Digitale Souveränität und die Einschätzung der Sicherheit von Lieferketten – eine Managementdisziplin. Problembeschreibung und Lösungsansätze

Ramon Mörl[1]

Kurzfassung:
Ein Handy ist nicht aus, wenn ein Anwender es ausgeschaltet hat. Der Anwender kann immer noch abgehört werden. Der Anwender ist nicht digital souverän. Der Artikel klärt, welche Maßnahmen ergriffen werden können, um Transparenz in die potenzielle Unsouveränität zu bringen und die Souveränität in nicht akzeptablen Abhängigkeiten gezielt zu verbessern.

Stichworte: Beschaffung, D.S. (Digitale Souveränität), Digitale Souveränität, , Heartbleed, ITSiG 2.0, Lieferkette, Log4Shell, No Spy, Sicherheitsarchitektur, Transparenz, Vertrauenskette

1. Management Summary

Digitale Souveränität – im Folgenden D.S. – ist begrifflich nicht klar definiert. In diesem Beitrag wird ein Akteur im Cyber-Raum als digital souverän bezeichnet, wenn er seinen Willen eigenständig durchsetzen und das Ergebnis sicher kontrollieren kann.

Beispielsweise ist das Ausschalten eines Handys nicht als souverän zu bezeichnen, denn nicht nur die Erkenntnisse aus den Pegasus- und den Snowden-Papieren haben gezeigt, dass auch im ausgeschalteten Zustand über Positionsmeldungen, Mikrofon und Kamera Überwachungsmöglichkeiten bestehen, die der Nutzer des Handys nicht mittels digitaler Mechanismen abschalten oder kontrollieren kann. Diese Einschränkung der Souveränität wird dem Nutzer auch nicht beim Kauf oder bei der Inbetriebnahme vermittelt.

In diesem Beitrag wird geklärt, welche Auswirkungen diese Erkenntnis auf verschiedene Akteure im Cyber-Raum haben könnte und welche Disziplinen notwendig wären, um in konkreten Handlungsszenarien die D.S. in geeigneter Weise den Anforderungen anzupassen.

In diesem Sinn ist D.S. ein Management-Prozess, dessen Ziel darin besteht, durch konkrete Verfahren Defizite in der D.S. erkennbar und die daraus resultierenden digitalen Abhängigkeiten kommunizierbar zu machen. Eine Prüfung unter Kosten-/Nutzen-Aspekten bildet die Grundlage für die Entscheidung, diese Defizite bei Bedarf zu minimieren oder ganz zu beheben und einem Controlling zu unterwerfen.

Da nicht jedem Akteur im Cyber Space das Know-how zur Verfügung steht, seine D.S. vollständig zu beurteilen, heutige Produkte zum großen Teil digitale Elemente enthalten und viele Produkte wie z. B. Autos, Züge oder Flugzeuge digitale Schnittstellen für potenziell Unbekannte anbieten, ergeben sich Abhängigkeiten, die die Komplexität signifikant erhöhen.

[1] itWatch GmbH, 81549 München

Die gesamte Lieferkette, alle Teilintegrationen, die beteiligten Betreiber können die D.S. eines Anwenders beeinflussen. Dadurch wird es notwendig, eine Vertrauenskette entlang der Lieferkette zu etablieren und die angebotenen Endprodukte bzgl. der D.S. auch mit zugesicherten Eigenschaften auszustatten und dafür mit einer Haftung zu unterlegen.

2. Themeneinführung

Aktuell wird diese Zuverlässigkeit des Systems und die Möglichkeit des Besitzers, in diesem System seinen Willen durchzusetzen, als Souveränität der Handlung oder, wenn es um IT geht, als Digitale Souveränität oder D.S. bezeichnet.

Bereits im Jahr 2017 hat Ursula von der Leyen als Verteidigungsministerin ausgeführt, dass die Fähigkeiten der Bundeswehr und das dazu benötigte Material zu Wasser, zu Lande und in der Luft viele Milliarden Euro kosten, aber die Nutzung all dieser Fähigkeiten fast vollständig von der in den Systemen integrierten IT-abhängig ist – dass also letztlich der Schutz dieser IT erst die Grundvoraussetzung dafür schafft, diese Fähigkeiten auch wirklich wie geplant nutzen zu können.

Diese Aussage gilt fast überall. Ob Mobilfunkgeräte, der internetfähige Kühlschrank, Autos, Flugzeuge, ICEs, Smart Home, Smart City oder einfach nur vernetzte IoT Devices: Das sind viele Beispiele von „Geräten“, deren Nutzung immer mehr von zugrundeliegenden IT-Komponenten abhängt.

Je weiter fortgeschritten die Digitalisierung in einem Produkt oder einer geplanten Wirkkomponente ist, je mehr das genutzte Gesamtsystem digitale Lösungen voraussetzt und je kritischer zum einen das digitale Subsystem für die Nutzung des Gesamtsystems und der spätere Einsatzbereich des Gerätes ist, umso wichtiger wird es, dieses digitale Subsystem geeignet dagegen zu schützen, dass der Wille der Nutzer nicht durchgesetzt wird. Um zu definieren welcher Schutz „geeignet“ ist, sind die klassischen Disziplinen des Risikomanagements hilfreich. Wie können die Risiken in diesem Anwendungsbereich minimiert werden?

Die digitalen im Endprodukt verbauten Komponenten benutzen häufig Standardbausteine in Hardware, Firmware und Software.

Am Beispiel von Heartbleed[2] und Log4j[3] wird klar, dass der Betreiber oder Händler von Geräten über alle verbauten Subsysteme informiert oder in kurzer Zeit informierbar sein muss, um potenziell zeitkritische Defizite in der D.S. sofort eliminieren zu können.

