Djeffal, C. (2019). IT-Sicherheit 3.0: Der neue IT-Grundschutz: Grundlagen und Neuerungen unter Berücksichtigung des Internets der Dinge und Künstlicher Intelligenz. *Multimedia Und Recht*, 289–294.

IT-Sicherheit 3.0: Der neue IT-Grundschutz

Grundlagen und Neuerungen unter Berücksichtigung des Internets der Dinge und Künstlicher Intelligenz

Christian Djeffal

Dieser Beitrag erläutert die Grundlagen und Neuerungen des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI), der in den letzten Jahren erneuert und am 1.2.2018 offiziell veröffentlicht wurde. Er zeigt die Relevanz auf, die der IT-Grundschutz sowohl für das Recht als auch für die Ausübung juristischer Berufe hat. Es wird auch erläutert, wann der IT-Grundschutz in Rechtsfragen relevant ist. Ferner widmet sich der Beitrag auch den weiteren Dimensionen des IT-Grundschutzes für die tägliche juristische Arbeit. Daher will der Beitrag vermitteln, wie sich Juristinnen und Juristen schnell und einfach über den Stand der Technik in Sachen IT-Sicherheit informieren können. Dazu wird erläutert, wie i.R.d. IT-Grundschutzes mit neuen technologischen Trends – Internet der Dinge oder Künstliche Intelligenz – umgegangen wird.

Lesedauer: 26 Minuten

I. Einleitung

Informationstechnologie ist zu einer grundlegenden Infrastruktur in allen Bereichen geworden. IT-Sicherheit ist genauso wichtig wie Informationstechnologie. Von ihr hängen reale, berufliche, politische und wirtschaftliche Existenzen ab. Kenntnisse über IT-Sicherheit sind schon heute zentrales Kriterium für Zuverlässigkeit und Vertrauenswürdigkeit, auch in allen juristischen Berufen. Kommunikation ist ein wichtiger Bestandteil aller juristischen Tätigkeiten, denn zunehmend spielen auch Informations- und Kommunikationstechnologien im Recht eine Rolle. Legal Tech,[1] eGovernment[2] und eJustice sind nur einige der Schlagworte, die die Digitalisierungstrends im juristischen Bereich kennzeichnen. Der IT-Grundschutz ist u.a. eine wichtige und zentrale Erkenntnisquelle über den Stand der Technik in der IT-Sicherheit und über technische und organisatorische Maßnahmen. Juristinnen und Juristen, die die Systematik des IT-Grundschutzes kennen, haben dadurch relativ einfachen Zugang zu Kenntnissen zur Schaffung von Informationssicherheit. Diese Kenntnisse spielen eine immer größere Rolle, denn beinahe täglich werden Angriffe auf IT-Systeme gemeldet. Mittlerweile ist auch das Bewusstsein in der Öffentlichkeit durch spektakuläre Angriffe und Datendiebstähle gestiegen: So wurden beim Equifax-Hack sensible Daten wie Sozialversicherungsnummer, Geburtsdatum und Adresse von 143 Mio. Amerikanerinnen und Amerikanern gestohlen. Beim Sony-Hack wurde gut dokumentiert, wie die Angreifer in einem Unternehmen sämtliche wichtige Daten inklusive Geschäftsgeheimnissen, Produkten und interner Kommunikation einsehen konnten. Was beim Doxing-Angriff vermutet wurde, bei dem personenbezogene Daten über einen großen Teil der deutschen politischen Elite kopiert wurde, ist für die Equifax-Attacke mittlerweile Gewissheit: die Angreifer nutzten das Fehlverhalten verschiedener Menschen aus dem Umfeld und der Organisation aus, dabei wurden einfachste Sicherheitsvorkehrungen außer Acht gelassen.[3] Diese Beispiele belegen deutlich,

dass Informationssicherheit nicht nur von der Sicherheit von Software und Geräten abhängt. IT-Sicherheit kann es nur geben, wenn sie gelebt wird. Das betrifft Organisationen, Verfahren und Menschen.

Auf nationaler Ebene wurde gerade ein „IT-Sicherheitsgesetz 2.0" eingebracht und auf europäischer Ebene hat man sich bereits auf den sog. Cybersecurity Act geeinigt. Dabei war in den vergangenen Jahren schon einiges passiert.

So hat der Gesetzgeber zwei umfassende Gesetzespakete verabschiedet, die die IT-Sicherheit in unterschiedlichen Bereichen fördern.[4] Eines dieser Gesetze setzt die europäische NIS-Richtlinie um, die den Schutz Kritischer Infrastruktur vorschreibt.[5] Verschiedene Anzeichen deuten darauf hin, dass es in den kommenden Jahren zu noch mehr Investitionen und Aktivitäten im Bereich der IT- und Cybersicherheit kommen wird. So sieht etwa der Koalitionsvertrag unter der Überschrift „sicheres Leben in Deutschland – auch online" zahlreiche Maßnahmen für die nächste Legislaturperiode vor. Sie stehen im Kontext der Cybersicherheitsstrategie der *Bundesregierung*, die ebenfalls zahlreiche Maßnahmen und Ziele formuliert.[6] Der *Kommissionspräsident* hat in seiner Rede vom September 2018 weitere Neuerungen in diesem Bereich angekündigt.[7] Es passt also ins Bild, dass in diesem dynamischen Bereich auch das *BSI* zum zweiten Mal seinen IT-Grundschutz sowohl inhaltlich als auch methodisch grundlegend überarbeitet hat. Dies geschah auf der Grundlage eines längeren Prozesses, an dem auch verschiedene Stakeholder beteiligt wurden. Eine finale Entwurfsfassung wurde am 11.10.2017 auf der Messe it-sa in Nürnberg vorgestellt, die redaktionell finalisierte Fassung ist am 1.2.2018 veröffentlicht worden. Das *BSI* hat den IT-Grundschutz runderneuert und auf eine neue Stufe gehoben. Die alten IT-Grundschutz-Kataloge werden vom IT-Grundschutz-Kompendium abgelöst. Damit sind nicht nur eine Aktualisierung und eine Verschlankung verbunden, vielmehr hat das *BSI* die Struktur des IT-Grundschutzes verändert und ihm neue Dimensionen gegeben. Diese Neuerungen wird dieser Beitrag vorstellen. Darüber hinaus wird die juristische Relevanz des neuen IT-Grundschutzes aufgezeigt und in seine Methodik eingeführt. Herausgehoben werden soll besonders ein Aspekt des neuen IT-Grundschutzes, nämlich sein Umgang mit neuen Technologien wie dem Internet der Dinge und Künstlicher Intelligenz.

