Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

S²: SAFETY UND SECURITY AUS DEM BLICKWINKEL DER ÖFFENTLICHEN IT

Nadja Menz, Petra Hoepner, Jens Tiemann und Frank Koußen

Fraunhofer FOKUS

IMPRESSUM

Autoren:
Nadja Menz, Petra Hoepner, Jens Tiemann, Frank Koußen

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage April 2015

VORWORT

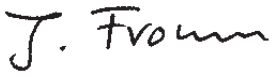
Der Roman »Blackout« von Marc Elsberg aus dem Jahr 2012 konfrontierte die breite Öffentlichkeit mit der Anfälligkeit einer vernetzten Gesellschaft nach dem Zusammenbruch der Stromnetze und führte so dem Leser die Verwundbarkeit von öffentlichen Infrastrukturen vor Augen. Gerade die Verletzbarkeit im Alltag, die Angreifbarkeit von unsichtbaren und sicher geglaubten Einrichtungen traf die Menschen im Roman unerwartet und regte damit die Leser zum Nachdenken an.

Fiktion wird zur Realität: Der öffentliche Raum wird zunehmend abhängiger von Informationstechnik. Obgleich Informationstechnik eine effiziente Erfassung und Steuerung von leistungsfähigen und hoch entwickelten Infrastrukturen erlaubt, beispielsweise von Verkehr oder der Versorgung mit Strom, führt die damit verbundene, fortschreitende Vernetzung gleichzeitig zu einer erhöhten Anfälligkeit unserer Gesellschaft. Die Vernetzung von vormals abgeschotteten Infrastrukturen stellt ein Anwendungsszenario dar, für das diese Systeme oftmals ursprünglich nicht konzipiert oder dessen Risiken nicht ausreichend analysiert wurden.

Der Begriff Sicherheit steht im Kontext von Infrastrukturen für den Schutz vor Angriffen von außen (Security), aber auch für das sichere Funktionieren (Safety) von immer komplexeren und voneinander abhängigen Strukturen, auf die wir im täglichen Leben inzwischen angewiesen sind. Durch die anhaltende Durchdringung unserer Gesellschaft mit Informationstechnologie (IT) verschwimmt nicht nur die Grenze zwischen Safety und Security zusehends, sie beeinflussen sich auch gegenseitig. Der erfolgreiche Angriff auf Industrieanlagen im Iran in 2013 (Stichwort Stuxnet) oder der Ende 2014 im Lagebericht des BSI publik gemachte gezielte Angriff auf ein Stahlwerk zeigte dies eindrucksvoll. Ein Angriff von außen – erst ermöglicht durch IT – betraf nun einen klassischen Safety-Aspekt, die sichere Funktionsfähigkeit von Teilen der Infrastruktur.

Diese Vorfälle allein zeigen bereits die Breite und Komplexität des Themas Sicherheit auf. Ebenso wird die Wechselwirkung zwischen Safety und Security deutlich. Für eine sichere Gesellschaft ist folglich ein detailliertes und integrierendes Verständnis der Sicherheitsanforderungen einer vernetzten, offenen und komplexen Welt unerlässlich.

Jens Fromm



Leiter Kompetenzzentrum Öffentliche IT

DANKSAGUNG

Das Kompetenzzentrum ÖFIT von Fraunhofer FOKUS dankt den folgenden Behörden für die hilfreichen Anregungen, Kommentare und Diskussionen: Bundesministerium des Innern (BMI), Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundespolizei.

Dieses Dokument gibt ausschließlich die Meinung der Autoren wieder und repräsentiert nicht notwendigerweise den Standpunkt der Kommentatoren.

UNTER ÖFFENTLICHER IT VERSTEHT MAN INFORMATIONSTECHNOLOGIEN, DIE IN EINEM ÖFFENTLICHEN RAUM DURCH DIE GESAMTGESELLSCHAFTLICHE RELEVANZ UNTER BESONDERER BERÜCKSICHTIGUNG DER STAATLICHEN VERANTWORTUNG STEHEN.

INHALTSVERZEICHNIS

1. EINLEITUNG UND THESEN

Informationstechnologie bezeichnet die Verarbeitung und Kommunikation von Informationen respektive Daten sowie die hierfür benötigte Soft- und Hardware. Der Schutz dieser IT-Systeme vor Fehlverhalten und Angriffen gewinnt in einer zunehmend digitalisierten und vernetzten Gesellschaft immer mehr an Bedeutung. Seit Sommer 2013 wird das Thema durch die Veröffentlichung des NSA-Materials durch Edward Snowden auch in der breiten Öffentlichkeit intensiv diskutiert.

Der Bedeutungszuwachs von IT hat jedoch nicht nur Auswirkungen im Bereich Datensicherheit. Dieses White Paper beschreibt, wie die Digitalisierung unserer Gesellschaft dazu führt, dass zwischen klassischen Security-Aspekten (wie bspw. Zugriffskontrolle und Verschlüsselung) und fast allen Bereichen des öffentlichen Lebens weitreichende Abhängigkeiten entstehen. Hierzu gehören Verkehr, Versorgung und Industrie – Bereiche, in denen umfassend vernetzte Systeme lange Zeit die Ausnahme waren. Der Fokus lag in diesen Bereichen auf dem Schutz gegen Fehlfunktionen der Systeme. Das Funktionieren dieser IT-gestützten, vernetzten Infrastrukturen gilt es als gesamtgesellschaftliche Herausforderung zu begreifen und zu gewährleisten.

Dieses White Paper beleuchtet die Thematik Safety und Security aus dem Blickwinkel der öffentlichen IT und zeigt die heutigen und zukünftigen Handlungsfelder und Forschungsfragen in diesem spannenden Themenbereich auf.

1. Ein Inseldenken im Bereich der Sicherheit übersieht Risiken.
Die fachspezifische Betrachtung einzelner Sicherheitsbereiche kann nur Risiken aus dem eigenen Erfahrungsbereich identifizieren. Die Komplexität heutiger Systeme verlangt aber nach einem multidisziplinären Ansatz, um Risiken in ihrer Gesamtheit zu betrachten und Gegenmaßnahmen zu ergreifen. Eine verstärkte Zusammenarbeit von Experten mit Domänenwissen und Sicherheitskenntnissen wird in Zukunft unerlässlich sein.

2. Informationstechnik übernimmt immer mehr Querschnittfunktionen.
Die zunehmende Vernetzung von Geräten im Internet der Dinge oder von industriellen Steuerungsanlagen sowie eingebetteten Systemen in Fahrzeugen verdeutlichen beispielhaft die Durchdringung unserer Infrastrukturen mit Informationstechnik. Informationstechnik kann einerseits zu einer sicheren Gesellschaft beitragen und Sicherheit verankern, andererseits aber auch als Einfallstor für neuartige Angriffe dienen.

3. Vernetzung erhöht die Komplexität.
3a. Systeme und Infrastrukturen werden durch Vernetzung sicherer.
Vielfältige und aktuelle Informationen erlauben bessere Entscheidungen, insbesondere im Zusammenhang mit informationstechnischen Systemen. Aufbereitete Informationen sind für Menschen einfacher und schneller zu erfassen und automatisierte Systeme entlasten Menschen von Routineaufgaben und verhindern menschliches Versagen.

3b. Systeme und Infrastrukturen werden durch Vernetzung unsicherer.
Vernetzt man zwei sichere Systeme, so entsteht nicht zwangsläufig ein sicheres Gesamtsystem. Sicherheitsmaßnahmen können auch entgegengesetzt wirken und sich aufheben oder Sicherheitslücken aus beiden Systemen können sich potenzieren. Neue Verfahren und Maßnahmen sind erforderlich, um auch den sicheren Verbund von Systemen und Geräten nachzuweisen.