D.S. ist also keine binäre Entscheidungsfrage (ja/nein), sondern Teil des Risikomanagements. Ziel ist es, den Entscheidungs- und Planungsprozess hinsichtlich digitaler Souve-

[2] Der Heartbleed-Bug ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek Open SSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden können. Der Fehler betrifft die OpenSSL-Versionen 1.0.1 bis 1.0.1f und wurde mit Version 1.0.1g am 7. April 2014 behoben.

[3] Seit dem 10.12.2021 warnt das BSI vor einer extrem kritischen Bedrohung in der Java-Bibliothek "Log4j". Die Sicherheitslücke (CVE-2021-44228) hat den Namen "Log4Shell" erhalten und führt eventuell zur Verwundbarkeit von global mehreren Milliarden Computern.

ränität zu verbessern und Empfehlungen bezüglich des Prozesses abzugeben, um das Management der D.S. als Teil der Digitalisierungsstrategie zu ermöglichen.

Um die Risiken managen zu können, muss man natürlich zuerst verstehen, welche Komponenten enthalten sind und wie diese aktualisiert oder durch andere Mechanismen verändert werden können – geplant, durch Angriffe oder Fehlverhalten. Erst dann kann man die Risiken des Gesamtsystems beurteilen und auf das gewünschte Maß minimieren.

Ziel dieses Beitrags ist es, die sinnvollen Verfahren und Managementmechanismen aufzuzeigen, die zur notwendigen Transparenz der fertig integrierten Produkte führen und eine Bewertung der Vertrauenswürdigkeit der Liefer- und Integrationskette nach den gängigen Sicherheitszielen Verfügbarkeit/Verlässlichkeit, Integrität und in manchen Punkten auch Vertraulichkeit ermöglichen. Ein „Aufsummieren“ von Sicherheitseigenschaften der einzelnen verbauten oder genutzten Elemente ist ein notwendiges, aber leider nicht hinreichendes Verfahren, um Aussagen über das Gesamtsystem treffen zu können.

In diesen Artikel werden die Ergebnisse der Arbeitsgruppen und Gespräche, die mit den Verbänden bitkom, BDSV, TeleTrusT, Sicherheitsnetzwerk München, DIN und verschiedenen Universitäten – allen voran der Universität der Bundeswehr – geführt wurden, sowie die Vorhaben zur Standardisierung von Begriffen und das Vorgehensmodell zu Trust und Vertrauensketten sowie viele Gespräche mit Forschungsinstituten, die auf dem Gebiet „Modellieren von Vertrauen“ forschen, eingebracht.

Allen Gesprächspartnern möchten wir an dieser Stelle herzlich danken, da sie mit ihren Beiträgen und den regen Diskussionen ermöglicht haben die vielen Facetten des Themas zu beleuchten.

3. D.S. managen

D.S. ist demnach kein definierter, erreichbarer Endzustand, sondern beschreibt den Wunsch nach einem selbstbestimmteren Handeln im Cyber- und Informationsraum (kurz CIR). Dieser Selbstbestimmung stehen verschiedenste Bedrohungen und damit verbundene Risiken im Weg, die zum einen durch Katastrophen aber auch mutwillig durch Dritte herbeigeführte oder als kollaterale Schäden in Kauf genommene Ereignisse eintreten können. Ein anhaltender Stromausfall ist beispielsweise ein Risiko, welches das souveräne Handeln im CIR beeinträchtigt, da die Nicht-Verfügbarkeit von Informationen oder digitalen Services den Handelnden in eine nicht souveräne Warteposition wirft. Der Verlust an Vertraulichkeit von Informationen beeinträchtigt ebenso wie der Verlust oder die Nicht-Prüfbarkeit der Integrität von Daten oder Systemzuständen die D.S.

Risiken aus diesem Bereich können über Haftungsszenarien sehr einfach auf Hersteller und Lieferanten durchschlagen. Abbildung 1 zeigt, wie das Management der Digitalen Souveränität in einer Organisation oder für ein Produkt durchgeführt werden kann:

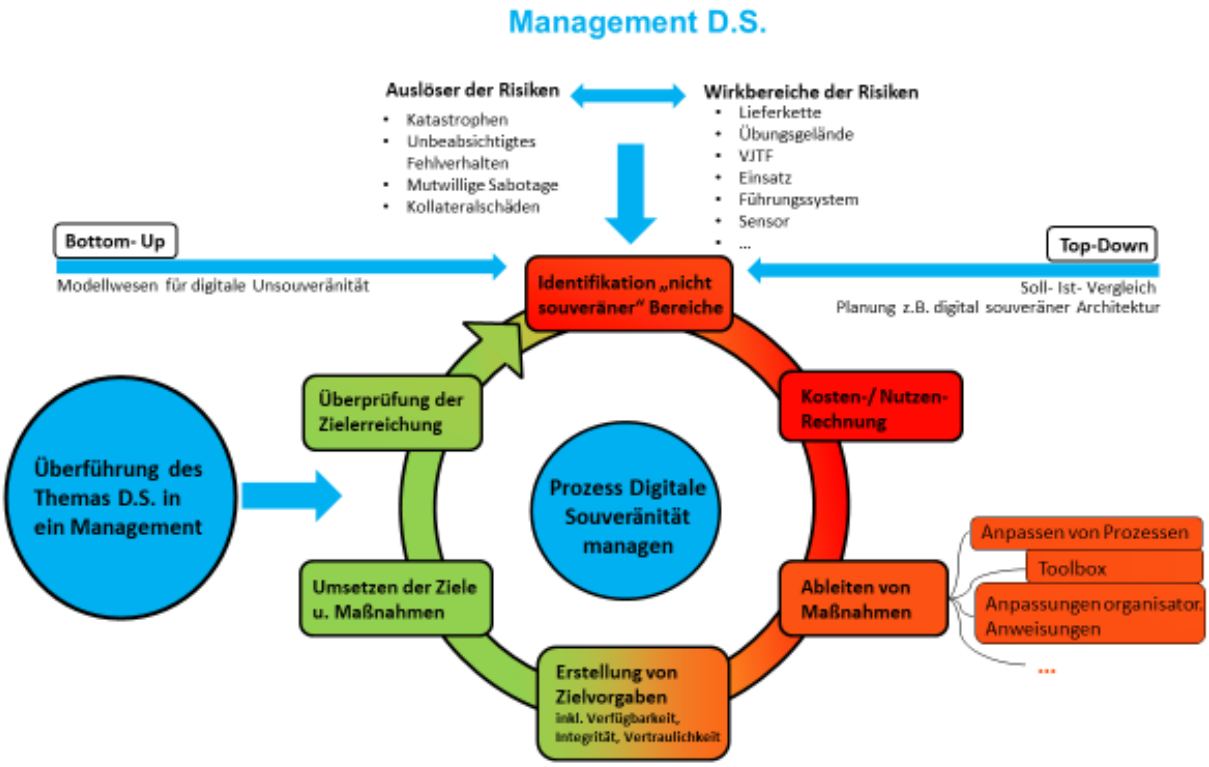

Abbildung 1: Digitale Souveränität managen

Digitale Risiken werden traditionell im Bereich der Cyber Security behandelt. Deshalb ist für D.S. auch in der Sprachwelt eine große Nähe zu den Risiken der Verfügbarkeit, der Integrität und der Vertraulichkeit gegeben.

4. Beteiligte am Managementprozess

Innerhalb einer Organisation sind nicht nur die Positionen CSO, CIO, CISO, Riskmanager und BCM beteiligt, sondern auch Einkauf, Rechtsabteilung, Business Owner, und viele weitere, um zum einen die Risiken zu identifizieren, aber auch um die geeignete Minimierung monetär bewerten zu können.

Auch wenn dieser Prozess bereits sehr komplex ist, muss für das Management der D.S. auch die gesamte Lieferkette mit ihren unterschiedlichen Organisationen und der jeweils gültige Rechtsrahmen der in globalen Lieferketten Handelnden berücksichtigt werden. In jeder Organisation sind wieder die oben beschriebenen, verschiedenen beteiligten Ansprechpartner relevant.

Die Anteile im BCM haben häufig auch mit der Verfügbarkeit von Ware zu tun, wie in 2021 durch die Lieferkettenunterbrechung und die Pandemiefolgen deutlich wurde. Die digitalen Anteile im Risikomanagement folgenden Themen der Cyber Security.

5. Hierarchie der Managementmechanismen

Auf der 7. Munich Cyber Security Conference (mcsc) 2021, einer regelmäßigen internationalen Konferenz am Tag vor der msc, wurde Ramon Mörl in einem Panel mit dem Titel „Corporate Cyber Risk Management – What Makes the Difference?“ von Mode-

rator Kai M. Hermsen[4], Global Coordinator of the Charter of Trust, Siemens (Munich), die Frage gestellt: „Wie ist der Zusammenhang zwischen dem Ecosystem Lieferkette und dem Risikomanagement*?"*[4]

Mörl erklärte „Das Risikomanagement ist die Top-Disziplin. An zweiter Stelle steht die Digitale Souveränität, mit der wir es schaffen unsere Bordmittel so zu gestalten, wie es unserem Bedarf entspricht, ohne dass uns irgendjemand in unserem Cyber-Raum stören kann. An 3. Stelle steht die Cyber-Sicherheit, mit der wir das Risiko, nicht arbeitsfähig zu sein, durch die Erhöhung unserer Investitionen in den Schutz reduzieren."

Hier ist bereits aufgezeigt, dass die bekannten Mittel der Cyber Security auch die probaten Mittel sind, um die Ziele der D.S. zu erreichen. Entnetzung oder Isolierung – also das Abkoppeln von anderen Netzen oder Informationsquellen, insbesondere dem Internet ermöglicht es, ein mit hohen Risiken eingestuftes System, bei dem die D.S. nicht den eigenen Wünschen entspricht, zumindest für eine Übergangszeit so zu betreiben, dass die IT-Ziele, eventuell mit Abstrichen z. B. in der Performance oder der Ergonomie, erfüllt werden können, aber die Risiken des unkontrollierbaren Eingriffes durch Dritte auf ein erträgliches Maß reduziert werden kann.

6. Wer spricht mit wem wie über die Risiken?

Normalerweise ist die Kommunikation „nach außen" in einer Organisation klar definiert. Nicht jeder ist berechtigt, über potenzielle Risiken in den hergestellten Produkten oder erbrachten Services beliebig nach außen zu kommunizieren.

In einigen Regionen sind Teile dieser Kommunikation bereits staatlich reguliert. Siehe z. B. das IT-Sicherheitsgesetz 2.0[5] in Deutschland.

Neben den fest vereinbarten Kommunikationskanälen kommen aber zunehmend auch anonyme oder sogar durch Gesetze regulierte Kanäle wie z. B. das „Whistleblowing"[6] dazu. Je anonymer ein Kanal ist, umso mehr muss natürlich eine Metrik und ex ante ein Prozess definiert und etabliert werden, wie die Glaubwürdigkeit der anonym eingebrachten Information bewertet werden kann.

Die Risiken lassen sich aufteilen in solche, die bei Beschaffung bereits (abstrakt) bekannt waren und solche, deren Existenz erst später entdeckt wurden. So ist ein abstrakt bekanntes Risiko das der „Hintertür"[7]. Der rechtlich saubere und mit einer hohen Haftung belegte Ausschluss dieses bekannten Risikos ist aber nicht einfach, wie z. B. auch die Diskussionen um den „No Spy Act"[8] zeigen.

---

[4] Weitere TeilnehmerInnen des Panels waren Martin Clements, Security Advisor Credit Suisse (Zurich), Mihoko Matsubara, Chief Cyber Security Strategist NTT Corp. (Tokyo), Melody Balcet, Director Operational Risk Barclays (Washington D.C.)