II. Grundlagen

Beim IT-Grundschutz handelt es sich um verschiedene Elemente einer umfassenden Methodik für Informationssicherheit in Organisationen. Der IT-Grundschutz will dazu beitragen, dass solche Organisationen, wie Unternehmen oder Behörden, ein ausreichendes IT-Sicherheitsniveau erreichen. Was dazu konkret notwendig ist, ist im IT-Grundschutz-Kompendium festgehalten. Auf dieser Grundlage können sich Organisationen auch nach den BSI-Standards 200-1 bis 200-3 zertifizieren lassen. Der IT-Grundschutz beschreibt also Empfehlungen und Best-Practices und erlaubt auch deren Zertifizierung. Ziel ist der sichere Einsatz der Informations- und Kommunikationstechnik von Unternehmen oder Behörden. Abgesichert werden sollen also nicht bestimmte Produkte in der Herstellung, sondern die Technik in ihrer Anwendung. Daher geht es beim IT-Grundschutz an vielen Stellen auch um Organisation, Personal und Prozesse. Hier stehen die Menschen im Fokus, nicht die Technik.

Der IT-Grundschutz vermittelt zwischen zwei grundsätzlichen Ansätzen in der IT-Sicherheit: Zwischen der sog. Grundschutzmethode und der Risikoanalysemethode.[8]

■ Die Grundschutzmethode beschreibt Anforderungen für bestimmte Fallgestaltungen und stellt Maßnahmen dar, die in der Regel als Best-Practices zu befolgen sind. Sie geht davon aus, dass bei der Einhaltung des Grundschutzes eine ausreichende Basissicherheit vorliegt.

■ Im Gegensatz dazu müssen die Risiken bei der Risikoanalysemethode erst im Einzelfall erkannt werden.

Beide Elemente finden sich im IT-Grundschutz des *BSI*, dessen Anfänge bis in die 1990er Jahre zurückreichen. Damals etablierte sich in Deutschland ein IT-Grundschutz-Handbuch, das vom *BSI* erstellt wurde und Einzelmaßnahmen zur Förderung der Informationssicherheit vorsah (IT-Grundschutz 1.0).[9] Im Rahmen einer ersten Überarbeitung wurde das Handbuch in die IT-Grundschutz-Kataloge überführt, die eine Zertifizierung nach der international anerkannten Norm ISO 27001 zuließen (IT-Grundschutz 2.0). Zu diesem Zweck wurden vier Standards entwickelt, die inhaltlich auf dem IT-Grundschutz-Handbuch aufbauten. Organisationen konnten sich nach diesen Standards auf der Grundlage der Kataloge zertifizieren lassen. In den IT-Grundschutz-Katalogen waren dabei schon viele Risiken und Maßnahmen typisiert dargestellt, besondere Gefährdungslagen mussten jedoch bestimmt werden. Schon vor der jetzigen Reform genoss der IT-Grundschutz des *BSI* großes Ansehen, er wurde u.a. von Schweden und Estland übernommen. Denn der IT-Grundschutz erlaubte zwar eine Zertifizierung auf der Basis der Norm ISO/IEC 27001, doch im Vergleich zu dieser Norm zeichneten ihn ein höherer Detaillierungsgrad und viele Hinweise zur tatsächlichen technischen Umsetzung aus.[10] Das Wissen um diese Maßnahmen war schon damals frei und öffentlich zugänglich. Was die neuerlichen Änderungen bedeuten und erreichen sollen, lässt sich insbesondere dann verstehen, wenn man die Kritik am IT-Grundschutz 2.0 kennt.[11] Kritisiert wurde dabei insbesondere, dass der IT-Grundschutz die Spezifika bestimmter Branchen und Unternehmen zu wenig berücksichtige.[12] Anders als bei Industriestandards[13] und besonders IT-Sicherheitsnormen, seien die betroffenen Unternehmen hier nicht in gleichem Maße an der Erstellung beteiligt worden.[14] Dies wiege umso schwerer, als Unternehmen im Vergleich zu ISO/IEC 27001 weniger Umsetzungsspielraum hätten.[15] Das war besonders für große Organisationen problematisch. Für kleine und mittlere Unternehmen war die Umsetzung der detaillierten Vorschläge oft schwer zu stemmen.[16] Diese Kritik wird in der neuen Version des IT-Grundschutzes adressiert. Der IT-Grundschutz wurde vor allem stark gekürzt, durch eine stringente Systematik sind von den zuletzt 5.028 Seiten nur noch 840 Seiten geblieben.

