Ivo Keller, Friedrich Holl

Kriterien: Wie Security auch für Safety verantwortlich wird

Safety-Inseln im Security-Komplex

Nahe Fukushima schien ein Atomkraftwerk seiner wesentlichsten Safety-Aufgabe nicht gerecht geworden zu sein: Durch die explodierenden Druckbehälter wurden Tausende strahlengeschädigt, die Umgebung ist für Jahrzehnte unbewohnbar geworden. Und wenn dies einem derartig hoch technologisierten Land schon nicht gelingt, dann scheint doch die Atomenergie grundsätzlich nicht beherrschbar sein, so die Begründung für Deutschlands Atomausstieg. – Es lag jedoch nicht an mangelhafter Safety. Stattdessen war die Bedrohungsmodellierung, also die Gestaltung der Security, unzureichend, denn hierbei wurden zwar abstürzende Flugzeuge mit erwogen, nicht jedoch derartig hohe Tsunamis.

1 Die heterogene Welt der Sicherheit

Im deutschen Sprachraum haben wir es eigentlich gut: wir kümmern uns um „Sicherheit" unabhängig davon, ob es sich um „Safety" oder „Security" handelt, wie „Sicherheit" international differenziert wird. Insofern sollte das Problem, das wir hier ansprechen, eigentlich gar nicht existieren. Aber, dies ist leider nicht der Fall, weil der Begriff der Sicherheit traditionell fast immer eher technisch geprägt ist und der Schutz insbesondere von Personen vor dem Fehlverhalten von Produkten oder Systemen traditionell eher der Safety zuzuordnen ist.

Dr. Ivo Keller

TH Brandenburg, Prof., Studiendekan Security Management, Datenschutzbeauftragter; Arbeitsgebiete: Machine Learning, Process Mining, Fraud Detection, Secure Software Engineering
E-Mail: Ivo.keller@th-brandenburg.de

Prof. Dr. Friedrich-L. Holl

Instititute for Safety and Security an der TH-Brandenburg, akkreditierter Datenschutzgutachter (EuroPriSe), Datenschutzbeauftragter. Arbeitsgebiete: Datenschutz, IT-Security, Informations- und Unternehmenssicherheit, Secure Software Engineering, Beratung und Schulung.
E-Mail: holl@th-brandenburg.de

Diese Safety zählt zu den ältesten adressierten Bedürfnissen der Menschheit; Verstöße dagegen wurden schwer geahndet. Bereits im Babylon Hammurapis wurden die Erbauer von später eingestürzten Häusern mit dem Tode bestraft [1]. Auch die Maslow'sche Bedürfnispyramide fußt u.a. auf Safety.

1.1 Safety

Bei **Safety** geht es vor allem darum, Systeme aus funktionaler Sicht so sicher zu machen, dass sie die Umgebung (Mensch, Umwelt, andere investive Anlagen usw.) nicht schädigen. Dabei wird grundsätzlich davon ausgegangen, dass es sich um geschlossene Systeme handelt und dass das „sichere System" in sich funktioniert und nichts und niemanden schädigt, selbst bei fahrlässigem Gebrauch [2].

Durch die Digitale Transformation, die konfektionierte und virtuelle Produkte als nächstes Wachstumsventil ausgemacht hat, erhielt Safety erneut politischen Rückenwind. Die Unversehrtheit der Person und ihr physisches Wohlbefinden stehen sakrosankt über den ökonomischen Voraussetzungen und müssen besondere Berücksichtigung finden. Grundsätzlich können Safety-Gefährdungen allerdings nur aus einem schlechten Design resultieren [1] und lassen sich somit *systematisch* und durch Sorgfalt *vermeiden*. Insofern treten Safety-Gefahren (bei ausreichender Sorgfalt) höchstens zufällig auf, außerhalb des Vorbeugungshorizonts.

Dabei haben sich im Zeitalter einer IT, auf der praktisch alles basiert und die fast allumfassend genutzt wird, die wesentlichen Schutzziele, an denen sich Safety messen lassen muss, auf *Vertraulichkeit* (*Confidentiality*), *Integrität* (*Integrity*) und *Verfügbarkeit* (*Availability*), *CIA*, verdichtet. Produkt- und einsatzspezifisch kommen dann noch weitere Schutzziele hinzu (Verhindern von Fehlern, Gesundheit schädigen, Einhalten von Lebenszyklen, usw.).

Im Laufe der Zeit haben sich sowohl im Safety-, als auch im Securitybereich Sicherheitsanforderungen manifestiert, die ausgehend von den sog. Würzburger Normen, bzw. der Dampfkesselverordnung, bereits in der Mitte des 19. Jh. mit Vorgaben zur Sicherheit (Safety) auf die stark gestiegene Anzahl von Unfällen (1877-1890 mehr als 200 Dampfkesselexplosionen mit mehreren hundert Toten) reagieren mussten [3].

Die ersten Sicherheitsregeln, die offiziell vor bzw. beim Betrieb einer technischen Einrichtung berücksichtigt werden mussten, sind damit Produkt- und Betriebssicherheit.

1.1.1 Produkt-/Betriebssicherheit

Produktsicherheit beginnt heute bei der Herstellung (CE-Zeichen) und endet in der Betriebssicherheit. Hierbei reduziert sich der Analysehorizont noch stark auf die isolierte Betrachtung. Das Produkt wird in funktionale Teile zerlegt, innerhalb derer auf kognitive, empirische oder heuristische Weise den möglichen Fehlern auf den Grund gegangen wird. Gehandelt werden muss erst, wenn sich gegenüber den Schnittstellen potenziell negative Folgen zeigen, die durch entsprechende Maßnahmen beseitigt werden können.

1.1.2 Software-Sicherheit

Auf die Schutzziele der Safety hat auch die Produktion von IT hinzuwirken. Die Entwicklung sicherer Software erstreckt sich dabei von den funktionalen Anforderungen des Endkunden über die Integration fremdhergestellter Bibliotheken bis hin zum Einsatzszenario mit seinen Bedrohungsszenarien – was die Herstellerverantwortung über den gesamten sog. „Software Development Lifecycle (SDL)“ umschließt.

Grundsätzlich ist **Software-Sicherheit** ein Qualitätsmerkmal und unterliegt wie die Nutz-Funktionalität einer sich ständig verändernden Umgebung und der daraus hervorgehenden Bedrohung. Und je komplexer diese Bedrohung später zu erwarten ist, desto stärker muss die Software bereits während der Herstellung auf Security-Bedrohungen eingerichtet und gehärtet werden.

1.1.3 IT-Sicherheit

IT-Sicherheit greift in der Intention der Safety die Betreiberseite des SDL auf. Hier überwacht sie zunächst die sichere Ausführung der Wartungsprozesse. Dies umfasst allerdings die gesamte Produktkette und erfordert daher seitens der Hersteller eine grundsätzliche Vertrauenswürdigkeit im Security-Sinne und schließt zumeist auch ein gemeinsames, gut abgestimmtes Change Management [4] mit dem Endanwender ein.