[5] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

[6] Beim Whistleblowing werden Hinweise auf Missstände in Unternehmen, Hochschulen, Verwaltungen etc. gegeben. Der Whistleblower ist meist Mitarbeiter oder Kunde und berichtet aus eigener Erfahrung. Er informiert Mittler und Medien oder direkt die Öffentlichkeit.

[7] Eine „backdoor" oder Hintertür ist ein Weg, um auf ein Computersystem oder verschlüsselte Daten zuzugreifen, der die üblichen Sicherheitsmechanismen des Systems umgeht.

[8] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html

Zur Bewertung der Qualität einer vereinbarten Haftungssituation für zugesicherte Eigenschaften gehören nicht nur Juristen, da sich in der Vergangenheit gezeigt hat, dass auch ein vorhandener Titel wegen verschiedener internationaler Gründe oder auch einfach wegen einer Insolvenz der haftenden Tochterorganisationen nicht durchsetzbar ist.

7. Hintertüren und „Mehrwerte“ in der Daten- und Internet-Ökonomie

In der Welt der Datensammler hat es sich eingebürgert, dass Produkte – auch Hardware – günstiger angeboten werden können, wenn über diese Produkte Daten zur Nutzung und über die Nutzer gesammelt werden können (Daten- und Internet-Ökonomie). In den meisten Beschaffungsvorgängen von Standardhardware wird diese "Zusatzfunktion" nicht explizit unter Strafe ausgeschlossen, sodass es gut sein kann, dass ein verbautes Element "von sich aus" aus Eigeninteresse des Herstellers wichtige Informationen nach außen gibt.

Die aus Sicht der Integrität schädlichen Veränderungen können natürlich auch nachträglich ohne Wissen des Herstellers z. B. auf dem Transportweg als Patch auf die Firmware eingebracht werden, wenn kein geeigneter Schutz dagegen besteht.

Die Daten- und Internet-Ökonomie treibt eigene Märkte an, sodass auf den ersten Blick günstige oder sogar kostenfreie Angebote mit Bewegungsdaten, persönlichen oder Unternehmensdaten „bezahlt“ werden, ohne dass der Anwender darüber informiert ist oder wird.

In Europa erfolgt traditionell die Beschaffung über Merkmale, die das Produkt haben soll (Leistungspunkte) und solche, die zum Ausschluss führen. Darauf basierend wird das beste Preis-/Leistungsverhältnis ermittelt. Diese Vorgehensweise ist immer schlecht für die D.S., denn der Nachweis, dass Hintertüren oder unsichtbare „Mehrwerte“ enthalten sind, kann entweder gar nicht erbracht werden, oder die vereinbarten Pönale sind gering im Vergleich zu dem Gewinn, der mit der gesammelten Information erzielt wurde.

Ein Produkt mit geeigneten „Mehrwerten“ kann immer deutlich unter Marktpreis angeboten werden, denn der wirtschaftliche Gewinn wird über die Datenökonomie erzielt.

8. Beispiel zur Infiltration einer Lieferkette

In vielen der digitalen Nutzungsszenarien sind Basiselemente wie z. B. Bluetooth Chips verbaut. Diese Chips sollen gerade die Möglichkeit haben, nach außen zu kommunizieren – aber nur kontrolliert, wenn der Besitzer bzw. Anwender das wünscht. Mit einer Hintertür kann diese Kommunikationsfähigkeit aber auch ohne Wissen des Anwenders von außen aktiviert werden.

Für eine sicherheitskritische Verwendung werden z. B. 10.000 Geräte einer besonderen Verwendung ausgeschrieben und später bestellt. Der Lieferant bestellt, zur Fertigstellung der Lieferung, seinerseits im Markt die benötigten Bauteile, z. B. Bluetooth Chips – immer in Stückzahlen 10.000 oder größer. Es bedarf nun keiner intensiven

Aufklärung, um einzelne Komponenten, deren Lieferanten und deren Lieferwege herauszufinden. Im Markt sind verschiedene Verfahren bekannt, um mit dieser Information das Endprodukt in gewünschter Art zu modifizieren. So werden z. B. Fabriken, die nicht 24/7/365 ausgelastet sind, mit einer Sonderschicht beauftragt, wobei sich die hergestellten Produkte in der digitalen Bestückung durch eine Hintertür oder einen digitalen „Mehrwert" unterscheiden. Das gleiche Ergebnis kann erzielt werden, indem die Standardprodukte im Markt gekauft werden und dann nachträglich anders digital bestückt und z. B. zu günstigeren Preisen in die Lieferkette eingebracht werden. Hier ist z. B. die Veränderung der genutzten Controller oder der Firmware zu nennen, wie das von Carsten Nohl in seinem Vortrag auf der Black Hat 2014 beschrieben wurde. Diese Angriffsart ist als BadUSB bekannt und wurde 2015 auf dem BSI Kongress diskutiert[9].

Wieder sind die Qualitätsmanagementsysteme meist nicht darauf ausgelegt, mit dieser Bedrohung der D.S. umzugehen. Ein häufig verwendetes Konzept, diese Art der Bedrohung zu minimieren ist es, Bestellungen in unterschiedliche Lieferkanäle zu geben und von verschiedenen Legal Entities aus zu organisieren. Leider verteuert dies den Prozess und die Einzelteile und schafft nur statistisch gesehen einen verbesserten Schutz. Je nach Architektur des digitalen Produktes kann es auch sein, dass ein einzelnes infiltriertes Gerät in der Lage ist, Daten aus allen anderen Geräten zu ermitteln und über die eigene Hintertür zu exfiltrieren, also auszuleiten. Insofern ist eine statistische Verbesserung einzelner Bauteile oft keine Verbesserung des Gesamtsystems.