III. Elemente des IT-Grundschutzes 3.0

Die überarbeitete Version des IT-Grundschutzes fügt seinen wesentlichen Strukturelementen einige wichtige Neuerungen hinzu. Sowohl die Grundlagen als auch die Neuerungen sollen im Folgenden erklärt werden. Die wichtigsten Instrumente des IT-Grundschutzes sind das IT-Grundschutz-Kompendium, die drei Standards und der Leitfaden zur Basisabsicherung. Dazu kommen noch die neu eingeführten Profile.

1. IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium stellt sich als „Nachschlagewerk zur Informationssicherheit" vor.[17] Es vermittelt, wie sich Organisationen gegen typische Gefährdungen der IT-Sicherheit durch ein ausreichendes Sicherheitsniveau schützen können. Zum 1. Februar eines jeden Jahres wird es erneuert, zu diesem Zeitpunkt bildet der IT-Grundschutz auch den Stand der Technik ab, also den „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen welcher zur Erreichung eines allgemein hohen Schutzniveaus geeignet ist.[18] Damit enthält das IT-Grundschutz-Kompendium einen großen und leicht zugänglichen Schatz an Wissen über IT-Sicherheit. Dieses Wissen ist so aufbereitet, dass man eine typische Organisation, also einen Informationsverbund aus der IT-Sicherheitsperspektive, nachstellen kann.

Der erste Schritt ist dabei die Erfassung des ganzen Informationsverbunds. Dies gelingt anhand eines Schichtenmodells, das verschiedene Bausteine vorsieht. Dieses Schichtenmodell kann man sich vorstellen wie ein großes Reservoir an Legobausteinen in verschiedenen Farben und Formen, mit dem man ein großes Gebäude von Innen und Außen nachbaut. Viele, aber nicht alle, Aspekte des Gebäudes spielen eine Rolle. Vor dem Nachbau muss das Gebäude erst einmal gründlich analysiert werden. Während des Nachbaus kommen dann sicher einige Dinge ans Licht, die man vorher nicht wahrgenommen hat und die nicht den Vorstellungen entsprochen haben, diese können dann im richtigen Gebäude geändert werden. Die Anordnung der Bausteine folgt einem Prinzip, das Juristen aus ihren Kodifikationen kennen: Zuerst werden die allgemeinen und abstrahierbaren Bausteine definiert, dann die speziellen.

Nach der Logik der IT-Sicherheitstechnik unterscheidet man zwischen prozessorientierten und systemorientierten Bausteinen. Erstere sind auf alle Prozesse unabhängig von der jeweiligen Technologie anwendbar. Letztere beziehen sich auf bestimmte technische Systeme und sind speziell auf diese ausgerichtet. Dabei sind die Bausteine übergreifend wie folgt gegliedert:

- Prozess-Bausteine
- Sicherheitsmanagement (ISMS)
- Organisation und Personal (ORP)
- Konzepte und Vorgehensweisen (CON)
- Betrieb (OPS)
- Detektion & Reaktion (DER)
- System-Bausteine
- Anwendungen (APP)
- IT-Systeme (SYS)
- Industrielle IT (IND)
- Netze und Kommunikation (NET)
- Infrastruktur (INF)

Diese Bausteine sind jeweils in einem Dreischritt aufgebaut, der mit der Grundrechtsprüfung entfernt vergleichbar ist. Zuerst wird der zu schützende Teil des Informationsverbundes definiert, dies wird als Zielobjekt bezeichnet. Dann werden wichtige typische Gefährdungen für das Zielobjekt beschrieben. Der neue IT-Grundschutz zeichnet sich dadurch aus, dass er alle möglichen Gefährdungen auf 47 Typen zurückführt. Mit den Gefährdungen korrespondieren jeweils bestimmte Anforderungen, also Maßnahmen, die zur Absicherung des Systems notwendig sind. Dabei gibt es verschiedene Kategorien. Basisanforderungen sind die absolut notwendigen Anforderungen, durch die mit geringem Aufwand ein hoher Nutzen für die IT-Sicherheit erzielt wird. Werden neben den Basis- auch die Standardanforderungen erfüllt, entspricht dies dem Stand der Technik. Die Anforderungen mit erhöhtem Schutzbedarf greifen in besonderen Fällen. Hier sind Maßnahmen zu ergreifen, die auf Grund einer Risikoanalyse zu ermitteln sind. Im Rahmen der Anforderungen werden auch die Hauptverantwortlichen genannt und ggf. auch weitere Rollen definiert. Der IT-Grundschutz verwendet die Modalverben „sollen" und „müssen" und ihre jeweilige Negation in ähnlicher Weise wie die verwaltungsrechtliche Ermessenslehre. „Müssen" indiziert eine ausnahmslose Verpflichtung der Erfüllung einer Anforderung. Demgegenüber erlaubt „sollen" begründete Ausnahmen. Solche Ausnahmen können sich insbesondere aus einer Risikoanalyse ergeben. Denn bei den Bausteinen handelt es sich um Typisierungen, die in der Regel anwendbar sind und den Aufwand bei der Absicherung reduzieren. Eine Risikoanalyse, die z.B. auf Grund der hohen Schutzwürdigkeit eines Objekts geboten sein kann, kann allerdings Abweichungen ergeben. Dies ist jeweils im Einzelfall zu prüfen.