Da hier zusätzlich auch die gesamte Einsatzumgebung von IT durchdrungen ist, überstreicht der Verantwortungsbereich das gesamte „System“ von Kernel-Programmen und Nutzer-Software über loyale Administratoren und das Reinigungspersonal bis hin zur Energieversorgung und dem Zaun.

1.1.4 Persönlichkeits-/Datenschutz

Der Schutz der **Persönlichkeit** und der Privatheit (Privacy) mit seinem Grundsatz „let to be alone“ steht insbesondere in der amerikanischen Rechtsprechung als wesentliches Schutzrecht Einzelner im Vordergrund [5].

Allerdings ist dieses Kant’sche Ideal einer von der Außenwelt abgeschirmten Privatsphäre als Quelle der Selbstverantwortung und der selbstbestimmten Lebensgestaltung in seiner Safety-Reinform in der vernetzten Gesellschaft nicht mehr zu halten: Die Menschen interagieren, ein Online-Händler muss die Lieferadresse erfahren dürfen, die Kunden bewegen sich in virtuellen Erlebniswelten – die auf Safety vertrauende Persönlichkeit hat sich einer vernetzten Umgebung geöffnet. Dabei entstehen Risiken für den Einzelnen, die die verschiedensten Ursachen haben und nicht mehr durch die funktionale Sicherheit (Safety) des Systems abgemildert werden können. Insbesondere in digitalen Systemen sind Risiken entstanden, die vor allem auf die Umgebungsparameter zurückzuführen sind. Damit müssen diese digitalen Systeme unbedingt nach Security-Erfordernissen gestaltet und betrieben werden.

Da die hier herrschende Wettbewerbskultur die Persönlichkeit nicht nur als Vertriebsziel, sondern auch als Ressource entdeckt hat, eröffnen sich durch die psychometrische Vermessung der Beteiligten nie gesehene Verwertungs- und Manipulationsmöglichkeiten. Totalitäre Gesellschaftssysteme scheinen durch IT, die ihrerseits einen immanenten Monopolcharakter besitzt, einen „eingebauten Vorteil“ zu besitzen [6]. Dieser „Vorteil“ geht aber vor allem auch deswegen zu Lasten der Betroffenen, weil die Funktionalität des Systems zum Alleinmaßstab gemacht wurde. Fehler in solchen Systemen hatten in der Vergangenheit folgerichtig regelmäßig zu „Kollateralschäden“ mit Millionen von Opfern geführt.

Der Datenschutz als wichtige „Waffe“ des Persönlichkeitsschutzes sieht dagegen die Sicherung der Privatheit als Voraussetzung für Masseninnovation und stellt sich deswegen dem „Kampf gegen die übermächtige Maschine“.

1.2 Security

Security geht über den Safety-Ansatz hinaus und versucht insbesondere die negativen Wirkungen beispielsweise von An- und Eingriffen auf das jeweilige (Teil-)System abzumildern. Bei dem zu schützenden System handelt es sich dann nicht mehr um ein geschlossenes, sondern um ein offenes System, das mit seiner Umgebung interagiert und gegen die daraus hervorgehenden Bedrohungen abgesichert werden muss. Insofern steht nicht mehr die reine Sicherung der *Verfügbarkeit* (*Availability*) im Vordergrund, sondern vielmehr die Zuverlässigkeit einer dauerhaften Funktion (auch unter bestimmten Angriffsbedingungen) bzw. der Verlässlichkeit bezüglich der Wahrung von *Vertraulichkeit* oder der Wahrung der Eigentumsrechte – letztendlich soll Security die Vorgaben entwickeln und die Regelung bereitstellen, die die Entwicklung und den Betrieb sicherer Systeme für eine sichere Gesellschaft ermöglichen [2].

Dies erweist sich allerdings bei jeder der digitalisierten Hochrisikotechnologien, wo weder alle Security- noch alle Safety-Aspekte berücksichtigt werden können, als nicht leicht umzusetzen. Nur das, was man vorhersagen kann, kann auch geschützt werden. Bei digitalen Systemen, die im Wesentlichen auf der Nutzung von Software basieren, kann bisher nicht einmal eine absolut sichere Funktionsfähigkeit garantiert werden. Bisher gibt es, zumindest für komplexere Systeme, keine in der Praxis nutzbare Methode, mit der die Abwesenheit von Fehlern und Fehlfunktionen zugesichert werden kann. Bisher kann man nur feststel-

len, dass Fehler existieren, und nicht, dass im System keine Fehler vorhanden sind. Zusammen mit der nicht vollständigen Vorhersagbarkeit aller unter Security-Gesichtspunkten zu berücksichtigenden relevanten Parameter führt das dazu, dass digitale Systeme nicht wirklich sicher designet, produziert und betrieben werden können.

Zudem werden Security-Maßnahmen wegen ihrer breiteren, auch ökonomisch motivierten Schutzziele meist „nur" effizienzmotiviert und kompromissorientiert umgesetzt. Dies öffnet die Tür insbesondere für Angriffe auf digitale Systeme. Schützen kann man sich nur gegen erwartbare Angriffe und auch dort meist nur gegen die unter „normalen" Bedingungen erwartbaren.

Dies ist umso problematischer, als derartige „Black-Swan"-Effekte, die durch Seltenheit, extreme Auswirkungen und nicht-prospektive Vorhersagbarkeit gekennzeichnet sind, zunehmen. Es ist demnach anzunehmen, dass sich zukünftig zusätzliche Angriffsvektoren und Bedrohungen ergeben werden. Außerdem sind digitale Systeme gegen neue Angriffsvektoren wohl anfälliger als traditionelle analoge.

1.2.1 Unternehmens-/Organisationssicherheit

Die beiden Bereiche Unternehmens- und Organisationssicherheit beschreiben im wesentlichen dieselbe Problematik aus unterschiedlichen Blickrichtungen heraus. Unternehmenssicherheit ist der umfassendere Ansatz; Organisationssicherheit beinhaltet den Schutz einer unternehmerischen Struktur vor Innentätern, Kompromittierung usw.

1.2.2 Informationssicherheit

Informationssicherheit widmet sich dem Schutz der Unternehmensdaten vor Spionage und Zerstörung. Ein wichtiges Element der Informationssicherheit beinhaltet den (gesetzlich erzwungenen) Schutz der personenbezogenen Daten, geht aber letztendlich weit darüber hinaus. Denn alle Daten (Informationen) innerhalb eines Unternehmens müssen in ihrer Gesamtheit geschützt werden – natürlich angepasst an die jeweils notwendigen und ggf. unterschiedlichen Sicherheitsanforderungen, -stufen und konzepte. Informationssicherheit ist gleichzeitig ein Teil der Unternehmens- bzw. Organisationssicherheit und basiert technisch gesehen zu großen Teilen auf der IT-Sicherheit.