9. Multi-Sourcing erhöht häufig die Angriffsmöglichkeiten

Um die zielführenden Managementmechanismen aufzeigen zu können, die zur Transparenz der fertig integrierten Produkte führen, muss eine Bewertung der Vertrauenswürdigkeit der Liefer- und Integrationskette nach den gängigen Sicherheitszielen Verfügbarkeit, Integrität und Vertraulichkeit ermöglicht werden. Und man muss verstehen, dass ein einfaches „Aufsummieren" von Sicherheitseigenschaften nicht das gewünschte Ziel erreicht.

Ein Beispiel dazu: Ein Unternehmen kauft zwei Firewall-Systeme von zwei Herstellern, um „die Sicherheit" des Gesamtsystems zu erhöhen. Diese Firewall-Systeme erhöhen nun die Integrität und die Vertraulichkeit des Systems, wenn sie hintereinander „auf der gleichen Nutzleitung" geschaltet werden, da ein Angreifer beide Systeme überwinden muss, um in die Unternehmens-IT einzudringen.

Auf der anderen Seite reduziert diese Nutzungsart die Verfügbarkeit, denn der Ausfall eines der Systeme macht die Kommunikation insgesamt unmöglich. Schaltet man die zwei Firewall-Systeme aber parallel, also auf zwei verschiedenen Zugangsstrecken in die Unternehmens-IT, erhöht man die Verfügbarkeit, reduziert aber gleichzeitig die Integrität und die Vertraulichkeit.

[9] Vortrag Ramon Mörl auf 14. Deutschen IT-Sicherheitskongress des BSI 2015: „Bad USB, vergleichbare Exploits - sinnvolle Verteidigungsstrategien" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-20-05-2015/Ramon_Moerl.pdf;jsessionid=699EDCA9AF835132914918221870 7F97.internet461?__blob=publicationFile&v=1

Diesen Zusammenhang kann man abstrakt als „Verfügbarkeit steht orthogonal zu Integrität und Vertraulichkeit“ bezeichnen. Dass das häufig gilt, sieht man, wenn man mehrere Verschlüsselungssysteme auf den gleichen Nutzdaten von mehreren Herstellern in ein System integrieren möchte, denn dann muss jedes Produkt auf alle Daten zugreifen können. Eine Hintertür in einem Produkt gefährdet die Vertraulichkeit aller Daten.

Multi-Sourcing ist also kein geeignetes Mittel, welches bei den Zielen Integrität und Vertraulichkeit hilft, wird aber als Hilfe für die Erhöhung von Verfügbarkeit und gegen Monopolbildung wahrgenommen. Zu den Verfahren, die benötigt werden, um sich vor der Abhängigkeit von Monopolbildung zu schützen, gehört aber ein weites Spektrum an Möglichkeiten, welches ein strategisches Management und einen detaillierten Überblick über ökonomische und technische Verflechtungen voraussetzt.

10. Digitale Risiken sind zeitlich „volatil“

Zu der bereits beschriebenen Komplexität kommt, dass digitale Elemente fast immerwährend ihrer Lebensdauer – oft ohne Kenntnis des Anwenders – verändert werden können. Ein System, welches integer ausgeliefert wurde, kann nach einiger Zeit durch einen „Patch“ verändert werden. Wenn diese Veränderung nicht beweissicher dokumentiert wird, kann sie unbeobachtet wieder zurückgesetzt werden, sodass auch erfolgreiche Angriffe ex post oft nicht mehr beweisbar sind.

Insofern bedarf es bei der Wahl der Bewertungsalgorithmen für die Vertrauenswürdigkeit von Komponenten und deren Lieferketten verschiedener Attributierungen und Auswertungsalgorithmen, die hier andiskutiert werden.

11. Vertrauenswürdigkeit von digitalen Produkten und der Lieferkette

Die Annahme, dass etwas per se vertrauenswürdig ist, ist falsch. Eine Bank mit der BAFin als Aufsicht ist vertrauenswürdig für definierte Geldgeschäfte, aber nicht per se vertrauenswürdig für „alles“. Einer Straße würde man hingegen nicht einfach Geld anvertrauen und annehmen, dass das Geld nach einigen Tagen noch da liegt. Diese Attributierung von Vertrauen – also ein Vertrauen für eine konkrete Sache – ist intuitiv in der analogen Welt und wird auch da, wie Bild 2 zeigt, manchmal gebrochen.

Abbildung 2: Busunglück 1994 in Trudering, München (Quelle: Abendzeitung München)

12. Notwendige Kenntnis aller Subsysteme

Im Zuge der Betrachtung der inhärenten Sicherheit der IT in einem System wird deutlich, dass der Bedarf an Sicherheit als Eigenschaft des Systems nicht nur durch die bei der Nutzung des Systems getätigten Handlungen, sondern auch durch die bei der Entwicklung, Fertigung, Integration von Komponenten und Lieferung des Systems definierten und gegebenenfalls böswillig manipulierten Eigenschaften, bestimmt wird.

Eine Software ist nicht per se sicher oder unsicher, sondern wird durch die gesamte Entwicklungsumgebung, die evtl. nötige Run Time oder den Compiler und das Umfeld, in dem sie schließlich zum Einsatz kommt, in ihren Sicherheitseigenschaften definiert[10].

Insofern ist es wichtig zu wissen, was denn eigentlich in den fertigen Produkten alles verbaut ist und wie sie hergestellt wurden. Und es ist auch unerlässlich, die Sicherheitseigenschaften dieser Teilkomponenten inklusive der Zusicherungen entlang des gesamten Lieferungs- und Herstellungsprozesses geeignet „aufzuaddieren“. Beispielsweise wäre es im Fall von Heartbleed notwendig gewesen, dass alle Verwendungen der betroffenen Software im Betrieb bekannt gewesen wären – was leider nicht der Fall war – da diese Open Source Lösung an vielen Stellen in zugelieferten Produkten genutzt worden war, ohne dass es dem Käufer oder Nutzer eines Endproduktes bekannt war.

Der Nutzer oder Betreiber konnte also das schädliche Teilstück oft gar nicht isolieren, ersetzen oder patchen, weil er von dessen Existenz im Gesamtprodukt nichts wusste.