2. Leitfaden zur Basisabsicherung und Standards

Der neue „Leitfaden zur Basisabsicherung nach IT-Grundschutz" ist eine Anleitung von weniger als 100 Seiten, die es kleinen und mittleren Unternehmen und Behörden ermöglichen soll, eine grundlegende Absicherung vorzunehmen, ohne sofort alle Anforderungen des IT-Grundschutzes erfüllen zu müssen.[19] Der Leitfaden richtet sich an kleinere oder mittlere Organisationen, die erst am Anfang einer Absicherung stehen. Auch wenn das Schutzniveau nicht an den IT-Grundschutz heranreicht, soll so das Sicherheitsniveau insgesamt angehoben werden.

Demgegenüber ist die Erfüllung der BSI-Standards 200-1, 200-2 und 200-3 anspruchsvoller. Diese Standards erlauben eine Zertifizierung auf der Basis von ISO 27001. Während der BSI-Standard 200-1 beschreibt wie ein erfolgreiches Management System aufgebaut sein kann, gibt der BSI-Standard 200-2 die Methodik des IT-Grundschutzes vor. BSI-Standard 200-3 sieht ein vereinfachtes Verfahren der Risikoanalyse vor, welches dann zum Tragen kommt, wenn die Anforderungen des IT-Grundschutzes kein ausreichendes Sicherheitsniveau versprechen.

3. Stakeholder Beteiligung, insbesondere IT-Grundschutzprofile

Im Laufe der Entwicklung des IT-Grundschutzes hat das *BSI* immer mehr Möglichkeiten geschaffen, betroffene Gruppen in die Fortentwicklung des IT-Grundschutzes zu involvieren. Bereits bei der redaktionellen Erstellung des Bausteins „besteht nun die Möglichkeit, zu kommentieren, Fragen zu stellen oder Inhalte zu ergänzen".[20] Mit dem IT-Grundschutz 3.0 wurde ein neues Kapitel der Akteursbeteiligung eröffnet. Diese ergibt sich bei der Erstellung von sog. IT-Grundschutzprofilen. Deren Ziel ist es, dass Anwendergruppen sich aus den verschiedenen Bausteinen

des IT-Grundschutzes ein typisiertes Sicherheitskonzept schaffen können. In der oben verwendeten Metapher des IT-Grundschutzes als Legobaukasten stellen die Profile eine fertige Bauanleitung dar. Man muss daher keine Konstruktionszeichnung der eigenen Organisation anfertigen, sondern kann sich auf Vorzeichnungen stützen. Die IT-Grundschutzprofile analysieren die Struktur und den Schutzbedarf für eine bestimmte Gruppe von Informationsverbünden, wählen darauf aufbauend IT-Grundschutz-Bausteine aus und beschreiben spezifische Sicherheitsanforderungen und Maßnahmen. Das bedeutet, dass der IT-Grundschutz noch stärker typisiert wird, indem die Bausteine für eine bestimmte Nutzergruppe angepasst werden. Veröffentlicht wurden bereits IT-Grundschutzprofile für Handwerkskammern und Kommunalverwaltungen.

IV. Rechtliche Relevanz

Wie bereits gezeigt, hat der IT-Grundschutz verschiedene Elemente, insbesondere Standards und das IT-Grundschutz-Kompendium. Standards werden in der Literatur entsprechend ihrer Urheber in exekutive, halbstaatliche und privatverbandliche Standards unterteilt.[21] Während frühere Versionen des IT-Grundschutzes exekutivische Standards waren, könnte man auf Grund der vielen Einflussmöglichkeiten der Stakeholder mittlerweile davon ausgehen, dass es sich beim IT-Grundschutz um einen halbstaatlichen Standard handelt. Unabhängig von dieser Einordnung basiert die Befolgung eines Standards grundsätzlich auf Freiwilligkeit. Es handelt sich um eine Form des „Soft Law". Rechtliche Wirkungen entfaltet der IT-Grundschutz damit nur mittelbar. Insofern stellt er eine Möglichkeit dar Zertifizierungspflichten nachzukommen, wo das Gesetz diese ausdrücklich vorsieht. Ferner kann der IT-Grundschutz normkonkretisierende Wirkung haben, wenn das Gesetz IT-Sicherungspflichten vorsieht. Eine wichtige Funktion erfüllt der IT-Grundschutz allerdings auch als Wissens- und Informationsressource, indem er aktuelles Wissen über Informationssicherheit frei verfügbar macht.

Während Pflichten zur Sicherung von IT-Systemen oft allgemein formuliert werden, verlangt das Gesetz an manchen Stellen ausdrücklich eine Zertifizierung der IT-Sicherheit. So erfordert etwa § 6 Abs. 1 Satz 1 HessLStatG[22] sowohl die Sicherheit der personenbezogenen Daten als auch Sicherheit zur statischen Geheimhaltung. Das *VG Gießen* sah durch die Zertifizierung nach IT-Grundschutz beide Voraussetzungen als erfüllt an.[23] Neben der vollen Zertifizierung verpflichten Gesetze auch zur teilweisen Einhaltung des IT-Grundschutzes. So erfordert § 20a Abs. 1 Nr. 5 des FVG Dienstleister zur Aufstellung eines IT-Sicherheitskonzepts nach dem IT-Grundschutz. Mittelbar wirkt der IT-Grundschutz insbesondere bei der Konkretisierung von IT-Sicherheitspflichten. Diese Sicherheitspflichten können aus allen Rechtsbereichen und verschiedenen systematischen Zusammenhängen stammen.[24] Für den Bereich des Verwaltungsrechts sind sie oft in den E-Government-Gesetzen niedergelegt, wie etwa in Art. 11 Abs. 1 des BayEGovG. Gem. § 9 Abs. 2 Satz 3 des SächsEGovG" sind für die staatlichen Behörden die Standards und Kataloge des *BSI* in der jeweils aktuellen Fassung maßgeblich". Andere IT-Sicherheitspflichten finden sich in §§ 13 Abs. 7, 109 TKG, Art. 32 DS-GVO und § 64 BDSG. Im Zivilrecht spielen besonders allgemeine Sicherungspflichten wie § 93 AktG und § 43 GmbHG, ebenso wie vertragliche Nebenpflichten und deliktische Verkehrssicherungspflichten eine Rolle.[25] Die meisten IT-Sicherungspflichten orientieren sich am Stand der Technik unter der Wahrung des Grundsatzes der Verhältnismäßigkeit. Unter dem „Stand