1.2.3 Cyber-Sicherheit

Cyber-Sicherheit meint „grenzenlose Informations-Sicherheit", wird aber durch die unterschiedlichen Interessen der am Cyberraum beteiligten Parteien konterkariert. Forciert werden diese Bedrohungen durch einen interkooperativen Wettbewerb mit den Mitteln zur Verletzung der Informationssicherheit. So werden Systemlücken in der IT bewusst offengehalten, um permanent strategische oder technologische Daten abzuziehen und dadurch die wirtschaftliche oder geopolitische Auseinandersetzung dominieren zu können. Geheimdienste, die diese Lücken im nationalen Interesse offenhalten, gefährden andererseits ihre jeweilige Wirtschaft durch das Offenhalten der Systeme für (Dritt)Hacker.

In einem sog. „Hybriden Krieg" gar erübrigt sich selbst die physische Kriegsführung, so die weit verbreitete Vorstellung, wenn es gelingt, die anzugreifende Bevölkerung durch großflächige Sabotage der Infrastruktur gefügig zu machen.

1.2.4 Infrastruktursicherheit: Banken und KRITIS

Die Aufrechterhaltung der eigenen Infrastruktur ist nicht nur eine Fürsorgepflicht, sondern auch die Voraussetzung für das Funktionieren eines Staates und die unternehmerische und staatliche Entscheidungsfreiheit. Die am weitesten ausgereiften Regularien zur Absicherung der Funktionsfähigkeit finden sich daher in denen zur Bankensicherheit und in den Rundfunkverträgen sowie seit einigen Jahren auch bei den sog. „Kritischen Infrastrukturen (KRITIS)".

Diese Regularien sorgen auf eine sehr formale Weise für eine Grundsicherung, was weitergehende angepasste Maßnahmen durchaus nicht ausschließt. Da aber die Haftungsfreistellung bereits mit der Grundabsicherung erreicht wird, bleiben umfassendere Risikobetrachtungen oft aus.

Derartiges zeigte sich vor kurzem in Berlin bei einem relativ großflächigen Stromausfall, bei dem über 30.000 Haushalte über 30 h ohne Strom waren. Als eine der ersten Kritischen Infrastrukturen fielen die Telekommunikationseinrichtungen aus – ungepufferte Festnetzsysteme sofort, aber auch die batteriebetriebenen Mobilfunkeinrichtungen. Es zeigte sich, dass nur ganz wenige Basisstationen der Mobilfunkbetreiber überhaupt eine längerfristige Absicherung besitzen (mehr als 4 h) und dass eine grundsätzlich länger funktionsfähige Infrastruktur recht schnell nicht mehr verfügbar war.

2 Sicherheitsprinzipien

Im Sinne einer Leitethik bedienen sich sowohl Safety, als auch Security jeweils anerkannter Sicherheitsprinzipien. Diese simplifizieren die grundsätzlichen Wesenszüge von Gefahren und Bedrohungen und geben Handlungsempfehlungen. Besonders in den durch Effizienz- und Kostendruck motivierten Bereichen sind sie das Handwerkszeug, durch das die Verwundbarkeit bereits an der Quelle verringert werden soll, während sie in den stärker regulierten Sicherheitsfeldern das haftungstechnisch erforderliche Mindestmaß gewährleisten sollen.

2.1 Safety

Die Safety kodifiziert ihre fehlerbezogene Sicht beispielsweise durch die nachfolgenden Prinzipien (vgl. [1]):

- Jedes System enthält potentielle Safety-Schwachstellen (man muss sie suchen).
- Safety-Schwachstellen werden durch Gefährdung und Risiko beschrieben (lassen sich quantifizieren).
- Eine Gefährdungsquelle führt zu vielen speziellen Gefährdungen (das Übel bei der Wurzel packen).
- Gefährdungen können nicht vollständig beseitigt werden.
- Eine beabsichtigte Funktionalität kann unbeabsichtigt einsetzen.
- System-Gefährdungen sind menschengemacht (fehlerhaft).

Die Auflistung beginnt mit einer Safety-typischen Fokussierung und endet mit einer Reflexion der systemischen Umgebung.

2.1.1 Persönlichkeits-/Datenschutz

Die Rahmenbedingungen, die für einen effektiven Datenschutz stehen, orientieren sich angesichts eines als übergriffig empfun-

denen Staates [7] und der persönlichkeitsbedrohenden Data-Mining-Giganten an nachfolgenden Prinzipien. Die Auflistung führt dabei von der Fehler- über eine Werte- zur Angreiferbetrachtung:

- Ohne Zulässigkeit keine Verarbeitung (Gefährdung verringern),
- Datenverarbeitung auf gesetzlicher Grundlage (Interessensvertreter Staat),
- Zweckbindung und Transparenz,
- Sparsamkeit und Löschungsgebot (Gefährdung verringern),
- Persönlichkeit achten (Selbstbestimmung),
- Direkterhebung (auf Augenhöhe mit dem übermächtigen System),
- Informationelle Gewaltenteilung (Defense-in-Depth),
- Fremdkontrolle (bestätigte Vertrauenswürdigkeit).

2.2 Security

2.2.1 Software-Sicherheit

In der Sicheren Software-Entwicklung geben die sog. „Security (Design) Principles" (vgl. [6]) den Programmieren Grundsätze an die Hand, die bei der Klarheit in der Fehlerbeseitigung beginnen und in einer Verteidigungssicht münden:

- Sichere Standardeinstellungen,
- No Security by Obscurity,
- Aufgabentrennung,
- Sicherheit einfach halten.
- Sicherheitsprobleme korrekt beheben (dazu testen, um das Problem zu verstehen).
- Minimiere die Angriffsfläche.
- Verteidigung in der Tiefe (Defense-in-Depth).
- Niedrigste Rechte (für den Betrieb).
- Misstraue den Diensten.
- (Angreifer) sicher scheitern lassen.

Natürlich führt die Einhaltung der Prinzipien der Sicheren Software-Entwicklung nicht dazu, dass IT-Systeme hundertprozentig sicher sind. Allerdings zeigte sich bisher, dass bei Missachtung dieser Prinzipien eine überaus große Angreifbarkeit des technischen Systems folgt, auf dessen permanente Funktionsfähigkeit wir uns immer verlassen.

3 Sicherheitskonzepte

Wie bereits die gewählte Rangordnung erkennen ließ, liegen den Sicherheitsprinzipien elementare Grundkonzepte zugrunde, in denen sich deren Intention der Prinzipien bündeln lässt.

