des Herstellers) – Wartungsplan – Periodische Motorfahrzeugkontrollen

Tabelle 1: Diese fünf Punkte sind die wesentlichen Anforderungen zur Sicherheit in Entwicklung, Herstellung und Betrieb von digitalen Produkten. Ein Vergleich mit der Automobilindustrie.

ten, Diensten, Anwendungsbereichen oder Industriesektoren?
- Wie kann die Einhaltung der Mini-malanforderungen überprüft werden, nicht nur bei der Zulassung, sondern auch während des gesamten Lebens-zyklus?

Diese verbindlichen Qualitätsnormen entsprechen in der Automobilindustrie den uns vertrauten aktiven und passiven Sicherheitsvorkehrungen und den vorge-schriebenen Services der Hersteller oder der periodischen unabhängigen Über-prüfung der Fahrtüchtigkeit durch die Kantone.

Die Industrie- und Technologiege-schichte zeigt, dass die Erarbeitung und Einführung entsprechender Sicherheits- und Qualitätsanforderungen oft Jahr-zehnte in Anspruch nimmt:
- Ralph Naders Buch «Unsafe at any Speed» von 1965 veranschaulicht diesen Konflikt und führte nach Auseinandersetzungen mit der Auto-mobilindustrie zur Einführung von Sicherheitsgurten und Crashtests sowie zu Produktrückrufen.[4]
- Die Flugzeugindustrie bekämpfte in der Frühzeit die Tests von Flugmoto-ren; über die Hälfte bestanden die ersten Tests anschliessend nicht.[5]

Was kann man bereits heute zur Si-cherung der Lieferkette tun?

Konkrete Anforderungen

Der Kunde muss in der Lage sein, vom Hersteller einen verbindlichen Nachweis zur Sicherheit des Produktes einfordern zu können. Sicherheitsanforderungen sind in einem Security-Appendix (Ver-tragsanhänge) festzuhalten. Industrie- und Branchenverbände sollten einheitli-che Vertragsanhänge erarbeiten und ihren Mitgliedern als Vorlage zur Verfügung stellen. Einheitlich dokumentierte und angewandte Sicherheitsanforderungen sind einfacher durchsetzbar und verein-fachen den Einkaufsprozess für Kunden wie auch Lieferanten.

Konkrete Anforderungen sind:
1. Der Hersteller verpflichtet sich zur vollständigen und abschliessenden Dokumentation aller im Produkt eingebauten «Default Accounts», Passwörter, Call-Home-Funktionen, Zertifikate und Keys/Schlüssel. Später entdeckte Zugänge gelten als Backdoor.
2. Der Produktlebenszyklus und die kontinuierliche Lieferung von Sicher-heitsupdates wird belastbar vereinbart.
3. Der Hersteller verpflichtet sich zu Coordinated Disclosure (ISO 29147) zur Handhabung von gemeldeten Schwachstellen. Er dokumentiert die Umsetzung des Prozesses, die An-sprechpartner und Bearbeitungsdau-er.
4. Der Hersteller räumt dem Kunden das Recht ein, die Hard- und Software des Produkts auf Integrität und Sicherheit zu prüfen (Reverse Engi-neering) ohne die Verletzung der Intellectual Property Rights (IPR).
5. Einhalten der anwendbaren nationa-len und internationalen Standards (z.B. Nist Cyber Security Framework, ISO, Common Criteria, Nist 800-161, EU4, EU5, Fips) zum Vendor Risk Management und zur Produktesi-cherheit von technischen, insbeson-dere vernetzten Systemen.

Fazit

Ohne effektive Qualitätsprüfung von di-gitalen Produkten muss davon ausgegan-gen werden, dass kompromittierte Kom-ponenten bereits heute im Einsatz sind. Durch glaubwürdige und unabhängige Tests ist die Sicherheit digitaler Produkte zu überprüfen. Cybersecurity darf sich dabei nicht auf Software, Netzwerksi-cherheit und den Faktor Mensch be-schränken, die Integrität und Sicherheit der Hardware ist mit einzubeziehen.

Ziel ist, für den Kunden ein transpa-rentes Sicherheitslabel ähnlich der Ener-gie-Etikette zu schaffen. Nur so werden die Chancen der Digitalisierung auch in Zukunft deren Risiken überwiegen. ■

Dieser Artikel basiert auf der Arbeit der Arbeitsgruppe Supply Chain Security von ICT Switzerland und dem Whitepaper Supply Chain Security vom September 2019. Infos: www.ictswitzerland.ch/white-paper-supply-chain-security

QUELLEN

1 Significant Cyber Incidents since 2006, http://bit.ly/2RqTbs8

2 Compromised By Design? https://brook.gs/30usoiB

3 ISO-IEC 29147 Standard zur Hand-habung von Schwachstellen, http://bit.ly/2swt0aT

4 Unsafe at Any Speed: The Designed-In Dangers of The American Automobile, http://bit.ly/2u4aYg0

5 A History of Aviation Safety: Featuring the U.S. Airline System, https://amzn.to/2FZGPSs

CHRISTOF JUNGO
Secintel GmbH
DR. STEFAN FREI
Accenture AG und ETH Zurich