der Technik" versteht man entsprechend der Definitionen des § 3 Abs. 6 BImSchG und des § 3 Nr. 11 WHG dabei Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, welcher praktisch zur Erreichung eines allgemein hohen Schutzniveaus geeignet ist. Im Kontext der meisten IT-Sicherungspflichten wie etwa § 13 Abs. 7 TMG tritt an die Stelle von „Verfahren, Einrichtungen und Betriebsweisen" der Begriff „technische und organisatorische Maßnahmen". Der IT-Grundschutz beschreibt gerade diese technischen und organisatorischen Maßnahmen im Hinblick auf die IT-Sicherheit. Besonders die Differenzierung, die der IT-Grundschutz mittlerweile erreicht hat, kann als Schematisierung, insbesondere bei Verhältnismäßigkeitsprüfungen, erste Anhaltspunkte liefern. So schreibt der Leitfaden zur Basisabsicherung die Mindeststandards auch für kleinere Organisationen vor, während der IT-Grundschutz in seinen Gefährdungsabstufungen bei mittleren und größeren Organisationen einschlägig ist. Umgekehrt können Organisationen auch davon ausgehen, dass sie ihre Sicherheitspflichten auf bestimmte Gefährdungen und Risiken erfüllt haben, wenn sie den Anforderungen des Grundschutzes nachgekommen sind.

Der IT-Grundschutz vermittelt daher auch prospektiv Orientierungswissen, eine für das Rechtssystem zentrale Funktion. Er ist ein gesamtgesellschaftliches Wissensreservoir über Informationssicherheit. Er ist frei im Internet verfügbar und beschreibt sowohl Gefährdungen als auch Maßnahmen. Da etwa für die meisten Anwaltskanzleien IT-Kompetenz und IT-Fähigkeiten nicht im Mittelpunkt ihrer Tätigkeit stehen, profitieren sie in besonderem Maße von den Möglichkeiten des IT-Grundschutzes.[26] Denn wenn das Recht sich in steigendem Maße informationstechnischen Systemen bedient, wird die Sicherheit der Systeme stärker zu einer rechtlichen Frage. Der IT-Grundschutz bietet ein einheitliches Begriffssystem und ist Erkenntnisquelle für Fragen der Informationssicherheit. Als Beispiel hierfür kann etwa ein Beschluss des *BKartA* angeführt werden, in welchem das *BKartA* die Definition von „Man-in-the-middle-Angriffen" unter ausdrücklichem Verweis auf den IT-Grundschutz übernahm.[27] Der IT-Grundschutz könnte als wichtige Ressource der Informationsverwaltung gekennzeichnet werden.[28] Diese Ressource wird besonders deshalb wichtig, weil der technische Fortschritt alle Bereiche der Gesellschaft vor ein manifestes Wissensproblem stellt. Selbst IT-Unternehmen müssen in manchen Fragen aufwendig ermitteln, was der Stand der Technik ist. Dies ist besonders im Lichte neuer Technologien der Fall.

V. Neue Technologien

Technologischer Fortschritt und technische Neuerungen müssen aus der Perspektive des IT-Grundschutzes fortwährend daraufhin untersucht werden, ob sie mit der bestehenden Systematik abgehandelt werden können oder ob der IT-Grundschutz erweitert werden muss. Dementsprechend stellen neue Technologien immer wieder eine große Herausforderung dar. Anhand zweier technologischer Trends soll kurz aufgezeigt werden, wie sich diese im IT-Grundschutz niederschlagen.

1. Das Internet der Dinge

Das Internet der Dinge (IoT) bezeichnet eine technologische Vision der zunehmenden Vernetzung und intelligenten Steuerung

von Gegenständen. Abseits des „Internets der Computer" werden Gegenstände vernetzt, die eine analoge Funktion haben, von der Zahnbürste hin zu Komponenten eines Elektrizitätskraftwerks. Diese technologische Vision wirft in ihrer Umsetzung zahlreiche Rechtsfragen auf,[29] insbesondere auch Fragen der Sicherheit.[30] Darauf reagiert das IT-Grundschutz-Kompendium mit einem Baustein für allgemeine IoT-Geräte.[31] Das *BSI* definiert das Internet der Dinge im Wesentlichen als vernetzte"[32], „intelligente" und „smarte" Gegenstände. Abgegrenzt wird das allgemeine IoT-Gerät von spezielleren Bedien- und Anzeigesystemen und Software- oder Hardwarearchitekturen, insbesondere aber von industriellen Steuerungssystemen, die in entsprechenden Bausteinen über die Industrielle IT abgehandelt werden. Allgemeine IoT-Geräte wurden zuerst in den Blick genommen, weil der IT-Grundschutz immer zuerst an allgemeine Anwendungen mit generellem Anwendungsbereich denkt. Dann werden relevante besondere Systeme in den Blick genommen, etwa das Internet der Dinge im industriellen Kontext.