3.1 Sicherheitskonzept Zone

Das Zonenkonzept, mehrere Objekte gleichen Schutzbedarfs zusammenzufassen, hat seinen Ursprung in der Reduktion der Komplexität. Nur im überschaubaren Bereich konnte Verantwortung übernommen werden, hier konnten die Fehler eingegrenzt werden und die jeweils spezialisierte Safety weiterhin gewährleistet werden.

Nachdem vernetzte Systeme wirtschaftlicher wurden, mussten (Security) Gateways eingeführt werden, um die Angriffsvektoren zumindest beim Bereichsübertritt herausziehen zu können.

Das Zonenkonzept mit der intendierten reduzierten Komplexität kommt wiederum der Security zugute – es mindert das grundsätzliche Bedrohungsrisiko, indem Bedrohungen spezialisiert, modelliert, zusammengefasst und gegebenenfalls idealtypisch dargestellt werden können und somit einfacher zu handhaben und letztendlich wirksamer sind. Es gestattet außerdem die Entwicklung von Gefährdungsclustern, mit deren Hilfe Systeme dann besser und wirtschaftlicher geschützt werden können. Das Zonenkonzept bleibt daher die unverzichtbare Basis zur Sicherung komplexer Systeme.

Da jedoch, wie bereits jetzt in Rechenzentren beobachtet werden kann, eine allzu große Vielfalt an interagierenden Zonen ebenfalls nicht mehr zu harmonisieren ist, erfolgen gegenwärtig erhebliche Anstrengungen zur Normierung des Außencharakters der Zonen. Dies setzt allerdings eine Security-Taxonomie (vgl. [9]) voraus.

3.2 Defense-in-Depth

Das Konzept der Zone wird erweitert durch **Defense-in-Depth** [10], in der Luftfahrt auch bekannt als „Schweizer-Käse-Modell": Die „Verteidigung in der Tiefe" adressiert, dass ein und derselbe Angriffsvektor zwar eine Verteidigungslinie durchbrechen darf, nicht aber noch eine weitere, und keinesfalls die der absoluten, unbedingt zu schützenden „letzten" Schutzzone.

Es wird üblicherweise bei besonders zu schützenden Systemen, beispielsweise auch bei Kernkraftwerken, angewandt. Neben der Aufteilung in Zonen (Reduzierung der Komplexität) und der Zuordnung der Systemteile zu den jeweiligen Zonen gleichen Schutzbedarfs soll durch Defense-in-Depth erreicht werden, dass ein Angriff so kanalisiert ablaufen muss, dass sein Angriffsvektor während des Angriffs nicht verändert und somit besser bekämpft werden kann.

Die Schutz-Software sollte hierbei außerdem auf unterschiedlicher physischer Hardware laufen, damit, um auf die Käse-Analogie zurückzukommen, sich „auch Schimmel nicht von einer Scheibe zur nächsten ausbreiten" kann.

Darüber hinaus ist zu verhindern, dass ein Brückenkopf installiert wird, von dem aus die nächste Angriffswelle ausgelöst werden kann. Da Angreifer üblicherweise nur über begrenzte Zeit und „Feuerkraft" verfügen, sollten sie, wenn sie einmal eingedrungen sind, dort möglichst lange aufgehalten werden, um aufgespürt werden zu können und möglichst viel von ihren Ressourcen zu verlieren.

Analysetechnisch kann einer solchen Bedrohung nur durch die Security-Sichtweise begegnet werden, denn diese kann relevante Angriffspfade erkennen und dann ggf. auch mehrfach sichern.

3.2 Sicherheitskonzept Redundanz

Redundanz ist ein Grundprinzip, mit dem der Betrieb eines Systems aufrechterhalten werden kann, wenn ein Teilsystem ausfallen sollte. Die kritischen Systemkomponenten bei Flugzeugen werden häufig mehrfach redundant ausgestattet, also jeweils mit mehreren gleichartigen, unabhängig voneinander funktionierenden Komponenten. Besondere Sicherheitsanforderungen erfordern noch weitere Redundanz. Über Redundanz werden Daten, aber auch Prozesse gesichert.

Besondere Sorgfalt muss jedoch auf die Zusammenführung der Daten gelegt werden: So wird eine Mehrheitsentscheidung

nur dann sinnvoll, wenn sie auf einer unterschiedlichen Grundlage fußt. So bleibt die Geschwindigkeitsbestimmung im Flugzeug auch dann fehlerhaft, wenn die beiden Stauröhrchen eingefroren sind, während sich das einzige GPS den Ergebnissen der anderen Geräte unterordnen muss.

Ebenso ist die Zusammenführung von Prozessdaten fehlerträchtig, wenn deren Aktualität, vielmehr noch ihre Integrität, nicht erkennbar ist. So beruhen Angriffe auf das Backup häufig darauf, dass Dateien unlesbar gemacht wurden. Anschließend fressen sie sich, weil sie ja die aktuellsten und damit „richtigen" sind, durchs Backup. Bisher behilft man sich dagegen durch das **Defense-in-Depth-Konzept**, indem man die Backups zeitlich staffelt – noch wirksamer wäre allerdings eine semantische Plausibilitätsprüfung, zumindest vor dem ersten Backup.

Eine unsachgemäß umgesetzte Redundanz schafft also sogar zusätzliche Gefahren, indem sie weitere versteckte Angriffsvektoren entstehen lässt. Derartige versteckte Fehler lassen sich nur entdecken, wenn die Safety-Analyse auf einer mehrstufigen Simulation beruht; sie gehen dann aber leicht in der Menge der False Positives, den Fehlalarmen, unter.

Etwas vorteilhafter ist hier die Security-Betrachtung, da sie zumindest die Kritikalität dieser Pfade erkennt und so die Safety-Ressourcen hierauf lenken kann.

4 Umsetzungskonzept Risikoanalyse

„Sicherheit" wird nun nicht allein mit Hilfe von Prinzipien und Konzepten gewährleistet, Sicherheit muss messbar werden. Hierfür eignen u.a. baumbasierte Analyseverfahren. In solchen Analysebäumen wird entlang der einzelnen Äste das Risiko ermittelt und anschließend bewertet. Die Äste mit dem höchsten Risiko rechtfertigen schließlich die dringlichsten Maßnahmen (vgl. [11], [12]).

In ihrem Bestreben, die Schutzziele *CIA* zugunsten ihres zu bewahrenden Objekts durchzusetzen, fokussiert sich die **Safety** auf die **Fehlersuche**. Dies ist für Insellösungen sinnvoll, da hier die Anzahl der möglichen Fehler überschaubar bleibt.