4. Ein übergreifendes Sicherheitsmanagement gewinnt an Bedeutung.
Technik und Organisation müssen auf Basis von anerkannter Praxis und gesetzlichen Regeln ihren Teil zur Sicherheit von offenen, vernetzten Systemen beitragen. Es muss dauerhaft überprüfbar sein, wer bzw. was einen Anteil an der Gesamtsicherheit verantwortet und welche Veränderungen während der Lebenszeit eines Gesamtsystems weitere Sicherheitsmaßnahmen erfordern. Sicherheitsmanagement ist ein dynamischer Prozess, der immer auch den Menschen einbeziehen muss.

5. Resilienz und Autonomie statt periphere Sicherheit.
Die Abschottung von komplexen, vernetzten Systemen kann nur bedingt funktionieren. Statt auf eine vollständige, dauerhafte Abschottung als alleinige Sicherheitsmaßnahme zu vertrauen, gewinnen Funktionen zur Stärkung der Widerstandsfähigkeit an Bedeutung. Diagnose, Lernfähigkeit und korrektive Adaption an neue Gegebenheiten stärken die innere Abwehrkraft vernetzter Systeme.


Feuerlöscher
6 kg ABC-Pulver
27 A
183 B
C
1. Sicherungsstift herausziehen
2. Schlauch fassen
3. Taste niederdrücken
A
B
C
Vorsicht bei elektrischen Anlagen.
Nur bis 1000 V; Mindestabstand 1 m.
Nach jeder Betätigung neu füllen!
Löscher längstens alle 2 Jahre auf Einsatzbereitschaft überprüfen.
Nur solche Lösch-Treibmittel und Ersatzteile verwenden,
die mit dem anerkannten Muster übereinstimmen.
Löschmittel: 6 kg PL-9/89
Treibmittel: 15 bar Stickstoff
Funktionsbereich: – 20° C bis + 60° C
Nr. d. Anerkennung: SP 33/92 DIN EN 3
PD 6 GA
Typ:

2. SICHERHEIT: SAFETY UND SECURITY

Sicherheit bezeichnet einen von Risiken und Gefahren freien Zustand, der bezogen auf Menschen, Objekte oder Systeme verwendet wird. Um Sicherheit zu erreichen ist es erforderlich, ein vorhandenes Risiko zu vermeiden, zu reduzieren, zu transferieren oder auch zu akzeptieren. Aufgrund der heutigen technologischen Dynamik ist Sicherheit jedoch kein fixer Zustand, sondern erfordert eine kontinuierliche Überprüfung und Anpassung. Relevante Informationen müssen ständig aktualisiert, analysiert und adäquate Maßnahmen eingeleitet werden.

Bedrohungen für die Sicherheit können ausgehen von kriminellen Angriffen (z. B. mittels Schadsoftware, aber auch ganz klassisch in Form eines physischen Einbruchs), von organisatorischen Mängeln aber auch von technischen Unfällen oder höherer Gewalt. Schwachstellen in einem System können wiederum durch Design- oder Konstruktionsfehler, menschliches Fehlverhalten oder ungenügende Standortsicherheit entstehen. Eine Bedrohung oder eine Schwachstelle allein reichen jedoch nicht aus, um die Sicherheit eines Systems zu gefährden. Eine Gefährdung für das angegriffene System besteht nur dann, wenn eine Bedrohung auf eine existierende Schwachstelle trifft. [BSI]

Sicherheit von (IT-)Systemen ist als technische und organisatorische Aufgabe zu begreifen [IT-Grundschutz], bei der Mensch, Technik und Umgebung zusammenwirken müssen. Es reicht nicht, nur technische Mechanismen zur Abwehr von Gefahren vorzusehen, auch der Mensch als Nutzer dieser Systeme spielt eine wesentliche Rolle – er kann die Technik korrekt nutzen oder nahezu jede technische Lösung durch sein »kreatives« Handeln konterkarieren. In einer umfassenden Betrachtung von Sicherheit muss zudem die Umgebung des Systems berücksichtigt werden, da diese Anforderungen und Bedingungen für einen sicheren Betrieb vorgibt.

Die englische Sprache bietet mit den Begriffen Safety und Security eine Differenzierung der komplexen Thematik Sicherheit. Zur Abgrenzung der beiden Aspekte kann man den Fokus einerseits auf die Auswirkungen und andererseits auf die Gefahrenursachen setzen. Durch die dargestellten Abhängigkeiten unterscheiden sich die Auswirkungen immer weniger. Konzentriert man sich auf die Ursachen, dann bezeichnet Safety den Schutz gegen zufällige oder unvorhersehbare Einflüsse, Security dagegen den Schutz gegen vorsätzliche Angriffe. [Alexander] Folglich kann die Bedrohung eines (IT-)Systems durch z. B. Naturgewalten, falsche Betriebsart oder Integrationsfehler (Safety) abgewehrt werden, indem sie schon beim Entwurf und der Implementierung berücksichtigt werden. Bei gezielten, von Menschen gesteuerten Angriffen wie z. B. Sabotage oder Viren (Security), greift die Abwehr meistens jedoch nur für eine begrenzte Zeit, da sich bessere Angriffsmethoden und Schutzmaßnahmen im gegenseitigen Wettstreit miteinander befinden.

2.1 SAFETY

Ihren Ursprung hatte die Betrachtung der funktionalen Sicherheit (engl. Safety) bereits zu Zeiten rein mechanischer Systeme, die in geschlossenen Umgebungen (z. B. industrielle Steuerungssysteme) bzw. als geschlossene Einheiten (z. B. Fahrzeuge) operierten, ohne Verbindung nach außen. Durch die kontinuierlich zunehmende Vernetzung jeglicher Systeme mit Informationstechnik weicht diese Isolierung von der Außenwelt jedoch immer mehr auf.

Das Hauptziel von Safety ist der Schutz der Umgebung vor dem Fehlverhalten des Systems. Im Fokus steht die Unversehrtheit von Umwelt und Mensch.

»Safety – Das System soll die Umgebung nicht schädigen.«

Sichere Systeme müssen sich konform zu ihrer korrekten Spezifikation verhalten und eine hohe Zuverlässigkeit und Fehlersicherheit gewährleisten. Systematische Fehler müssen in der Entwicklung vermieden, das Auftreten von zufälligen Fehlern durch Überwachung im laufenden Betrieb erkannt und erkannte Fehler beherrschbar gemacht werden, indem der Übergang in einen als sicher definierten Zustand ermöglicht wird. Durch die Verknüpfung dieser physischen, vormals von der Umgebung abgeschotteten Systeme mit IT, entstehen jedoch neue Herausforderungen für Safety-Experten, um die Sicherheit dieser Systeme weiterhin gewährleisten zu können.

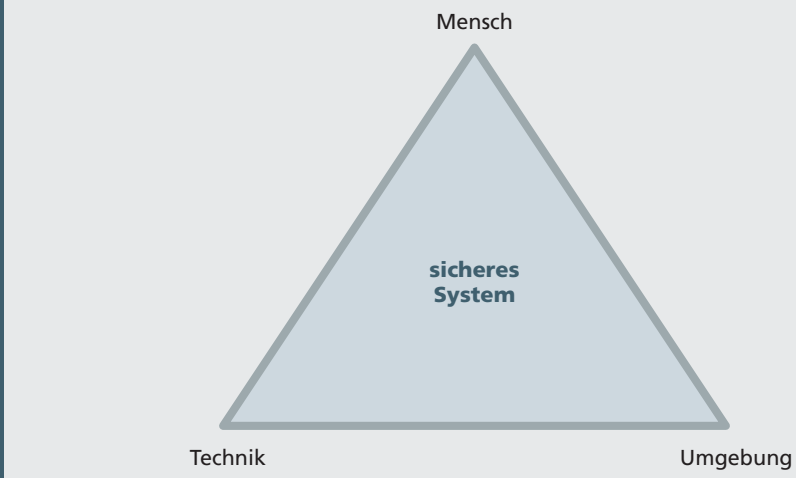


Abbildung 1: Zusammenwirken von Mensch, Technik und Umgebung für sichere Systeme

2.2 SECURITY

In der Informationstechnik stehen die technische Verarbeitung, Lagerung und Übertragung von Informationen im Vordergrund. Das Hauptziel von Security ist daher der Schutz der (IT-)Systeme und der gespeicherten Daten vor unerwünschten Einwirkungen aus deren Umgebung.