Erschwerend kommt zum Tragen, dass der bestehende Kosten- und Wirtschaftlichkeitsdruck und die Globalisierung in der Vergangenheit zu einer Spezialisierung der einzelnen beteiligten Unternehmen, einem hohen Time-To-Market-Druck und damit zu einer höheren Fragmentierung und Internationalisierung der Fertigungs- und Lieferketten geführt haben. Diese Ketten bestehen auch aus den Schritten vor und nach der Lieferung, der Integration und Inbetriebnahme eines Systems. Wenn man nicht genau weiß, welche Komponenten verbaut sind und wie diese verändert werden können, kann man die Risiken nicht einschätzen und dadurch die D.S. nicht managen.

13. Risiken in Lieferketten

Es gibt nun traditionelle Mechanismen, die Risiken in den Lieferketten bezüglich der Vertrauenswürdigkeit und Sicherheit nach den eigenen Interessen zu optimieren. Erhöhung der Haftung in den Verträgen oder eigene Qualitätsprüfungen sind beispielhaft solche Mechanismen. Erfahrungsgemäß ist das Testen auf unbekannte Funktionen um den Faktor 10 bis 1000 teurer als das Testen auf die Funktionsfähigkeit der vereinbarten Nutzfunktionen. Insofern ist es extrem teuer, nachträglich auf Hintertüren oder unerwünschte Funktionen zu testen, da diese auch, abhängig von z. B. Zeitpunkten, Geolokationen, ungewöhnlichem Nutzerverhalten oder anderen unerwarteten Situationen, spontan aktiviert werden können.

[10] Pressemeldung von itWatch, 16.12.2021: https://itwatch.de/News/Sicherheitsluecke-Log4j-ist-kein-Problem-beim-Einsatz-von-itWatch-Produkten

Oft ist es auch nachträglich gar nicht mehr möglich, in die verbauten Teile hineinzusehen, da z. B. bei besonders gegen Beschädigung durch Wasser, Stoß oder Umwelteinflüsse geschützten Systemen nachträglich nicht mehr auf die Einzelkomponenten zugegriffen werden kann, ohne das System signifikant zu beschädigen.

14. Modellieren von Vertrauensketten in Lieferketten

Strategisch ist es also essenziell, die Lieferketten im Sinne der D.S. zu modellieren und die für eine D.S. geeigneten Eigenschaften der Produkte zu definieren, sodass die Erwartung an das Vertrauen der Lieferkette abgeleitet werden und dann vertraglich umgesetzt werden kann. Im globalen Handel wird es immer Parameter geben, die vertraglich schlecht oder gar nicht umgesetzt werden können. An diesen Stellen ist eine Regulierung – ähnlich wie eine CE-Kennzeichnung – ein möglicher Weg in globalen Märkten.

Aus Sicht der D.S. ist also die Freiheit von Hintertüren eine wesentliche Anforderung an digitale Zulieferungen, wobei das Risiko bei einer nicht vernetzten Kaffeemaschine geringer ist als an einer offenen digitalen Car2Car-Schnittstelle.

15. Ziele der D.S.

Erst wenn ein digitales Element in die Nutzung geht oder der Integrator die intendierte Nutzung kennt, wird die Kritikalität dieses Teilsystems sichtbar. Die Managementherausforderung bei D.S. besteht also darin, die Kritikalität der einzelnen Komponenten vorab zu definieren und die einzelnen Teilkomponenten und ihre Lieferwege mit der geeigneten Vertrauenskette und den richtigen Meldewegen für Vorfälle auszustatten. Dies geschieht durch ein Attributieren der Teilkomponenten, der beteiligten Organisa

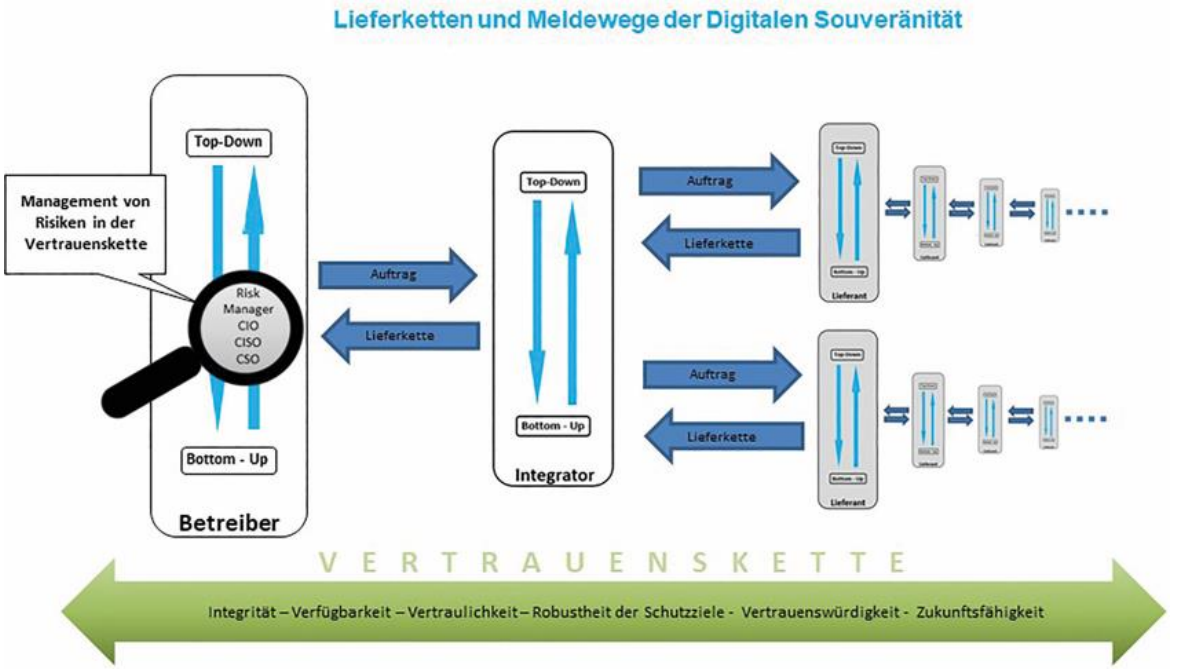

Abbildung 3: Die Lieferketten und Meldewege der Digitalen Souveränität

tionen, der Lieferkette, der Logistik und durch das Etablieren eines Vertragswerkes, welches die Ziele der D.S. respektiert.