Durch die Systematik des IT-Grundschutzes wird dabei auch immer besonders deutlich, welche besonderen Gefahren einer bestimmten Technologie innewohnen. Weil bei zuvor erwähnten Gefährdungen konsequent nach oben auf allgemeinere Technologien verwiesen wird, werden die spezifischen Gefährdungen explizit abgehandelt. So zeigt sich, dass im Rahmen von allgemeinen IoT-Geräten nicht mehr nur um den Schutz der Informationssysteme und der darauf verkörperten Daten geht, sondern um die Lebenswelt, in welche sie eingebettet sind. So wird als Gefährdung etwa die Ausspähung der realen Lebenswelt ausgemacht oder aber Schäden, die Dritte erleiden, wenn die Geräte übernommen werden. Bisher haben sich solche Schäden Dritter besonders in sog. DDoS-Attacken materialisiert, daneben ist aber nicht auszuschließen, dass es auch zu anderen konkreten Schäden kommen kann. So gab es bereits mehrere erfolgreiche Cyberattacken auf vernetzte Fahrzeuge.[33] Aus dem IT-Grundschutz lässt sich ablesen, dass die Schäden Dritter eine neue Gefährdungsdimension darstellen. Denn in der neuen Version sind schädliche Seiteneffekte IT-gestützter Angriffe als Gefährdung hinzugekommen.

Eine andere technische Gefährdung sind die sog. „universal plug&play"-Voreinstellungen, die Geräte auch außerhalb des betreffenden Informationsverbunds über das Internet sichtbar und erreichbar machen. Daraus können dann bedeutende Sicherheitslücken für den ganzen Informationsverbund entstehen. Als verpflichtende Einsatzkriterien werden Updatemöglichkeit, Authentisierung und Änderbarkeit codierter Zugangsdaten beschrieben.[34] An diesen Anforderungen lässt sich die Anwenderorientierung des IT-Grundschutzes gut zeigen. Ein Problem, welches auch im Koalitionsvertrag adressiert ist,[35] ist die mangelnde Wartung von IT-Produkten durch Updates um später auftretende Sicherheitslücken zu schließen. Eine solche Wartung ist im IT-Grundschutz vorgesehen. Dabei kann es durchaus zu Spannungen zwischen der Zertifizierung von Informationsverbünden und Produktzertifizierungen kommen. Ein Update kann etwa eine Produktzertifizierung hinfällig machen, insbesondere wenn es um das Betriebssystem geht. Aus der Perspektive eines Informationsverbunds stellt sich die Lage aber umgekehrt dar: Updates sind verpflichtend. Diese Update-Pflicht ist einer der Wege, wie sich der IT-Grundschutz positiv auf das Sicherheitsniveau bei den Herstellern auswirken kann. Denn auch für Produkte mit höherem Sicherheitsniveau gibt es einen Markt, obwohl sie teurer sind als andere Produkte. Das gilt auch für die Pflicht der Veränderbarkeit von Passwörtern. Billigprodukte, die diese Funktionalität nicht bieten, können umfassend gehackt werden, sodass sie entweder ferngesteuert oder anderweitig missbraucht werden können.

Im industriellen Kontext fehlt ein einheitlicher Baustein für IoT-Geräte. Dort sind die Herausforderungen besonders groß, weil es zu einem zunehmenden Verschmelzen der Bürotechnik (Information Technology) mit der Industrietechnik (Operational Technology) kommt.[36] Nach

der Systematik des IT-Grundschutzes sind hier entsprechend der konkreten Architektur des Systems verschiedene Bausteine zu berücksichtigen, daneben sind nicht abgedeckte Risiken zu ermitteln. Dies betrifft die Bausteine

- Allgemeine ICS-Komponente[37],
- Speicherprogrammierbare Steuerung[38],
- Sensoren und Aktoren[39] und
- Maschine[40].

Die vier Bausteine bauen zwar aufeinander auf und sind so anwendbar, verdeutlichen aber einmal mehr, dass Industrieanlagen schwer nach einem einzelnen Katalog abgesichert werden können. Sowohl der in Erstellung befindliche Baustein als auch etwaige Profile können also große Synergieeffekte erzeugen.

2. Künstliche Intelligenz

Künstliche Intelligenz (KI) ist eine Forschungsfrage, die zahlreiche Forschungsergebnisse wie auch eine Subdisziplin der Informatik hervorgebracht hat. KI hat in den vergangenen Jahren bedeutende Fortschritte gemacht und neue technische Möglichkeiten eröffnet. Nach einer Arbeitsdefinition von *Klaus Mainzer* versteht man darunter Systeme, die selbstständig und effizient Probleme lösen können.[41] Im Moment werden dabei insbesondere lernende Systeme in den Blick genommen, die auf der Basis von künstlichen neuronalen Netzen operieren. Die Diskussion innerhalb der Informatik thematisiert die IT-Sicherheit im Bereich der KI bereits intensiv. In Organisationen fehlt dabei aber oft die nötige Sensibilität für dieses Thema. Ein Grund dafür wird auch prominent im IT-Grundschutz angeführt: „Vielfach wird fälschlicherweise davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch produziert werde."[42] Tatsächlich spielen „intelligente Systeme" in der IT-Sicherheit bereits heute eine große Rolle. Um die Chancen und Herausforderung von KI-Anwendungen für die IT-Sicherheit richtig einordnen zu können, ist die Klassifikation Künstlicher Intelligenz als Querschnittstechnologie entscheidend. Das bedeutet, dass KI-Technologien grundsätzlich zweckoffen sind und so auf unterschiedliche Weise in unterschiedlichen Kontexten eingesetzt werden können. Das lässt sich auch sehr gut an der Gliederung des IT-Grundschutzes verdeutlichen, denn hier kann KI auf unterschiedlichen Ebenen vorkommen. KI kann auf der Ebene der zu schützenden Systeme, der Gefahren und der Maßnah-