»Security – Die Umgebung soll das System nicht schädigen.«

Ebenfalls relevant sind Aspekte der Kommunikationstechnik, vornehmlich der sichere Austausch von Informationen. Für Behörden, Betriebe, Organisationen etc. stellt die Sicherheit von IT-Systemen eine ökonomische Größe dar, die es zu schützen gilt. Unzulässige Zugriffe und unzulässige Preisgabe von Informationen müssen verhindert werden, um wirtschaftliche und immaterielle Schäden zu vermeiden.

Durch die zunehmende Verwendung von informations- und kommunikationstechnischen Kernkomponenten in der deutschen Infrastruktur wird die Sicherheit dieser Teilkomponenten relevant für die öffentliche Sicherheit. Um ihre Sicherheit in adäquatem Maße gewährleisten zu können, müssen Sicherheitsanker so tief in ihren Design- und Entwicklungsprozess integriert werden, wie es in klassischen Safety-Bereichen wie der Automobilbranche seit Jahrzehnten bereits der Fall ist.

Im Deutschen wird Security im Kontext von Informationstechnik in der Regel mit IT- bzw. Informationssicherheit übersetzt. Neben der häufig synonymen Verwendung von IT- und Informationssicherheit umfasst Informationssicherheit jedoch auch von der IT losgelöste Facetten: So umspannt sie z. B. auch die Sicherheit von nicht elektronisch verarbeiteten Informationen. Das englische Wort Security bedeutet jedoch mehr als Informationssicherheit, denn es umfasst auch den Schutz von materiellen und immateriellen Werten z. B. physikalische Objekte wie Fahrzeuge. Dies könnte man am ehesten als Angriffssicherheit bezeichnen.

2.3 SAFETY UND SECURITY AM BEISPIEL LUFTVERKEHR

Die heutige noch übliche getrennte Betrachtung von Safety- und Security-Belangen lässt sich am Beispiel Luftverkehr dokumentieren. Die Sicherheit des Luftverkehrs ist eines der Schutzgüter, deren »Bewahrung zu den Kernaufgaben der Polizei sowie anderer Gefahrenabwehrbehörden zählt« [Borsdorff].

Air Safety, also die innere Sicherheit des Luftverkehrs, behandelt die Abwehr von betriebsinternen Gefahren für die Zivilluftfahrt. Ebenso befasst sie sich mit der Abwehr von Gefahren für die öffentliche Sicherheit oder die öffentliche Ordnung, die durch den Luftverkehr als solchen bedingt sind. Dem gegenüber steht Air Security, also die äußere Sicherheit des Luftverkehrs. Sie betrifft den Schutz vor solchen Gefahren, die von außen kommend auf den Luftverkehr einwirken, mit oder ohne Bezug zu Informationstechnik. Hierzu gehören u. a. die Entführung von Flugzeugen, Sabotageakte und terroristische Anschläge. [Borsdorff]

Beide Bereiche werden heute in verschiedenen Gesetzen (Luftsicherheitsgesetz bzw. Luftverkehrsgesetz) behandelt und entsprechend von verschiedenen Behörden begleitet. Die Gefahr, dass durch die Zuständigkeit verschiedener Behörden im Rahmen unterschiedlicher rechtlicher Grundlagen eine Grauzone entsteht, scheint nicht unbegründet und eine stärkere Verzahnung von Security und Safety daher auch in diesem Bereich wünschenswert. Ein mögliches Beispiel für diese Grauzone ist das Szenario eines Cyberangriffs von außen (Air Security) auf die elektronischen Systeme eines Luftfahrzeugs mit dem Ziel eine Turbine zu überhitzen (Air Safety).

3. SICHERE SYSTEME FÜR EINE SICHERE GESELLSCHAFT

In unserem Lebens- und Wirtschaftsraum vollzieht sich eine Veränderung in Richtung Informationstechnik. Ehemals rein mechanische, elektrische oder physische Systeme wie beispielsweise Kühlschränke, Herde, Heizungen und Fahrzeuge, aber auch unsere Stromversorgung und industrielle Steuerungsanlagen werden mit IT aufgewertet. Dies eröffnet allerdings neue Einfallstore für Kriminelle, welche Internet-Konnektivität, USB- und Funkschnittstellen oder Wartungs- und Diagnosezugänge für IT-Angriffe ausnutzen. Folgende Beispiele skizzieren den Zusammenhang von Safety und Security im Kontext öffentlicher IT:

3.1 VERKEHR

Versagende Bremsen, ein nicht mehr kontrollierbares Lenkrad oder eine inkorrekte Tachoanzeige; dieser Albtraum eines jeden Autofahrers wird von Tag zu Tag realistischer. Grund ist der technologische Fortschritt im Automotive-Bereich von geschlossenen hin zu komplexen, offeneren Systemen, die Schnittstellen zu anderen Systemen bereitstellen. Moderne Fahrzeuge integrieren dutzende elektronische Steuereinheiten in der Unterhaltungselektronik, Assistenzsystemen, schlüssellosen Einstiegssystemen oder Anti-Diebstahleinheiten, die auch unzählige neue Schnittstellen, sowohl fahrzeugintern als auch nach außen aufweisen. Welche Gefahren diese zunehmende Komplexität und deutlich vergrößerte Angriffsfläche mit sich bringen, zeigen die beiden folgenden Fälle: Eine Sicherheitslücke in einem verbauten Mobilfunkmodul zur Vernetzung von Fahrzeugen mit dem Automobilhersteller hätten Angreifer ausnutzen können, um die Türen der betroffenen Fahrzeuge zu öffnen. [BMW] Und bereits im Juli 2014 war es Studenten im Rahmen eines Sicherheitswettbewerbs gelungen, die Sicherheitsmechanismen eines Elektroautos zu überwinden. Der Angriff erlaubte es ihnen bei voller Fahrt per Funk die Türen und das Sonnendach zu öffnen sowie die Hupe und das Licht zu betätigen. Als Angriffspunkte diente das schlüssellose Einstiegssystem in Verbindung mit der mobilen App des Herstellers. [Tesla]

Neben den Fahrzeugen selbst können aber auch Kernkomponenten der Verkehrsinfrastruktur zum Ziel von Angriffen werden. Wissenschaftlern in den USA ist es beispielsweise gelungen, Sicherheitslücken in einem vernetzten Verkehrsleitsystem auszunutzen. [Jacobs] Auf diesem Wege war es ihnen möglich, fast 100 drahtlos miteinander vernetzte Ampeln aus der Ferne zu übernehmen. Für den Angriff wurden drei der am meisten verbreiteten Schwachstellen ausgenutzt: Standardzugangsdaten, unverschlüsselte Drahtlosverbindungen und schlecht gesicherte Wartungszugänge.

3.2 VERSORGUNG

Die kontinuierliche Versorgung der Bevölkerung und Wirtschaft wird durch komplexe Infrastrukturen beispielsweise für Strom, Wasser oder Gas gewährleistet. Ein Ausfall oder umfangreiche Störungen dieser Versorgungsinfrastrukturen können erhebliche Schäden verursachen und die öffentliche Sicherheit gefährden.