Dabei verwendet sie sowohl rein qualitative Analysen, wie die Fishbone-Methode, als auch die quantitative Risikoabschätzung nach der *Fehlermöglichkeits- und Einflussanalyse* (*Failure Modes and Effects Analysis, FMEA*). Hier werden für ein *Bezugssystem* die *Fehlerquellen*, wie beispielsweise der unbefugte Zugang an der Einlasskontrolle eines Gerichtsgebäudes, hinsichtlich ihrer *Fehlerfolgen* und anschließend hinsichtlich ihrer *Fehlerursachen* (*Schwachstellen*) analysiert: Aggressive Angehörige können den Mitarbeitern gefährlich werden, und die Schwachstelle wird verursacht durch die Vergabe der Sicherheitsdienstleistung hauptsächlich nach Kostengesichtspunkten, wodurch unterqualifiziertes Wachpersonal beschäftigt wurde.

In der anschließenden Risikobewertung werden die (hier hohe) *Auftrittswahrscheinlichkeit*, die (sehr geringe) *Entdeckungswahrscheinlichkeit,* dass dies auffliegt, der (immateriell hohe) *Schweregrad* der psychischen Belastung der Gerichts-Mitarbeiter und die (hier gar nicht so hohen) *Fehlerkosten* mittels einer Skala bewertet und zusammengeführt. Dies entspricht dem Entlangwandern entlang eines Astes im Fehlerbaum von der Fehlerquelle bis hinunter zu den Fehlerkosten. Jeder dieser Pfade wird dadurch hinsichtlich seiner mittleren *Bedeutung* (*Impact*) bewertet und priorisiert; aus betriebswirtschaftlicher Sicht werden die Fehler nach *Effektivitäts-* und *Effizienzkriterien* behoben.

Diese Fehlerbäume können auch einen recht ausschließlichen Charakter besitzen. Je nach Bewertung am Entscheidungspunkt wird dann exklusiv und unumkehrbar verzweigt.

So hatte sich beispielsweise das **Datenschutz**-Altrecht noch sehr formal auf die Festlegung gestützt, unter welchen Umständen eine IP-Adresse denn nun als „personenbezogen" zu interpretieren sei. Von dieser Interpretation hing dann die Legitimität der nachfolgenden Argumentationskette ab.

Auch die reine Persönlichkeitsschutzbetrachtung der DSGVO ist nicht ganz frei von diesem Entscheidungszwang ohne Umkehr. So ist eine einmal getroffene Entscheidung, beispielsweise „Rechtsgrundlage oder Einwilligung?", im Nachhinein nicht mehr korrigierbar. Möchte man bei der Datenerhebung den erlaubten Rahmen geringfügig verlassen und entscheidet sich vorbeugend für die Einwilligung, so könnte diese jedoch kurz danach widerrufen werden. Wegen der ursprünglich getroffenen Entscheidung ist dann aber zumindest für diesen Datensatz die gesamte Verarbeitungsgrundlage entfallen [13]. Der einzuschlagende Pfad sollte daher an jedem der Verzweigungspunkt sorgfältig abgewogen werden. Dies erfordert oft sehr breite Kenntnisse hinsichtlich der Rechtsvoraussetzungen und –folgen; die Vorgehensweise der aktiv geschaffenen Pfade bedingt also einen erheblichen fachgestützten intellektuellen Aufwand. Dies mag als wenig operabel erscheinen, liegt aber in der Rechtsnatur begründet: Nicht die vermutete Schädigungsabsicht wird bewertet, sondern das formale Verletzen von vorher festgehaltenen Schutzregeln.

Die **Security**-Betrachtung dagegen möchte die *CIA*-Schutzziele für ein komplexes, vernetztes System durchsetzen. Da sie sich hier einer nahezu unermesslich vielgestaltigen und zumeist auch noch vorsätzlichen, systematischen Bedrohung gegenübersieht, fokussiert sie sich auf den **unmittelbaren Schutz der Werte**.

So beschreibt ein *Angriffsvektor* in der **Sicheren Software-Entwicklung** das Vorgehen eines *Angreifers* (Social Engineering, Malware, usw.) gegen eine *Schwachstelle* (*Vulnerability*) im System. Eine *Bedrohung* (*Threat*) ist die potentielle Gefahr, die durch diese Schwachstelle verursacht wird.

Bedrohung und *Schwachstelle* führen zur *Gefährdung;* Gefährdungen beziehen sich immer auf eine ganz bestimmte Situation und sind mit der *Wahrscheinlichkeit* behaftet, dass die Bedrohung (mittels des Angriffsvektors) die Schwachstelle trifft.

Diese Nomenklatur umschließt auch eine Safety-Zone innerhalb des Security-Netzwerkes: So ist, wenn das innerhalb der **Informationssicherheit** (in juristischer Abwägung) ermittelte **Datenschutzrisiko** zu hoch sein sollte, eine Datenschutz-Folgeanalyse erforderlich. Spätestens hier kommt dann wieder die gesamtsystemische Sicht der Security zum Tragen, indem die *technisch-organisatorischen Maßnahmen (TOM)* in die Risiko-Analyse mit einbezogen und hinsichtlich *Effektivität* und Zumutbarkeit (*verhältnismäßige Effizienz*) bewertet werden. Der rechtsgrundsätzliche Nachteil dieser Operabilität ist die Beweislastumkehr.

Im **KRITIS**-Bereich stützt sich das Risiko auf eine methodisch wohldefinierte Strukturanalyse; auch ist die anschließende Risikobewertung dann reguliert: Hier wird über den Katalog der *Elementar-Gefährdungen* klassifiziert.

Verfahrenstechnisch ähneln sich also die Risikoanalysen der quantitativen Safety und der Security. Je besser die wettbewerbliche Selbstregulierung wirkt, desto nachdrücklicher wird das Risiko hinsichtlich Effektivitäts- und Effizienzgesichtspunkten aus-

gelotet. Dagegen übernimmt der Staat zunehmend die Rolle des Interessenswahrers und reguliert, wenn die Persönlichkeit oder die infrastrukturelle Grundversorgung bedroht sind.

Allerdings unterscheiden sich Safety und Security hinsichtlich ihrer Blickrichtung:

- **Nach der Safety-Betrachtung sollen Mensch und Umwelt dadurch bestmöglich bewahrt werden, indem die Fehler des Systems reduziert werden. Stellschrauben sind die Fehler selbst, die Maßnahmen aus einem Safety-Risiko werden also fast ausschließlich gemäß der Bedeutung des Fehlers veranlasst.**
- **In der Security-Analyse geht man dagegen umgekehrt vor: Man *schützt das System* vor seiner Umgebung, indem man seinen *Kern analysiert*, denn das System soll nur Mittel zum Zweck bleiben. Stellschrauben sind dann die Werte selbst, die Angriffspfade oder die Systemschwachstellen („Fehler").**

Beide Sichtweisen möchten beispielsweise nun den Autofahrer schützen. Allerdings sind Analysekapazitäten der Safety auf ein „Fahrzeug als insulares System" beschränkt, während die Security die Vielzahl der eventuellen Interaktionen im Straßenverkehr dadurch ignorieren kann, indem sie prüft, welche Interaktion (Angreifer) das Leben des Fahrers (Kern) unmittelbar bedroht und was am Auto die gefährdende Schwachstelle wäre.