men relevant werden. Im Hinblick auf die Systeme ist zu beachten, dass KI-Anwendungen bereits viel verbreiteter sind als man denkt. Das zeigt schon das Beispiel der öffentlichen Verwaltung, die etwa bei der Verkehrssteuerung oder in der Steuerverwaltung auf KI-Lösungen setzt.[43] Aber auch das Gefährdungspotenzial von KI-Anwendungen ist mittlerweile als bedeutend einzuschätzen. Das System „Mayhem" der *Carnegie-Mellon-Universität* bewies in Wettkämpfen, dass ein autonomes System selbstständig unbekannte Sicherheitslücken finden kann und sich durchaus auch mit den besten Hackerteams messen kann.[44] Aber auch als Maßnahmen werden KI-Anwendungen verwendet. Schon heute stützt sich die Netzwerksicherheit ganz wesentlich auf Anomalieerkennung, die sowohl im Training der Systeme als auch in der tatsächlichen Überwachung automatisiert abläuft. In einem viel beachteten Aufsatz entwickelte eine *Forschungsgruppe der NATO* eine Referenzarchitektur für einen intelligenten Agenten, der für Verteidigungszwecke eingesetzt werden kann.[45]

Aus der Perspektive des IT-Grundschutzes können bereits einige Fragen der Absicherung von KI-Anwendungen geklärt werden, schließlich handelt es sich dabei auch um informationstechnische Systeme. Auf der Ebene der Maßnahmen etwa sind bereits intelligente Sensoren (IND.2.3) und mit dem Internet der Dinge (SYS. 4.4) „intelligente Geräte" angesprochen. Was die Maßnahmen anbetrifft, finden etwa Angriffserkennungssysteme (Intrusion Detection Systems) mehrfach im IT-Grundschutz Erwähnung.[46] Dennoch werfen KI-Anwendungen einige grundlegende Fragen auf, die auch in der Weiterentwicklung des IT-Grundschutzes eine Rolle spielen werden.[47]

Die besonderen Herausforderungen für die IT-Sicherheit bestehen darin, dass es sich bei KI nach dem heutigen Stand um eine emergente Technologie handelt, und die Auswirkungen auf die IT-Sicherheit sich erst im Laufe der Entwicklung zeigen.[48] So wird heute intensiv an der Validierung aus der Perspektive der IT-Sicherheit geforscht. Dies betrifft insbesondere die technische Ebene, hier soll der IT-Grundschutz jedenfalls das wichtigste Überblickswissen vermitteln. Aus der Perspektive der Organisationssicherheit und des IT-Grundschutzes ist es allerdings von entscheidender Bedeutung insbesondere die Interaktion zwischen Mensch und Maschine in den Blick zu nehmen. Diese werden z.B. relevant bei Spracherkennung und Bilderkennung, denn sie erlauben eine direkte und automatisierte Interaktion der Maschine mit Menschen. Ferner ist zu erwarten, dass insbesondere die Definition der Schadprogramme (G 0.39) noch stärker KI-gestützte Anwendungen berücksichtigt. Dies potenziert die Möglichkeiten von KI-getriebenen IT-Systemen in gleichem Maße wie die daraus entstehenden Sicherheitsanforderungen. Diese beziehen sich dann nicht nur auf die Systemsicherheit, sondern auch auf den Umgang mit der Technik. Diese und weitere Fragen stellen große Herausforderungen für den IT-Grundschutz dar, gleichzeitig bedeuten sie auch die Möglichkeit, KI-Technologien in einem frühen emergenten Stadium entlang der Werte der IT-Sicherheit gesellschaftsverträglich zu erforschen und zu entwickeln. Insofern kann es dem IT-Grundschutz gelingen, nicht nur mit den technischen Entwicklungen Schritt zu halten, sondern diese auch durch Standards mit zu gestalten.

Dr. Christian Djeffal
ist assoziierter Forscher am Alexander-von-Humboldt Institut für Internet und Gesellschaft sowie Gastforscher am Institute for Technology, Society and Law der Universität Zürich.

1 *Hartung/Bues/Halbleib* (Hrsg.), Legal Tech, 2018.
2 S. dazu *Eifert*, Electronic government, 2006; *Heckmann*, in: Heckmann (Hrsg.), Juris PraxisKommentar Internetrecht, 2017.
3 Eine Zusammenfassung des Berichts des US-Kongresses der Vereinigten Staaten bei *Sokolov*, Megahack Equifax' war „absolut vermeidbar", abrufbar unter: https://www.heise.de/security/meldung/Megahack-Equifax-war-absolut-vermeidbar-4259677.html?seite=all.
4 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) v. 17.7.2015, BGBl. I, S. 1324 ff.; Gesetz zur Umsetzung der RL (EU) 2016/1148 des Europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur

Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, BGBl. I, S. 1885 (Nr. 40).

5 RL 2016/1148 v. 6.7.2016 (o. Fußn. 4).

6 *Bundesministerium des Innern*, Cyber-Sicherheitsstrategie für Deutschland, abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile.