Die Auswirkungen eines mindestens zweiwöchigen und auf das Gebiet mehrerer Bundesländer übergreifenden Stromausfalls wurden vom Ausschuss für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages untersucht und als katastrophal eingestuft [DBT]: Telekommunikations- und Datendienste fallen teils sofort, spätestens aber nach wenigen Tagen aus. In Transport und Verkehr sind die elektrisch betriebenen Elemente der Verkehrsträger Straße, Schiene, Luft und Wasser sofort oder nach wenigen Stunden nicht mehr funktionsfähig. Dabei werden beispielsweise Menschen in U-Bahnen eingeschlossen, Ampeln funktionieren nicht mehr, Tanksäulen fallen aus, Flugzeuge können nur noch kurzzeitig starten und landen und Schiffe können nicht mehr be- und entladen werden. Die Wasserinfrastruktursysteme können ohne Strom bereits nach kürzester Zeit nicht mehr betrieben werden. Körperpflege, Essenzubereitung oder Toilettenspülung sind nicht möglich und die Seuchengefahr wächst. Auch die Versorgung mit Lebensmitteln ist problematisch, da Klimatisierung und Durchlüftung nicht funktionieren.

Bedingt durch die potenziell katastrophalen Folgen, die ein Ausfall dieser Infrastrukturen für unsere Gesellschaft hätte, werden entsprechend viele Ressourcen in die Gewährleistung ihrer Sicherheit aufgewendet. Immer relevanter werden neben funktionalen Ausfällen in diesem Zusammenhang aber auch Angriffe von außen, z. B. solche, die über informationstechnische Leit- oder Steuerungssysteme für sicherheitskritische Prozesse auf die physikalische Versorgungsinfrastruktur erfolgen. Werden beispielsweise Sensoren oder Aktoren so beeinflusst, dass falsche Werte gemeldet werden und Notfallmechanismen auslösen, dann könnte dies einerseits zur Selbstabschaltung

DIE SICHERHEITSANFORDERUNGEN IN EINER VERNETZTEN, KOMPLEXEN WELT VERÄNDERN SICH.

eines voll funktionsfähigen Infrastruktursystems führen oder aber andererseits eine notwendige Selbstabschaltung verhindern. Besonders kritisch sind eintretende Kettenreaktionen, die sich auf weitere Systeme ausweiten.

3.3 INDUSTRIE

Unsere Gesellschaft ist auf industrielle Produktionsprozesse angewiesen, die sich stetig weiterentwickeln. Unter dem Schlagwort »Industrie 4.0« wird die Vision einer stark vernetzten industriellen Produktion verstanden, bei der sich sowohl bei Maschinen zur Produktion als auch bei Materialien und Produkten die Kluft zwischen der physischen Welt und der informationstechnischen Abbildung immer weiter verringert. Maschinen werden zu cyber-physikalischen Systemen (CPS), einem engen Verbund aus Software und Hardware, die sich auf Basis von komplexen Algorithmen weitgehend an aktuelle Anforderungen anpassen können. Die Fertigung nach den Konzepten von Industrie 4.0 wird sehr flexibel gestaltet werden. Maschinen müssen sich miteinander abstimmen und ggf. auf Menschen oder andere Objekte in der Produktionshalle Rücksicht nehmen. In der Zusammenarbeit von Mensch und autonom agierenden oder hochflexiblen Maschinen darf es nicht zu Schäden an Produkten, an Maschinen oder gar Mensch und Umwelt kommen.

Es ist daher leicht vorstellbar, dass in der Industrie gerade durch den Verbund von Maschinen mit IT-Steuerungen und eingebetteten Systemen auch die Angriffsszenarien nicht nur wachsen, sondern auch individuell gestaltet werden könnten. Das reicht von der Veränderung einzelner Produkte, ganzer Produktionsstraßen bis hin zu den verarbeiteten Materialen, mit den entsprechenden Konsequenzen. Meldungen wie »Hunderte Industrieanlagen in Deutschland sind kaum vor Hackerangriffen geschützt« [Heise], haben bereits die ersten Betreiber aufgeschreckt. Eine Sicherheitslücke ermöglichte den Zugang aus dem Internet zu Steuerungsanlagen von Fernwärmekraftwerken, einer Brauerei, einer Justizvollzugsanstalt und vielen mehr.

3.4 SYSTEME ALS GEMEINSAMKEIT

Was ist die Gemeinsamkeit der vorangegangen Beispiele Verkehr, Versorgung und Industrie? Grundlage aller Beispiele sind sogenannte Systeme. Der Begriff »System« bezeichnet im Kontext dieses White Papers eine Anzahl von technischen Komponenten, die miteinander kombiniert werden und damit als Einheit angesehen werden können. Das entstandene, informationstechnische System wird dabei von seiner Umgebung abgegrenzt und stellt zugleich eine Möglichkeit zur Abstraktion dar. Beispielsweise besteht ein Computer als Gesamtsystem aus einer Anzahl von Teilkomponenten und kann bestimmte Aufgaben erfüllen, ohne dass der Endanwender Details zu internen Zusammenhängen und Abläufen wissen muss. Über Schnittstellen ist ein System mit anderen Systemen oder der Umgebung verbunden. Die Abstraktion und die Kombinierbarkeit sind mächtige Prinzipien, um leistungsfähige technische Systeme aus Teilsystemen aufzubauen.

Für die Sicherheit spielt die Größe und Komplexität von IT-Systemen eine wichtige Rolle. Mit der Anzahl der Komponenten eines Systems steigt die Wahrscheinlichkeit von Fehlern und Schwachstellen. Wie sich diese auswirken, hängt dabei stark vom konkreten System und seiner Einsatzumgebung ab. Gerade in einem sehr komplexen System kann es Zustände geben, die sich nur schwer vorhersagen und überprüfen lassen, an die daher vorher niemand gedacht hat. Derartige Zustände können im Ausnahmefall und auch bei einer vorangegangenen Risikobetrachtung zu einem Versagen des Systems und seiner Schutzmechanismen oder zu unangemessenen Gegenmaßnahmen führen.

Für die Sicherheitsbetrachtung ist fernerhin die Unterscheidung zwischen offenen und geschlossenen IT-Systemen von grundlegender Bedeutung. Offene Systeme, per Definition mit Schnittstellen zum Austausch von Informationen mit der Umgebung ausgestattet, gehen von Natur aus mit einem teilweisen Ver-

VERNETZTE IT-SYSTEME MÜSSEN SICH SELBST SCHÜTZEN KÖNNEN UND WIDERSTANDSFÄHIG GEGEN ANGRIFFE UND WIDRIGE BETRIEBSBEDINGUNGEN SEIN.

zicht auf Kontrollmöglichkeiten einher. Dieser Austausch von Informationen mit zum Teil nicht vorhersehbaren Kommunikationspartnern und einer i. d. R. als feindlich einzustufenden Umgebung wird bei geschlossenen Systemen explizit verhindert. An den Systemschnittstellen gilt es also, die richtige Balance zu finden: Schnittstellen mit geringer Funktionalität begrenzen einerseits die Einflussmöglichkeiten auf ein System und bieten damit Schutz, andererseits verhindern sie erwünschte leistungsfähigere Anwendungen.

In Bezug auf Sicherheit kommt also den Systemgrenzen und Schnittstellen eine besondere Bedeutung zu. Nur innerhalb der Systemgrenzen kann ein bestimmtes Sicherheitsniveau durchgesetzt werden. Schnittstellen wiederum erlauben von Natur aus eine Beeinflussung des Systems von außen. Traditionell wird daher das Paradigma der Perimeter-Sicherheit verfolgt, d. h. ein System wird durch die Verankerung von Sicherheitsfunktionen an seinen Außengrenzen geschützt. Für komplexe, offene oder automatisierte IT-Systeme reicht, wie die folgenden Kapitel belegen, dieser Ansatz allein jedoch nicht mehr aus.

4. ZWEI WELTEN WACHSEN ZUSAMMEN

Je nachdem, ob bei der Sicherheitsbetrachtung von IT-Systemen die Unversehrtheit der Umgebung oder die Unversehrtheit der IT-Systeme selbst im Fokus steht, liegt das Hauptaugenmerk auf der Wahrung der funktionalen Sicherheit (z. B. bei Flugzeugen oder Autos) oder der IT- und Informationssicherheit (z. B. Schutz von Systemen oder Daten). Eine gemeinsame Betrachtung der beiden Welten ist mangels geeigneter Vorgehensmodelle für dieses komplexe Querschnittsthema bisher nur in Nischenbereichen erfolgt. Die Gefahren für die öffentliche IT die von einer getrennten Betrachtung dieser beiden Sicherheitsfacetten ausgehen, müssen identifiziert und adäquate Gegenmaßnahmen entwickelt werden.