4.1 Bedrohungsmodellierung

Ein **Security-Risiko** wird folglich, begünstigt durch den Analysefokus auf den Kern, in der Schnittmenge zwischen *Unternehmenswert* (*Asset*), *Angreifer* und *Schwachstelle* [14] bestimmt. Je nachdem, woher man die größte Gefährdung vermutet, analysiert man also das System in Bezug auf die Unternehmenswerte, die Angreifer oder die Systemstruktur.

4.1.1 Wert-fokussiert

Nicht erst mit der Verabschiedung der DSGVO wurde für den **Datenschutz** die Rechtsgüterabwägung (Verhältnismäßigkeit) Grundprinzip: Der Schutzbedarf des Werts *Persönlichkeits-Autonomie* ist stets mit den geschäftlichen Erfordernissen abzugleichen und wird von der Legitimität des Geschäftszwecks beeinflusst.

In der **Security** werden generell *Unternehmenswerte* (*Assets*), also Geschäftsgeheimnisse, die Logistikkette oder der Kundenstamm, nach ihrem betriebswirtschaftlich-strategischen Potential beurteilt. Im einfachsten Fall kann das nach der ABC-Analyse [15] erfolgen, in der nur A-Elemente (Produktlinien, Kunden, usw.) berücksichtigt werden, die dem Paretoprinzip nahekommen, mit 20% des Gesamtaufwands zu 80% der Wertschöpfung beizutragen. Es kann aber auch differenzierterer analysiert werden, wie beispielsweise mit der BCG-Matrix [16], die den Produktlebenszyklus vor Marktwachstum und Marktanteil berücksichtigt.

In der **Unternehmens-/Organisationssicherheit** werden diejenigen Werte noch stärker betrachtet, die die *Unternehmensperspektiven* im generellen Sinne stützen, wohingegen die **Informationssicherheit**, und speziell die **IT-Sicherheit**, die *technologischen und strategischen Geschäftsgeheimnisse* schützen. *Kundendaten* werden meist als Data-Mining-Rohstoff betrachtet, die das Gros des Unternehmenswertes ausmachen, andererseits aber auch erhebliche **Datenschutz**-Risiken bergen können. Geschäftsgeheimnisse und Kundendaten bestimmen dann den insgesamt umzusetzenden *Schutzbedarf*.

Bei den Kritischen Infrastrukturen, **KRITIS**, gilt als zu erhaltender Wert die *Versorgungsicherheit* der Bevölkerung. Dieser Wert wird jedoch derartig hoch gewichtet, dass er Sicherungsmaßnahmen praktisch vordefiniert und relativ enge Grenzen für eine unternehmensbezogene Auslegung vorsieht. Da die Kritischen Infrastrukturen jedoch für das Überleben der Bevölkerung im Krisenfall besonders relevant sind, erscheinen diese Vorgaben akzeptabel. Zudem werden die Kosten für diese Aufwendungen weitgehend ausgeglichen.

- **In der Unternehmens*wert*-Betrachtung wird das Risiko aus dem *Schutzbedarf* abgeleitet.**

4.1.2 Angreifer-fokussiert

Häufig bedingen Unternehmenszweck und Angreifer einander. So werden die Internetauftritte von Urheberrechtsvertretern wohl zumeist durch jugendliche Script-Kiddies bedroht, während sich ein Bürgerrechtler-Forum eher auf geheimdienstliche Angreifer einrichten sollte. Es ist dann sinnvoll, diese Angreifer ähnlich wie die archetypische Persona des Usability Designs qualitativ zu inkarnieren.

In der **Sicheren Software-Entwicklung** quantifiziert man eine derartige Angreifer-Persona beispielsweise hinsichtlich ihrer (vgl. [17]):

- Fähigkeiten (technisch gering, Fortgeschrittener, Netzwerk- und Programmierkenntnisse, Penetrations-Tester),
- Motivation (gering, möglicherweise vergütet, hohes finanzielles Interesse),
- Gelegenheiten (Vollzugriff, spezielle Ressourcen, wenige Ressourcen, keine weiteren Tools benötigt),
- Anzahl (Entwickler und Administratoren, Intranet User, autorisierte Nutzer, anonyme Internet-Nutzer).

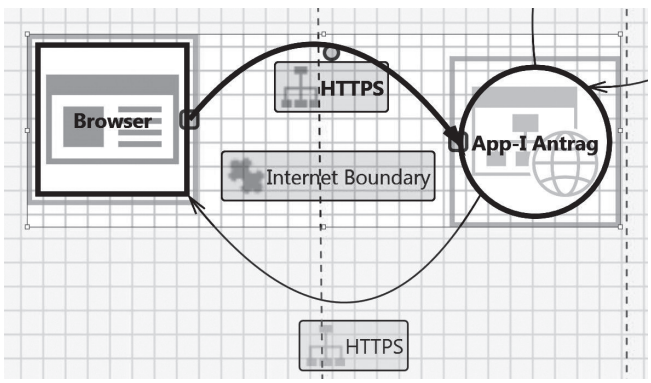
Die Auseinandersetzung mit der Frage, welcher potentielle Angreifer zu erwarten ist, wird auf jeden Fall erheblichen Einfluss auf die Einschätzung des jeweils nötigen Schutzbedarfs der Unternehmenswerte bzw. des Gesamtsystems haben.

- **In der *Angreifer*-Betrachtung wird das Risiko aus der *Angreiferanalyse* abgeleitet.**

4.1.3 System-fokussiert

In der **Software-Sicherheit** lassen sich Designfehler häufig bereits in einer grob skizzierten Systemarchitektur erkennen. Dabei hilft es, die funktionalen Kundenanforderungen mittels einer graphischen Modellierungssprache abzubilden (vgl. Abbildung 1).

Abbildung 1 | Beispiel einer Datenfluss-Skizze



Bereits auf dieser Abstraktionsstufe finden sich automatische (Safety-)Analysewerkzeuge, die, jeweils bezogen auf die Haupt-Schadenskategorien, die Design-Schwachstelle erläutern: „Der Gegner könnte Sicherheitsbarrieren umgehen oder sich als sein Opfern ausgeben und damit höhere Zugriffsrechte erlangen."

Wegen der nicht gerichteten und konzeptionell nicht ausreichend bewerteten Fehlersuche liefern derartige Tools jedoch oft eine Vielzahl von sog. False Positives, was die Fehlerbehebungskosten gerade bei größeren Projekten in die Höhe treibt.