Im Zuge des Managements der D.S. versucht man nun durch die Identifikation der „nicht souveränen Bereiche“, die mit der fehlenden Souveränität verbundenen Risiken und ihre Auswirkungen zu erkennen und in ein Management zu überführen. Das Management dieser Erkenntnisse kann Teil des Risikomanagements (RiskM) oder auch des Business-Continuity-Managements (BCM) oder anderer Disziplinen sein. Eine fehlende Souveränität in einem Bereich ist unproblematisch, wenn kein Risiko dadurch entsteht.

16. Identifikation von Risiken aus der D.S.

Es gibt mehrere Vorgehensmodelle, um Risiken aus der D.S. in bestehenden Systemen oder auch in zukünftig geplanten Systemen zu identifizieren:

16.1. Top-Down

Top-Down beschreibt die Möglichkeit, eine Landkarte der gesamten bestehenden digitalen Elemente in einer Organisation zu erstellen und dabei die extern angelieferten, die intern genutzten und erstellten sowie die an Dritte ausgelieferten Elemente zu unterscheiden, da die Möglichkeiten der Beeinflussung des D.S. in allen drei Fällen unterschiedlich sind. Die jeweils in diesen digitalen Elementen liegenden Risiken können abstrakt von den jeweiligen Ownern identifiziert und dann bei den höchsten Risiken mit konkreten Mechanismen der Architekturanalyse, White- und Black-Box-Tests sowie Penetrationstests bedarfsorientiert analysisert werden. Daraus resultieren dann konkrete Defizite der D.S., deren verbundene Risiken auch schon monetär bewertet sind, sodass es einfacher ist, eine Liste mit Prioritäten zu erstellen.

16.2. Bottom-Up

Eine pragmatische, effiziente Möglichkeit besteht darin, eine interne Meldestelle für signifikante Probleme im Umfeld der D.S. einzurichten. Dabei wird das Unternehmenswissen optimal genutzt, die monetäre Bewertung und die Einbettung in die gesamte Organisation muss aber jeweils noch erstellt werden. Zu den verschiedenen eingehenden Meldungen kann jeweils eine Kosten-/Nutzen-/Zeitbedarfs-Rechnung aufgemacht werden. Nach einigen Meldungen werden sich Schwerpunktbereiche und verschiedene Kritikalitätsstufen herauskristallisieren.

17. Welche Prozesse sind betroffen

Es ist zu kurz gesprungen, nur die Bestandssysteme zu betrachten, um dann mit potenziell neuen Mechanismen und Werkzeugen eine Verbesserung der D.S. herzustellen. Strategisch muss ein Management der Digitalen Souveränität (DSM) bereits bei der Beschaffung geeignete Maßnahmen vorsehen, wie die zu beschaffenden Produkte und Services unter den Anforderungen des D.S. unter Kosten-/Nutzen-Aspekten optimiert sind. Viele der Risiken der Informationssicherheit sind heute bekannt, und im Lebenszyklus notwendige Veränderungen zur Erhaltung oder Steigerung der Attraktivität können geplant werden.

Wie der Fall der Unix-basierten Endgeräte[11] in München zeigt, genügt es in der Kosten-/Nutzen-Rechnung nicht, die Vorteile aufzuzeigen. Es ist ebenso wichtig zu analysieren, welche neuen Risiken oder Verluste von Fähigkeiten bei dem vollständigen Ersetzen von Bestandssystemen entstehen (in dem Fall München z. B. die Fähigkeit der Nutzung von jeweils aktuellen IT-Bestandteilen anderer Systeme).

Es gilt also insbesondere, die Beschaffungs-, Entwicklungs- und Transformationsprozesse für digitale Produkte und Services mit einzubeziehen.[11]

18. Fehlende Metrik für das Management der D.S.

Verschiedene Untersuchungen[12] zeigen, dass das Fehlen von Metriksystemen und anderen Faktoren das Definieren konkreter erfolgversprechender Handlungsweisen für die Verbesserung von D.S. erschwert. Beispielsweise existieren für die Schutzqualität gegen Angriffsvektoren, die Vertrauenswürdigkeit von digitalen Systemen und die Verlässlichkeit von (zugesicherten) Systemeigenschaften keine konkreten Messverfahren und Maßeinheiten.

Die Zertifizierung von Produkten z. B. nach Common Criteria leidet darunter, dass nur gegen das Protection Profile, oder in den meisten Fällen ein selbst definiertes Security Target, zertifiziert wird. Zuerst also verstanden werden muss, ob dieses Zertifikat überhaupt für die intendierte Nutzung geeignet ist.

19. Bewusst definierte Grenzen der Souveränität

Für den Eigentümer/Besitzer eines auf IT zurückgreifenden Systems ist es wichtig, dass das System das tut, was der Eigentümer oder aktuelle Nutzer will.

Der Fahrer eines Kfz erwartet beim Drücken des Bremspedals eine Bremswirkung. Bereits vor Jahren wurden Angriffe live vorgeführt, wie ein Auto über mehrere hundert Meter Entfernung gegen den Willen des Fahrers gebremst wurde oder auch die Bremse blockiert werden konnte, sodass der Fahrer nicht mehr bremsen konnte.