In der Safety-Welt gilt es, die Umgebung vor Schäden durch das IT-System zu schützen. Weil IT-Systeme und Infrastrukturen jedoch mehr und mehr miteinander verwoben sind, entstehen neue Gefährdungen für diese vormals abgeschotteten Systeme. Autos, Schiffe, Flugzeuge, Häuser und sogar Herzschrittmacher, alles wird vernetzt bzw. ist von außen erreichbar. In Zukunft könnte bei nicht ausreichenden Sicherheitsvorkehrungen das via Bluetooth oder WLAN erreichbare Infotainmentsystem eines Autos benutzt werden, um auf die Steuerung oder Bremselektronik zuzugreifen. Analog könnte über Fernwartungsschnittstellen für Industrieanlagen gezielte Systemstörungen wie z. B. Stromausfälle erfolgen. Technische Fehlfunktionen wären somit nicht mehr nur vom System selbst abhängig, sondern könnten von außen bewusst ausgelöst werden.

In der Security-Welt hingegen gilt es, die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Daten zu schützen. Diese klassischen Security-Schutzziele gilt es auch für externe Einflüsse durch Naturkatastrophen, Stromausfälle oder die fehlerhafte Bedienung von technischen Geräten zu sichern, da diese ebenfalls zu irreparablen Schäden für unsere IT-Systeme und unsere Daten führen können. Auch ein funktionales Fehlverhalten, ohne Einwirkung von außen, könnte zu einer ungewollten Preisgabe von Informationen führen. Umgekehrt könnte ein gezielter Angriff auf ein IT-System, mit dem vornehmlichen Ziel die Integrität oder Vertraulichkeit von Daten zu kompromittieren, als Konsequenz auch zu einem Systemausfall mit Folgen für Menschen und Umwelt führen.

4.1. SICHERE DIGITALISIERUNG UND VERNETZUNG

Mit der fortschreitenden Digitalisierung und Vernetzung unserer Gesellschaft ist die Trennung von Safety- und Security-Aspekten bereits heute nicht mehr zeitgemäß. Die Komplexität digitaler, vernetzter IT-Systeme verlangt nach einem multidisziplinären Ansatz, da eine fachspezifische Betrachtung ausschließlich Risiken aus dem eigenen Erfahrungsbereich identifiziert.

So erfolgt die Steuerung von Industrieanlagen heutzutage durch Computer und galt lange Zeit als ausreichend gut von der Außenwelt abgeschirmt. Seit Stuxnet [Stuxnet] ist die Manipulation dieser Anlagen, auch ohne direkte Anbindung an das Internet, jedoch nicht mehr nur theoretischer Natur. Ziel des Angriffs war die Manipulation der Geschwindigkeit der Zentrifugen und der Drucksteuerung, um die Urananreicherung in iranischen Atomanlagen nahezu unbemerkt zu stören. Die erste Angriffswelle ging möglicherweise von einem mit dem Schadprogramm infizierten USB-Stick aus. Eine weitere Verbreitung der Schadsoftware erfolgte anschließend über das interne Netzwerk der Anlage.

Dieser klassische Security-Angriff (Schadprogramm) auf ein klassisches Safety-Umfeld (die Sicherheit einer industriellen Anlage) zeigt, dass sich die beiden Welten faktisch bereits vermischt haben. Ein weiteres Beispiel hierfür sind neue, sich durch Vernetzung und Digitalisierung eröffnende Angriffsflächen für Cyberangriffe auf konventionelle Security-Umfelder im öffentlichen Leben. Diese waren in der Vergangenheit geprägt von autarken, mechanischen oder fest verdrahteten, technischen Hilfsmitteln, die aufgrund ihrer einfachen Aufgabenstellung bzw. der direkten Erkennung der Auswirkungen insgesamt vom Menschen überwachbar und kontrollierbar waren. Die hierfür notwendigen, technischen Hilfsmittel werden zunehmend komplexer und basieren mittlerweile nicht nur auf der Verwendung von individuellen Lösungen, sondern aus Kostengründen vielfach auf Standard-IT.

Vor dem Hintergrund der Einsparung von Personal durch Zentralisierung und Automatisierung entwickelt sich auch hier ein Trend zur (stärkeren) Vernetzung. Die ehemals sicheren Hilfsmittel werden somit zu lukrativen Angriffszielen für Cyberangriffe, in deren Auswirkung z. B. gefährliche Gegenstände durch manipulierte Gepäckscanner nicht dargestellt (false negatives)

DIE TRENNUNG VON SAFETY- UND SECURITY-ASPEKTEN IST NICHT MEHR ZEITGEMÄSS.

oder die Kontrollkräfte durch eine Häufung von Fehlalarmen (false positives) dazu verleitet werden, spätere richtige Alarme zu ignorieren. Die früher übliche Trennung der beiden Sicherheitsbelange ist als Folge der hier skizzierten Entwicklungen somit nicht mehr zeitgemäß, da die Verknüpfung von Einzelrisiken zu einem hohen Risiko für die Unversehrtheit unserer Gesellschaft und unserer Werte führt.

4.2. STANDARDISIERUNG

Auch die Standardisierung muss sich an diese neuen Gegebenheiten in der Welt der Sicherheit anpassen. Noch werden Standards im Safety- und Security-Bereich vorwiegend separat und ohne gegenseitigen Bezug von unterschiedlichen Standardisierungsgremien behandelt. Dadurch überlappen sie sich oder definieren verschiedenartige Sicherheitsklassen und -maßnahmen. Wichtige Standards aus den beiden Welten sind:

- Im Security-Umfeld existieren Standards zur Bewertung und Zertifizierung verschiedener IT-Sicherheitsaspekte. So bildet die internationale ISO/IEC 27000-Normenreihe die Grundlage für Informationssicherheits-Managementsysteme (ISMS), um angemessene technische und organisatorische Maßnahmen gegen identifizierte Risiken ergreifen zu können. Die Evaluierung und Zertifizierung von IT-Sicherheitsprodukten hingegen erfolgt vornehmlich gemäß der Norm ISO/IEC 15408 (Common Criteria). Risikomanagement wiederrum wird in der Normenreihe ISO 31000 behandelt.
- Im Safety-Umfeld wird die funktionale Sicherheit von elektrischen, elektronischen sowie programmierbaren elektronischen Systemen anwendungsunabhängig als Sicherheitsgrundnorm in der Normenreihe IEC 61508 (in Deutschland VDE 0803) spezifiziert. Ziel der IEC 61508 ist es, Ausfälle von Steuerungssystemen (die z. B. zu Brand, Freisetzen giftiger Stoffe, Wiederanlauf einer Maschine usw. führen) und unerkannte Ausfälle in Schutzsystemen (z. B. in einem Notabschaltsystem) zu verhindern. Anwendungsspezifische Ausprägungen der Grundnorm sind beispielsweise ISO 26262 für Fahrzeugelektronik, IEC 62061 für Maschinensteuerungen oder IEC 61513 für Kernkraftwerke.
- Zu den wenigen Standards, die Security im Safety-Umfeld behandeln, gehören die Normen der Reihe IEC 62443, die IT-Sicherheitsmanagement in industriellen Automatisierungssystemen und kritischen Infrastrukturen (z. B. Energie-, Gas- und Wassernetze) spezifizieren. Security-Konzepte für diesen klassischen Safety-Kontext sind u. a. Sicherheitszonen und -kanäle zur Strukturierung von mehrfachen Verteidigungslinien und zur sicheren Kommunikation, Sicherheits-Level, die Bewertung der Reife von IT-Sicherheitsprogrammen sowie IT-Sicherheitsleitlinien.