Erst die Security-Sicht macht dann die Fehlerreduktion effizient: Meist reicht es ja aus, sich die Angreifer-Persona und ihre Begehrlichkeit (das Angriffsziel, den Wert) zu vergegenwärtigen, um auch die wahrscheinlichsten Angriffspfade zu erkennen. Diese *müssen* dann unbedingt *gesichert werden*, weitere Schwachstellen *in der Nähe der geringeren Werte* und den unwahrscheinlicheren Angriffspfaden *sollten*, andere *können* – stets gemäß den Security Design Principles – behoben werden.

Eine derartig schwerpunktgelenkte Bedrohungsmodellierung ermöglicht dann bereits einen sehr effizienten Sicherheitstest der Systemarchitektur, so dass man vom „Penetrationstest des Designs" sprechen könnte. Dies käme jedoch einer Herabsetzung gleich, denn diese erschöpfen sich noch an einer reinen Safety-gerechten Vorgehensweise.

In der **IT-Sicherheit** werden die laufenden Systeme regelmäßig Penetrationstests unterzogen. Hierbei wird in aller Regel nach nicht-registrierten Netzteilnehmern und (per Katalog) nach veralteter oder schlecht konfigurierter und damit unsicherer Software gefahndet. Und obwohl oft schon die Scanzeit sehr hoch ist, wird die anschließende Interpretation der False Positives noch weitaus aufwendiger und kostenintensiver. Zudem werden unbekannte Fehler hiermit (Safety-prinzipbedingt) nicht gefunden. Diese Tests bieten zwar keine echte Gründlichkeit, sondern vor allem mehr Bequemlichkeit, sind aber dennoch weit verbreitet. Sie weisen einen hohen Automatisierungsgrad auf und scheinen sich damit für die Implementierung effizienz- und sicherheitsfördernder Security-Maßnahmen zu eignen: Derartige „Fuzzy"-Penetrationstester implementieren die oben geschilderten Security-Betrachtungen der Software-Sicherheit, was dann zu einem echten Sicherheitsgewinn auch in der IT-Sicherheit führen würde.

Nicht ganz überraschend fußt auch die Infrastruktur-Sicherheit von **KRITIS** gemäß dem sog. IT-Grundschutz-Katalog zunächst auf einer lückenlosen Bestandsaufnahme. Von unten nach oben, vielmehr von innen nach außen, also beginnend mit der Maus am PC, wird die Fehlerfreiheit des jeweiligen Analyseradius' gegen den Katalog geprüft. Wenn sich dann darunter Produkte aus nicht-vertrauenswürdigen Quellen befinden, müssen diese entweder gekapselt werden, oder es dürfen sich keine zu schützenden Assets in Reichweite befinden. Dabei macht die Nutzung der Vorgehensweise nach der DIN EN ISO/IEC 27001 und die Umsetzung der Umsetzungsvorschläge aus der ISO 27002 auch eine effektivitätsgesteuerte Risikoanalyse zulässig. Dies führt zwar nicht zwingenderweise zu wirklicher Sicherheit, unterstützt jedoch bei qualitativ ausreichendem Einsatz den Weg „hin zu" sichereren IT-Systemen.

- **In der *System*-Betrachtung wird das Risiko aus der *Schwachstellenanalyse* und einem daraus resultierenden *Schutzbedarf* abgeleitet.**

4.2 Risikoanalyse

Nachdem nun also über die Bedrohungsmodellierung der Schutzbedarf bestimmt werden konnte, geht dieser in die finale Risikoanalyse ein. Aus der Risikoanalyse wiederum wird abgeleitet, welche Sicherheitsmaßnahme in welcher Reihenfolge umgesetzt werden sollte.

5 Zusammenführung

Auch wenn man „Safety" meist mit Produkten und „Security" mit vernetzten Systemen assoziiert, so sind sie doch primär nicht technologisch zu verorten, sondern unterscheiden sich hinsichtlich der Bedrohungsrichtung. Wird das Schutzobjekt bedroht, spricht man von Safety, wird das System angegriffen, handelt es sich um eine Herausforderung an die Security.

Da aber die Systemgrenzen fließen und eine Bedrohung des lebensbewahrenden Systems unmittelbare Auswirkungen auf das innerste Schutzobjekt hat, wird die formale Abgrenzung problematisch. So mag eine bewährte Inselbetrachtung weiterhin jeweils eine sehr schnelle Abschätzung einer bestimmten Gefährdung liefern. Da aber heutzutage buchstäblich jedes System, und sei es auch innerhalb einer Zone geclustert, zumindest über kontrollierte Zugangspfade mit seiner Umgebung interagiert, kann Sicherheit nur über eine Security-Analyse umgesetzt werden. Die formale Unterscheidung zwischen Safety und Security ist dabei eher hinderlich, vielmehr geht es um Risiko-Analysen, die der Komplexität gerecht werden.

Bedrohungen werden in beiden Gebieten mittels Fehlerbäumen, bzw. Angriffspfaden ermittelt.

Wegen ihrer überschaubaren Binnenverantwortung können **Safety-Fehlerbäume ihre Wurzel auf die Fehlerquelle**, beispielsweise eine Quellcodezeile, setzen. Von hier aus können dann die möglichen Fehlerfolgen erhoben oder simuliert werden. Wenn die Fehlerfolge dagegen erst im Test entdeckt wird, werden die Fehlerbäume von den Blättern her begonnen. Hat man dann die Fehlerursache geortet, kann wieder vorwärts simuliert werden, um noch weitere Verästelungen zu suchen. Das ist leistbar, wenn die Anzahl der Fehler begrenzt ist: In der Safety beginnt der Fehlerbaum „außen", im System, und beseitigt werden müssen die Blätter mit den am schwersten wiegenden Folgen für das „innenliegende" Schutzobjekt. Will man eine Analogie aus dem Schach bemühen, so wird hier jede einzelne gegnerische Figur hinsichtlich ihres Bedrohungspotentials analysiert.

Die **Security-Verteidigung** geht dagegen von einer nahezu unüberschaubaren Vielfalt von Außenbedrohungen aus und wählt den umgekehrten Weg: Sie **setzt die Wurzel ihres Bedrohungsbaumes auf die Werte**. Dies entspricht der Vorgehensweise von Personenschützern. Lassen sich dann aus einer Angreifer- oder Schwachstellenanalyse zusätzlich die Haupt-Verästelungen der Bedrohungspfade „nach draußen" erkennen, so wird auch hierfür Schutzbedarf gefordert; die Schutzmaßnahmen schließen dann primär diese Bedrohungspfade, denn alle „Angreifer"-Blätter können sowieso nicht beseitigt werden.

Die Security-Bäume sind also bereits per se schon dadurch effizienter, dass sie sich auf den Selbstschutz und nicht auf die Angreifersuche fokussieren, und durch die Bedrohungsmodellierung (hinsichtlich Werten, Angreifer-Personas oder System-Schwachstellen) wird diese Effektivität noch wesentlich gesteigert. In der

obigen Schach-Analogie würde man sich hier auf die unmittelbare Umgebung um den eigenen König herum konzentrieren, was erheblich geringerer Ressourcen bedarf.