In modernen Fahrzeugen wird aber bewusst auf „unterstützende“ Systeme gesetzt, die z. B. die Kollision von Fahrzeugen vermeiden sollen. Diese Systeme übernehmen in durch bestimmte Sensoren erkannten Gefahrensituationen einen Teil der Kontrolle und führen Aktionen eigenständig durch – z. B. eine Vollbremsung, um einen Unfall zu verhindern oder die Schäden abzumildern.

20. Beispiele für Risiken

Globalisierung: Im Zuge der D.S. wird immer wieder beklagt, dass viele Fähigkeiten aus dem lokalen, nationalen oder näheren Umland abgewandert bzw. verschwunden sind. In der Sprache der Geisteswissenschaftler wird eine langsame Erosion häufig als „slippery slope“ bezeichnet, um dazustellen, dass, wenn eine Sache einmal ins „Rut-

[11] heise.de: „Woran LiMux scheiterte und was wir daraus lernen können: 07.09.2020 — München galt als leuchtendes Beispiel für den Einsatz von Open-Source-Software in Behörden. Doch dann kehrte man zu Microsoft zurück.

[12] Ideenpapier zu Leitthema „Digitale Souveränität“, Ergebnisse des Expertenkreises BMVg, BDSV e.V., Bitkom e.V., Berlin 2021

schen“ gekommen ist und es keine gesetzten und nachhaltig gefestigten Haltepunkte gibt, das „Rutschen“ naturbedingt immer weiter und schneller stattfindet. Ein Blick in die Standardformel bei Ausschreibungen (Leistung/Preis) und die Praxis der Beschaffung (nicht nur bei öffentlichen Auftraggebern) zeigt, dass in dem Parameter Leistung keine Parameter für D.S. und ganz selten KPI (Key Performance Indicators) für die Vertrauenswürdigkeit, Qualität, die Sicherheit oder die Nachhaltigkeit der Ressourcen inklusive des Energieverbrauchs enthalten sind. Will man in der Beschaffung „low hanging fruits“ ernten, sollte die Transparenz des Inhalts jedes Bauelements, der Lieferkette, der Logistik, des Preiswettbewerbs sowie der verwendeten Standards gegeben sein, sodass Sicherheits-, Monopolisierungs- und Kontinuitäts-Problematiken nicht durch eine „best-price“ Beschaffung gefördert werden.

Verfügbarkeit: Eine manipulierte Motorsteuerung könnte z. B. auf ein bestimmtes Signal, das über die Luftschnittstelle, also ohne Kabel, ankommt, den Dienst einstellen. Das ganz Fahrzeug wäre nicht mehr nutzbar; ein Verlust der Verfügbarkeit, der den gesamten Invest in diese Technologie obsolet machen kann und Menschenleben in Gefahr bringen kann. Daraus resultieren moderne Erpressungsszenarien auf hochwertigen Produkten.

Integrität: Die angesprochenen Risiken der verfälschten Lieferung von Waren durch eine manipulierte Lieferkette oder der manipulierte Chip sind Risiken, die durch den Bruch der Integrität entstehen. Häufig ist die Integrität aber nicht einfach sichtbar, denn bei der Beschaffung eines Speicherchips schreibt man für gewöhnlich nicht in die Vertragsunterlagen, dass der beschaffte Chip keine Antennen und keine drahtlosen Kommunikationsfähigkeiten besitzen darf. Die Integrität ergibt sich also häufig aus der „Stand der Technik“- und „Best Practice“-Annahme, dass nur und ausschließlich das Geforderte enthalten sein darf – ohne das explizit in der Beschaffung unter Vertragsstrafe zu nehmen. Durch den Verlust der Integrität kann ein Gegner Fähigkeiten einbringen, die zum Verlust der Verfügbarkeit und/ oder zum Verlust der Vertraulichkeit führen.

Vertraulichkeit: Kommunikation sensibler Inhalte findet im digitalen Raum meist mittels Verschlüsselung statt. Die Verschlüsselung kann ein guter Schutz vor dem Verlust der Vertraulichkeit sein. Anwendungen, die auf den sensiblen Daten arbeiten, benötigen diese aber immer im Klartext (homomorphe Verschlüsselungen sind noch nicht einsatzfähig). Gelingt es also einem Angreifer, die Daten aus dem Datenraum der Anwendung auszuleiten, ist die Vertraulichkeit gebrochen, ohne dass die Verschlüsselung gebrochen wurde.

Je nachdem ob die sensiblen Daten die Zielkoordinaten, die in einem Navigationssystem eingegeben wurden, ein strategischer Plan auf einem Notebook oder die schützenswerten Privatadressen bestimmter Personen sind, entstehen andere Risiken – evtl. auch für Leib und Leben von Unbeteiligten.

Literaturhinweise

[1] Bitkom AG 2: „Digitale Souveränität im Cyberraum – wo ist Schlüsseltechnologie nötig?

[2] Bitkom AG 2: „Basis Schlüsseltechnologien als Voraussetzung für Digitale Souveränität“

[3] Vortrag Ramon Mörl auf 14. Deutschen IT-Sicherheitskongress des BSI 2015: „Bad USB, vergleichbare Exploits - sinnvolle Verteidigungsstrategien“ sowie

[4] Artikel von Ramon Mörl und Andreas Koke: „BadUSB, aktuelle USB Exploits und Schutzmechanismen“ (https://www.itwatch.de/content/download/1976/11986/file/BadUSB_aktuelle%20USB%20Exploits%20und%20Schutzmechanismen.pdf)

Herausgeber des kompletten Tagungsbandes, für den dieser Autorenbeitrag geschrieben wurde, ist das Bundesamt für Sicherheit in der Informationstechnik, Titel: „Cyber-Sicherheit ist Chefinnen- und Chefsache“, Tagungsband zum 18. Deutschen IT-Sicherheitskongress des BSI, SecuMedia-Verlag 2022. Sie können das Buch ab Ende Februar im Buchhandel und auf www.secumedia.shop erwerben, ISBN 978-3-922746-84-3.