Historisch gesehen werden Safety-Standards schon wesentlich länger entwickelt und gelebt. Gerade deshalb ist für den Informationssicherheitsbereich die Übernahme und Anpassung etablierter, erfolgreicher Konzepte sinnvoll. Regeln, wie die Einschränkung der Funktionalität von Software auf das zwingend erforderliche Maß (Minimalprinzip), vollständig definierte Schnittstellen ohne undokumentierte Funktionen, die Verwendung gesicherter Softwareelemente oder die Reduktion von Abhängigkeiten, um kaskadierende Fehlereffekte zu unterbinden, sind im Safety-Bereich gängig (siehe beispielsweise die Anforderungen an Software in IEC 61508-3:2010), werden aber im Informationssicherheitsbereich nicht immer beachtet, wobei hier häufig Kostengründe angeführt werden. Umgekehrt sind kryptographische Lösungen u. a. für Identifizierung, Authentisierung, Verschlüsselung und Zugriffkontrolle in Safety-Standards selten verankert. Um beide Welten zu verbinden und Sicherheit ganzheitlich zu betrachten, sind »gemeinsame« Standards zukünftig erforderlich.


PENCON

5. NEUE HERAUSFORDERUNGEN UND TRENDS FÜR GANZHEITLICHE SICHERHEIT

Komplexe Infrastrukturen und IT-Systeme werden technisch aus einzelnen Bausteinen zusammengesetzt. Die Komponenten oder Teilsysteme können Hard- oder Software umfassen und von einfachen Funktionen bis zu sehr komplexen Teilsystemen reichen. Im Mittelpunkt von Sicherheitsbetrachtungen muss daher der Systemgedanke stehen: Welche Aufgaben hat das betrachtete System, aus welchen Teilsystemen ist es zusammengesetzt und wie reagiert es in verschiedenen Situationen? Diese und viele weitere Fragen lassen sich dann verlässlich auf Basis von wissenschaftlichen Theorien zur Funktion beantworten. In vielen Technikbereichen hat sich dieses Vorgehen bewährt. Im Bereich der relativ jungen Softwareentwicklung muss es sich gegenüber einem Drang nach neuen Funktionen oder einfachen Lösungen in vielen Bereiche jedoch erst noch durchsetzen.

Notwendige Schritte zur Entwicklung sicherer IT-Systeme sind bekannt: Bspw. eine präzise Beschreibung der Systemfunktion und der Schnittstellen, ein systematischer und dokumentierter Entwurfsprozess, das umfangreiche Testen der Implementierung und die Begleitung der Betriebsphase z. B. mit Sicherheitsupdates. Allerdings besteht durchaus Forschungsbedarf, bspw. wie komplexe Systeme aufgebaut werden können oder wie sich die Kombination verschiedener Systeme auf die Systemsicherheit auswirkt. Im Weiteren werden entsprechende Herausforderungen und Forschungsansätze vorgestellt.

5.1. WIEDERVERWENDUNG VON IT-SICHERHEITSBAUSTEINEN

In den verschiedensten Anwendungsgebieten werden immer wieder die gleichen informations- und kommunikationstechnischen Kernkomponenten eingesetzt und um spezifische Anwendungslogik ergänzt. Solche Kernkomponenten sind beispielsweise Steuerungscomputer mit ihrem Betriebssystem (embedded systems/eingebettete Systeme) oder Softwarebibliotheken. Auch werden die gleichen Kommunikationsinfrastrukturen für verschiedene Anwendungsgebiete genutzt, vom offenen Internet bis zu privaten Übertragungsstrecken auf Basis der Glasfaserinfrastruktur eines Netzbetreibers. Durch die bereits beschriebene Durchdringung herkömmlicher Infrastrukturen mit den immer gleichen IT-Bausteinen und zumindest gradueller Nutzung der gleichen Kommunikationsinfrastrukturen ergeben sich neue Gefährdungen.

Zwei eindrucksvolle Beispiele sind der im April 2014 bekannt gewordene Heartbleed-Bug sowie die Sicherheitslücke Shellshock aus dem September 2014. [Heartbleed, Shellshock] In beiden Fällen wog besonders schwer, dass OpenSSL und die Unix-Shell Bash in zahllosen Produkten eingesetzt werden und somit in kürzester Zeit nicht nur ein einzelner Gerätetyp, sondern sehr viele verschiedene Systeme und Geräte angreifbar wurden.

Entwickler müssen sich darauf verlassen können, dass ihre Systeme durch den Einsatz solch weit verbreiteter Softwarekomponenten sicherer oder zumindest nicht unsicherer werden. Dies gilt insbesondere für kryptografische oder ähnlich komplexe Algorithmen, die nicht ohne weiteres von Nicht-Fachleuten überprüft werden können. Aufgrund der Komplexität dieser Funktionen stehen im Allgemeinen jedoch nur wenige Implementierungen zur Verfügung, sodass die Mehrzahl der heutigen Systeme in der öffentlichen IT auf dem gleichen und in Teilen schwachen Fundament aufbauen. Hier muss mit geeigneten Mitteln Zuverlässigkeit und Sicherheit nachgewiesen werden können.

5.2. RESILIENZ – WIDERSTANDSFÄHIGE ÖFFENTLICHE IT

Die wachsende Vernetzung und Entgrenzung von Systemen in einer zunehmend unsichereren Umgebung kann dazu führen, dass bereits kleine Störungen in Teilsystemen ein unvorhersehbares Verhalten und letztlich gravierende Probleme für das Gesamtsystem bewirken. Ein Lösungsansatz für diese zunehmend bedeutsame Herausforderung für unsere Gesellschaft ist die Verbesserung der Fähigkeit von Systemen, mit widrigen Ereignissen umgehen zu können (Resilienz).

Bedingt durch die ansteigende Popularität des Trendthemas Resilienz existieren zahlreiche Begriffsdefinitionen. Diese lassen sich zusammenfassen als »die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen« [acatech].

Um das komplexe Konzept besser erfassen und darstellen zu können, wurde in [acatech] ein Resilienzzyklus entwickelt. Die darin abgebildeten fünf Resilienz-Phasen sind aufgeteilt in

Abbildung 2: Die fünf Phasen des Resilienzzyklus

- die Vorbereitung auf Katastrophen (prepare),
- die Reduzierung der Risikofaktoren, um das Eintreten eines Ereignisses soweit wie möglich zu verhindern (prevent),
- den Schutz vor negativen Auswirkungen durch geeignete Schutzsysteme (protect),
- das Aufrechterhalten der essenziellen Funktionsfähigkeit, um schnell und adäquat reagieren zu können (respond) und
- die eigenständige Erholung des Systems und das Lernen aus dem Ereignis, um für künftige Bedrohungen besser gerüstet zu sein (recover).

Das Resilienz-Engineering als Forschungsgebiet beschäftigt sich mit der Erforschung und Entwicklung von Methoden zur Erhöhung von Widerstandfähigkeit, Anpassbarkeit und Selbstorganisation von Systemen. Resilience-by-Design als übergreifende Sicherheitsstrategie zielt analog zu Security-by-Design auf eine ganzheitliche Integration dieser Systemeigenschaften in den Entwicklungsprozess ab. Diese Strategien sind nicht neu. Dank des aktuellen Hypes um das Internet der Dinge und Industrie 4.0 sind die Chancen für ihre weitere Erforschung und tatsächliche Umsetzung jedoch größer als jemals zuvor.

Die Gefahr beim Resilienz-Engineering besteht darin, dass ein System auf der Basis von Erfahrungen konstruiert wird, wobei aus der Natur der Sache heraus nur vorhersehbare Gefährdungen betrachtet werden können. Das implementierte System ist dann zukünftig nicht in der Lage, unerwartete Bedrohungen abzuwehren. Es ist daher wichtig, dass die Lern- und Anpassungsfähigkeiten eines Systems berücksichtigt werden. Resilienz ist also kein statischer Zustand, sondern die Eigenschaft lernfähiger und adaptiver Systeme, Funktionsfähigkeit in einer unsicheren Welt zu ermöglichen.