7 *Juncker*, State of the Union Address 2016.

8 Die Unterschiede werden zusammengefasst von *Kramer/Meints*, in: Hoeren/Sieber/Holznagel (Hrsg.), Hdb. Multimedia-Recht, Teil 16.5, 39. EL Juli 2014, Rdnr. 15–19; umfassend dargestellt sind sie in der Norm ISO/IEC 27005.

9 *Kilian*, DuD 2007, 49.

10 *Krabbes*, in: Friedel/Spindler (Hrsg.), Zertifizierung als Erfolgsfaktor, 2016, S. 539, 543; *Kilian*, DuD 2007, 49, 52; *Meints*, DuD 2006, 13, 14.

11 Eine Zusammenfassung verschiedener Kritikpunkte bieten *Greveler/Reinermann*, CCZ 2015, 274-281.

12 *Böhmer/Milde*, DuD 2017, 104, 105.

13 Zur Typologie der Standardsetzung s. *Kloepfer*, in: *Schröder/Schulte* (Hrsg.), Hdb. des Technikrechts, 2011, S. 151, 182-186.

14 *Kinast/Schröder*, ZD 2012, 207, 208.

15 *Loomans/Matz*, Wirtschaftsinformatik & Management 6/2014, S. 62, 63.

16 *Greveler/Reinermann*, CCZ 2015, 274-281.

17 *Bundesamt für die Sicherheit in der Informationstechnik (BSI)*, IT-Grundschutz-Kompendium – Edition 2019, abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html, S. 1.

18 S. Legaldefinitionen in § 3 Abs. 6 BImSchG und § 3 Nr. 11 WHG.

19 *Bundesamt für die Sicherheit in der Informationstechnik*, Leitfaden zur Basis-Absicherung nach IT-Grundschutz, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=2.

20 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GS_Drafts/gs_drafts_node.html.

21 S. *Kloepfer* (o. Fußn. 13).

22 Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz – HessLStatG), GVBl. I 1987, S. 67 v. 22.5.1987.

23 *VG Gießen*, B. v. 23.2.2012 – 4 L 4634/11.GI.

24 *Erben*, in: *Holzhauser* (Hrsg.), Interdisziplinäre Aspekte von Compliance, 2011, S. 115, 116; umfassend *Voigt*, IT-Sicherheitsrecht, 2018.

25 *Erben* (o. Fußn. 24), S. 115, 120; *Grünendahl/Steinbacher/Will*, Das IT-Gesetz: Compliance in der IT-Sicherheit, 3. Aufl. 2017, S. 2.

26 *Schröder*, Datenschutzrecht für die Praxis, 2. Aufl. 2016, S. 192.

27 *BKartA*, B. v. 29.6.2016 – B 4-71/10, Sorgfaltspflichten in den Sonderbedingungen für das Online-Banking – Beschluss der Spitzenverbände der Deutschen Kreditwirtschaft, Rdnr. 53.

28 Dazu *Augsberg*, Informationsverwaltungsrecht, 2014.

29 *Bräutigam/Klindt*, NJW 2015, 1137; *Hofmann/Hornung*, in: Engemann/Sprenger (Hrsg.), Internet der Dinge, 2015, S. 205; *Weber/Weber*, Internet of Things, 2010, p. 23 ff.

30 *Weber/Weber* (o. Fußn. 29), p. 41 ff.

31 *BSI*, IT-Grundschutz-Kompendium Final Draft.

32 Vernetzung bedeutet dabei aber nicht, dass die betr. Systeme auch an das Internet angeschlossen sein müssen. Auch ein „Intranet der Dinge" kann also zum Internet der Dinge gehören, s. vertiefend *Bucherer/Uckelmann*, in: Uckelmann/Harrison/Michahelles (Hrsg.), Architecting the Internet of Things, 2011, p. 1.

33 *Maier*, Auto hacken leicht gemacht, abrufbar unter: https://www.computerwoche.de/a/so-gehen-die-auto-hacker-vor,3215159.

34 Baustein SYS4.4.A1.

35 Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land, abrufbar unter: https://www.bundesregierung.de/Content/DE/_Anlagen/2018/03/2018-03-14-koalitionsvertrag.pdf?__blob=publicationFile&v=6.

36 So auch im Baustein IND 1, S. 2.

37 Baustein IND 2.1.

38 Baustein IND 2.2.

39 Baustein IND 2.3.

40 Baustein IND 2.4.

41 *Mainzer*, Künstliche Intelligenz – wann übernehmen die Maschinen?, 2016, S. 3.

42 *BSI*, IT-Grundschutz-Kompendium – Ed. 2019 (o. Fußn. 17).

43 *Djeffal*, in: Mohabbat Kar/Thapa/Parycek (Hrsg.), (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, S. 493, 497 ff.

44 *Daemmrich*, AI and the Challenge of Cybersecurity, abrufbar unter: http://invention.si.edu/ai-and-challenge-cybersecurity.

45 *Kott/Mancini/Théron u.a.*, Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense, abrufbar unter: https://arxiv.org/abs/1803.10664.

46 So z.B. SYS. 1.1.A27, SYS. 1.2.2.A11.

47 In jüngster Zeit gibt es zu diesen Fragen einige Berichte und Einschätzungen, s.*ENISA*, Looking into the crystal ball, 2018.

48 Forschungsfragen und eine Forschungsagenda in dieser Hinsicht formulieren etwa *Dario Amodei, Chris Olah, Jacob Steinhardt* u.a.