Und dies führt nun zum entscheidenden Punkt: Beide Bäume sind mittels Simulationen durchfahrbar, aber da durch die Digitalisierung mittlerweile eine unüberschaubare Interaktionsvielfalt erreicht wurde, sind auch die Simulationsverfahren an ihre Kapazitätsgrenzen gekommen. So kann beispielsweise die Fehleranalyse mittels einer Statischen Code-Analyse einige Stunden benötigen, bis alle Fehlermöglichkeiten des Quellcodes durchsimuliert wurden. Dagegen ist es deutlich effizienter, wenn man lediglich vom Schutzobjekt auszugehen hat.

Um den Aufwand der manuellen Fehlerbehebung jedoch zu reduzieren, ist in kleineren Systemen auch der kombinierte Weg denkbar: Zunächst wird nach der Safety-Sicht von den möglichen Fehlerursachen (Quellcode) ausgegangen und alle Fehlerfolgen werden aufgelistet. Diese werden dann – aus Security-Sicht – auf ihre Relevanz hinsichtlich Werten, Angreifern oder System gefiltert.

Die Komplexitätsbetrachtung lässt erahnen, warum Safety gemeinhin mit einer traditionellen mechanischen Produktwelt assoziiert wird, in der ein gründlicher Geist allen Fehlern auf die Schliche kommt; jede Industriebranche pflegt ihre eigene Nomenklatur.

Security-Analysen dagegen betrachten höchstens drei Bedrohungsbäume und scheinen sich dadurch weitaus besser in eine automatisierte Prozessumgebung einzufügen. Security betrachtet ihren Ansatz als ganzheitlich und pflegt eine generische Nomenklatur, was sie auch leicht zugänglich für Process Mining und Künstliche Intelligenz macht.

Die Lösung liegt schließlich im Verantwortungshorizont:

- **Bei überschaubaren Fehlerquellen sind Safety-Analysen weitaus tiefgründiger und können dadurch auch die Restgefährdung sehr weit reduzieren. Für Inselsituation sind sie daher zu bevorzugen.**
- **Security-Betrachtungen dagegen sind selbst größter Komplexität gewachsen, allerdings sind sie das zulasten der Restbedrohung. Da aber, wo unter Effizienzerfordernissen agiert werden muss, akzeptiert man auch Effektivitätsnachteile.**

Wegen ihrer generischen Herangehensweise wird die Security-Sicht bereits heute auf Unternehmens-, Produktions- und IT-Prozessebene sowie in den Produkteinsatz-Szenarien angewendet. Sie ist auch zunehmend in der Lage, ohne Fachwissen in Safety-Domänen einzudringen, indem sie die kritischen Pfade von ihrem Schutzobjekt aus ermittelt – die dann natürlich nur mit profunder Fachkompetenz beseitigt werden können.

Dieses Marginalisieren der Safety legt aber auch eine zunehmende Verantwortung in den Schoß der Security, der sie, komplexitätsbedingt, nicht voll gerecht werden kann. Und während Security-Fehler bisher meist lediglich teuer waren, so kosten sie nun, statistisch zunehmend, mitunter auch Menschenleben.

In den (haftungsrelevanten) Kernbereichen wird und sollte man sich daher auch weiterhin zwingend auf solide Safety-Analysen verlassen können. Fukushima war zwar eine außerordentlich schwere Katastrophe, die Lehren daraus sind jedoch in erster Linie eine Aufforderung an die Adresse einer zukünftig hoffentlich erfolgreicheren Security.

Literatur

[1] Ericson, C. A.: System Safety Engineering, CreateSpace Inc., Charleston, NC, 2015

[2] Kompetenzzentrum Öffentliche IT (Hrsg.): S2: Safety und Security aus dem Blickwinkel der öffentlichen IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Berlin, 2015

[3] TÜV Nord Gruppe (Hrsg.): Die Geschichte der Technischen Überwachung in Norddeutschland. Books on Demand, Nordersted, 2003 S. 13 ff.

[4] von Faber, E., Behnsen, W.: Joint Security Management: organisationsübergreifend handeln. Mehr Sicherheit im Zeitalter von Cloud Computing, IT-Dienstleistungen und industrialisierter IT-Produktion, <kes>, Springer Vieweg, 2018

[5] Wittern, F.: Das Verhältnis von Right of Privacy und Persönlichkeitsrecht zur Freiheit der Massenmedien. E-Dissertationen der Universität Hamburg, 2004

[6] Gersemann, O., Rosenfeld, D., Zschäpitz, H.: Top-Ökonom warnt vor dem Ende von Marktwirtschaft und Demokratie, Welt, https://www.welt.de/wirtschaft/article187766858/Top-Oekonom-warnt-vor-dem-Ende-von-Marktwirtschaft-und-Demokratie.html, 27.1.2019

[7] Burkhardt, K.: Man muss sie zwingen, Spuren zu hinterlassen, Blog, 19. Nov. 2018, https://blog.mozilla.org/internetcitizen/de/2018/11/19/teil-1-man-muss-sie-zwingen-spuren-zu-hinterlassen/, letzter Zugriff 16.3.2019

[8] Security by Design Principles: https://www.owasp.org/index.php/Security_by_Design_Principles, letzter Zugriff am 16.3.2019

[9] von Faber, E., Behnsen, W.: Security ICT Service Provisioning for Cloud, Mobile and Beyond – ESARIS: The Answer to the Demand of industrialized IT Production Balancing Between Buyers and Provider, 2nd Ed., <kes>, Springer Vieweg, 2017

[10] Secupedia: Defense-in-Depth, https://www.secupedia.info/wiki/Defense-in-Depth, letzter Zugriff 24.3.2019

[11] Bundesministerium des Innern, für Bau und Heimat (Hrsg.): Organisationshandbuch, https://www.orghandbuch.de/OHB/DE/Organisationshandbuch/7_Management/72_Risikomanagement/risikomanagement-node.html, letzter Zugriff 16.3.2019

[12] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-4, Notfallmanagement, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1, letzter Zugriff 16.3.2019

[13] Haar, J.: Beschäftigtendatenschutz – ausgewählte technische und rechtliche Problemfelder im Lichte der EU-DSGVO, Masterarbeit im Studiengang Security Management, Technische Hochschule Brandenburg, 18.1. 2019

[14] Shostack, A.: threat modelling, designing for security, Wiley, 2014

[15] Dickie, H. F.: ABC Inventory Analysis Shoots for Dollars, not Pennies, in Factory Management and Maintenance, 6(1952) 109

[16] Baum, H.-G., Coenenberg, A. G., Günther, Th.: Strategisches Controlling, 5. Aufl., Schäffler Poeschel, 2013

[17] OWASP Risk Rating: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, letzter Zugriff 16.3.2019