5.3. AUTONOME SYSTEME – SICHERHEIT TROTZ KOMPLEXITÄT

Zur Realisierung resilienter Systeme sind die Forschungsgebiete Selbstorganisation und autonome Systeme (Autonomic Computing/Networking) relevant. Ziel des Einsatzes autonomer Systeme ist zunächst die Automatisierung. So ist es z. B. nicht möglich, in einem Mobilfunknetz tausende von Basisstationen von Hand einzurichten und im Betrieb manuell zu kontrollieren. Für diese Aufgaben werden daher bereits heute hochgradig automatisierte oder autonome Systeme eingesetzt, die selbständig in der Lage sind, vorgegebene Aufgaben in einem sich ändernden Umfeld zu erfüllen.

Autonome IT-Systeme sind durch vier Hauptfunktionen charakterisiert [IBM]:

- Selbstkonfiguration – Anpassung an eine dynamische Umgebung
- Selbstoptimierung – Optimierung des Ressourceneinsatzes
- Selbstschutz – Erkennung und Schutz vor Angriffen
- Selbstheilung – Diagnose und korrektive Aktionen zur Vermeidung von Unterbrechungen

Dabei sind die Aufgaben für derartige Systeme weit komplexer als einfache Regelschleifen traditioneller adaptiver Systeme. Die Vorsilbe »selbst« verweist darauf, dass ein System diese Aufgaben eigenständig im Rahmen seiner Möglichkeiten übernimmt, ohne dass eine konkrete Reaktion schon bei der Entwicklung des Systems vorgegeben wurde. Die verschiedenen Aufgaben können in der Realität widersprüchlich sein und daher eine hohe technische Intelligenz vom System verlangen.

Am Beispiel autonomer Systeme zeigt sich deutlich die Verbindung der verschiedenen Aspekte von Sicherheit. Autonome Systeme sind besonders geeignet, verschiedene Ziele gleichzeitig zu berücksichtigen. Daraus ergeben sich aber auch neue Herausforderungen für die Sicherheit: Die starke Anpassbarkeit

LERNFÄHIGKEIT UND KORREKTIVE ADAPTION AN NEUE GEGEBENHEITEN STÄRKEN DIE INNERE ABWEHRKRAFT VERNETZTER SYSTEME.

in einem dynamischen Umfeld kann für Angriffe ausgenutzt werden. Ein System könnte über die Manipulation seiner Umgebung oder von Eingangsinformationen zunächst geschwächt werden, um danach gezielt angegriffen zu werden. Die ausgeprägte Flexibilität eines derartigen Systems erlaubt also nicht nur einen erweiterten und automatisierten Einsatz im Vergleich zu herkömmlichen Systemen, sondern kann auch für neuartige Angriffe ausgenutzt werden.

Autonome Systeme sind eine vielversprechende Möglichkeit, komplexe Infrastrukturen effizient aufzubauen und zu steuern, um die zuvor angesprochene Resilienz zu verwirklichen. Auf Grund ihrer inhärenten Komplexität, durch die autonome Systeme nur schwer vorhersagbar und somit risikoreich sind, muss die Forschung neue Entwurfs- und Testmethoden entwickeln, um die Sicherheit derartiger Systeme zu gewährleisten.

6. HANDLUNGSFELDER UND FORSCHUNGSFRAGEN

Die im White Paper dargestellten Beispiele lassen eine Reihe von Handlungsfeldern im aktuellen Forschungsgebiet Sicherheit erkennen, die auf der fortschreitenden Vernetzung unserer Gesellschaft mit IT beruhen. Die Wechselwirkung zwischen den Teilaspekten Safety und Security spielt für zukünftige Sicherheitsbetrachtungen im Bereich der öffentlichen IT eine zentrale Rolle.

Sicherheit ist jedoch nur ein Aspekt beim Betrieb von Systemen, in der Praxis konkurrierende Aspekte sind Wirtschaftlichkeit und Leistungsfähigkeit. Teure oder langsame Lösungen, die zwar sicherer als Konkurrenzprodukte sind, werden nur in Bereichen mit besonders hohen Sicherheitsanforderungen Akzeptanz finden.

Die Entdeckung des einen neuen Prinzips, des sogenannten »silver bullet« (dt. Allheilmittel), mit dem alle Systeme auf einen Schlag sicher gemacht werden können, wird es auch nicht geben. Es zeichnen sich aber eine Reihe von Prinzipien ab, deren Erforschung und Weiterentwicklung Erfolg versprechen bzw. konkrete Mechanismen, deren Einsatz das Sicherheitsniveau in Zukunft anheben wird.

1. Unterschiede zu Gemeinsamkeiten machen.
Um langfristig zu verhindern, dass Unsicherheit zu einer Grundeigenschaft der IT-Welt wird, ist es unabdingbar, von der Erfahrung anderer Fachgebiete in Bezug auf Sicherheit zu lernen. Im Security-Bereich gilt es, Sicherheit genauso tief im Design- und Entwicklungsprozess zu verankern, wie es bei Safety bereits seit Jahrzehnten der Fall ist. Hierfür fehlt es jedoch weiterhin an entsprechenden domänenspezifischen, standardisierten Vorgehensweisen, Werkzeugen und Methoden. Für den Safety-Bereich gilt derweil, aus den unzähligen Security-Sicherheitsvorfällen der letzten Jahre zu lernen und die grundlegenden Informations- und Datenschutzfehler nicht zu wiederholen.

2. Sicherheit erfordert ein Denken in Systemen.
Sicherheit muss schon im Systemdesign angelegt sein (Safety-by-Design und Security-by-Design). Dazu müssen Computer nicht neu erfunden werden, aber es muss bewertbar sein, auf welche Teile des Systems man sich in welcher Situation verlassen kann. Abschottung allein reicht nicht mehr aus, wenn Systeme vernetzt, hochflexibel und autonom sein sollen. Systeme müssen sich selbst schützen können und widerstandsfähig gegen Angriffe und widrige Betriebsbedingungen sein. Gleichzeitig muss die Komplexität des Systems begrenzt und kontrollierbar werden, bspw. durch die Wiederverwendung von in sich abgeschlossenen Teilsystemen, die über ein bekanntes und verifiziertes Systemverhalten verfügen. Das Minimalprinzip muss noch viel häufiger Verwendung finden – Die Verknüpfung von Systemen sollte immer über möglichst minimale und beherrschbare Schnittstellen erfolgen.

3. Die Integration, Komposition bzw. Einbettung von Systemen mit unterschiedlichen Sicherheitsniveaus muss schlussendlich zu einem sicheren Gesamtverbund führen.
Bisher wurden technische Systeme wie Industrieanlagen, Strom- und Wasserinfrastrukturen oder Atomkraftwerke mit erheblichem zeitlichem und monetärem Aufwand entwickelt, getestet und betrieben, um ihre Sicherheit zu gewährleisten. Mit Informationstechnologie wandelt sich diese Systematik und wird offener und schnelllebiger, beispielsweise durch Internetzugang, Software-Updates oder regelmäßiges Patchen von Sicherheitslücken. Das betrifft nicht nur neue, sondern durch Systemvernetzung oft auch Altsysteme und Anlagen, die in vielen Betriebsdekaden nicht verändert wurden. Die Herausforderung, Sicherheit auch nachträglich zu integrieren, beziehungsweise langlebige und sich schnell ändernde Systeme und Komponenten mit unterschiedlichen Sicherheitsniveaus zu einem sicheren Gesamtverbund zu gestalten, eröffnet umfassende Forschungsfelder für die nächsten Jahre.

4. Sicherheit messbar machen und mit Unsicherheiten leben
Wann kann ein System als ausreichend sicher angesehen werden? Wie können (potenziell) unsichere Systeme in kritische Systeme integriert werden? Diese und weitere Forschungsfragen gilt es zu untersuchen. Gefördert werden muss vor allem die Entwicklung von geeigneten Metriken und Werkzeugen, um Sicherheit mess- und bewertbar zu machen. Bewertungsmethoden aus Sicherheitszertifizierungsstandards können hierfür etwa als Ausgangspunkt verwendet werden. Die Messbarkeit von Sicherheit ist gleichzeitig die Grundlage, um ein realistisches Sicherheitsniveau auszuwählen, das Risiken und Auswirkungen miteinander in Beziehung setzt.

5. Komplexität durch Tests und Simulationen beherrschbar machen.
Unsere moderne, vernetze Welt gibt Anlass, über neue IT-Sicherheitsprüfungen nachzudenken. Dies ist vor allem in Berei-

FÜR KOMPLEXE UND OFFENE IT-SYSTEME REICHT DAS PARADIGMA DER PERIMETER-SICHERHEIT ALLEIN NICHT MEHR AUS.

chen notwendig, die sich bis dato nur peripher mit IT-Sicherheit befasst haben. An erster Stelle gilt es, die Erforschung und Weiterentwicklung von Sicherheitstests und Angriffssimulationen maßgeschneidert für offene, komplexe Systeme voranzutreiben. Diese müssen auch der Tatsache gerecht werden, dass die Kombination von Teilsystemen neue Komplexität mit ins Spiel bringt. Um eine durchgängige Testkette zu realisieren, müssen die verteilten System- und Testexpertisen für alle Systemkomponenten (Hardware, eingebettete System, Betriebssystem, …) zusammengebracht werden.

6. Sicherheit darf nicht primär vom Benutzer bzw. der Benutzung abhängen.
Um Informationssicherheit zu gewährleisten, werden meist Anforderungen an die Fähigkeiten der Nutzer gestellt, wie beispielsweise Passwortregeln, Patch-Verhalten oder Installationsanweisungen. Ist ein Schutz vor Fehlbedienung in IT-fernen Bereichen längst Standard, so müssen zukünftig auch IT-nahe Produkte und Systeme eine sichere Benutzung garantieren. Auch wenn eine Sensibilisierung und Befähigung der Menschen für Sicherheitsaspekte weiter gefördert werden muss, so sollte jedoch die Hauptverantwortung für Sicherheit von den Herstellern und Betreibern nicht auf den Endnutzer abgewälzt werden. Um dies zu erreichen, muss Sicherheit weitestmöglich unabhängig von Benutzer und Benutzung werden.

7. Standards und Architekturen sind die Grundlage von Sicherheit.
Standards müssen dem Bedarf nach umfassenden Sicherheitskonzepten gerecht werden und sich dahin weiterentwickeln. Leistungsfähige Architekturen und mit der Praxis abgestimmte Einsatzkonzepte (Best Practices) tragen dazu bei, die Entwicklung neuer Systeme zu vereinfachen oder sichere Komponenten auch in entferntere Anwendungsbereiche einzuführen. In sensiblen Bereichen kann darauf aufbauend die Forderung nach verbindlicher Einhaltung von Mindeststandards für Produkte die gesamte IT-Landschaft sicherer machen.

8. IT-Sicherheit als strategisch wichtiges Ziel annehmen und Hilfe zur Selbsthilfe geben.
Sicherheitsmanagement ist ein ressortübergreifendes Thema, das nur durch eine intensive Verzahnung von IT- und Fachabteilungen nachhaltig bearbeitet werden kann. Der Mensch mit all seinen Stärken und Schwächen ist dabei immer als Teil des Sicherheitsmanagementsystems zu beachten und darf nicht vergessen werden. Die Politik hat hier die Aufgabe, Rahmenbedingungen für das sichere Leben, Arbeiten und Wirtschaften in der digitalen, vernetzen Welt zu schaffen.

9. IT-Hersteller und -Diensteanbieter sollen für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften.
Die diesbezügliche Forderung aus dem Koalitionsvertrag [Koalitionsvertrag] muss mit Leben gefüllt werden. Das IT-Sicherheitsgesetz und die geplante Cybersicherheitsrichtlinie der EU sind erste Schritte, um bestimmte Meldepflichten für Sicherheitsvorfälle einzuführen. Allerdings besteht dadurch noch keine Verpflichtung für Hersteller, bekannte Sicherheitslücken in Hardware- und Softwareprodukten zu beseitigen bzw. für mögliche Schäden zu haften. Hier muss die Politik den nächsten Schritt gehen, um Hersteller stärker in die Verantwortung zu nehmen.

7. LITERATUR

[acatech] Klaus Thoma (Hrsg.): Resilience-by-Design: Strategie für die technologischen Zukunftsthemen, acatech Studie, April 2014, http://www.acatech.de/de/publikationen/stellungnahmen/acatech/detail/artikel/resilien-tech-resilience-by-design-strategie-fuer-die-technologischen-zukunftsthemen-1.html

[Alexander] Thomas Alexander und Jens Tölle: »Safety and IT-Security: Transfer of methods, knowledge and lessons-learned?«, Tagungsband Future Security 2014, Seiten 532-539

[BMW] Spiegel Online: »Sicherheitslücke: 2,2 Millionen BMW konnten gehackt werden«, http://www.spiegel.de/auto/aktuell/adac-entdeckt-it-sicherheitsluecke-bei-bmw-connected-drive-a-1015819.html

[Jacobs] Suzanne Jacobs: Hackangriff auf Ampeln, Technology Review, 26.8.2014, http://www.heise.de/tr/artikel/Hackangriff-auf-Ampeln-2301450.html

[Borsdorff] Anke Borsdorff und Martin Kastner: Definitionskalender polizeiliches Einsatzrecht, Lübecker Medien Verlag, 2. Auflage, 2012.

[BSI] Bundesamt für Sicherheit in der Informationstechnik: Cybersicherheit, Begriffserläuterung und Einführung, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/Sicherheitsvorfaelle/Begriffserlaeuterungen/Begriffserlaeuterungen_node.html

[DBT] Deutscher Bundestag, Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung, TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung, Drucksache 17/5672, 27. 04. 2011, http://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf

[Heartbleed] Heise Security: Der GAU für Verschlüsselung im Web: Horror-Bug in OpenSSL, http://www.heise.de/security/meldung/Der-GAU-fuer-Verschluesselung-im-Web-Horror-Bug-in-OpenSSL-2165517.html

[Heise] Heise: Hunderte Industrieanlagen ungesichert im Internet, Presseinformation, 2. Mai 2013, http://heise-medien.de/-1854654 und http://heise.de/-1854385

[IBM] Jeffrey O Kephart, David M Chess: The vision of autonomic computing, Computer 36(1), 41--50, IEEE Computer Society, 2003

[IT-Grundschutz] Bundesamt für Sicherheit in der Informationstechnik, »IT-Grundschutz – die Basis für Informationssicherheit«, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[Koalitionsvertrag] Koalitionsvertrag: Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, http://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/koalitionsvertrag-inhaltsverzeichnis.html

[Lagebericht] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2014, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

[Shellshock] Heise Security: ShellShock: Standard-Unix-Shell Bash erlaubt das Ausführen von Schadcode, http://www.heise.de/security/meldung/ShellShock-Standard-Unix-Shell-Bash-erlaubt-das-Ausfuehren-von-Schadcode-2403305.html

[Stuxnet] Heise Security: Stuxnet-Wurm kann Industrieanlagen steuern, http://www.heise.de/security/meldung/Stuxnet-Wurm-kann-Industrieanlagen-steuern-1080584.html

[Tesla] Spiegel Online: Tesla Model S: Hacker-Attacke bei voller Fahrt, 23.07.2014, http://www.spiegel.de/auto/aktuell/tesla-model-s-von-hackern-fremdgesteuert-a-982481.html

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Nadja Menz
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 1504 (Fotos: Fraunhofer FOKUS)