SANDRO GAYCKEN / MICHAEL KARGER

Entnetzung statt Vernetzung

Paradigmenwechsel bei der IT-Sicherheit

Datenschutzrecht

Der Trend zur fortschreitenden Vernetzung von IT-Infrastrukturen scheint ungebrochen, Cloud Computing gilt als Zukunftsmodell. Mit dem Computervirus Stuxnet scheint sich jedoch ein Paradigmenwechsel anzubahnen: Angreifer mit militärischem Hintergrund, umfassenden technischen und finanziellen Ressourcen attackieren unerkannt kritische Infrastrukturen und leiten damit die erste Phase des Cyberwarfare ein. Sofern traditionelle Sicherheitsvorkehrungen nicht mehr greifen, muss darüber nachdacht werden, ob kritische Infrastrukturen vom Netz abzukoppeln sind. Diese bis vor kurzem noch undenkbare Option kann unter bestimmten Voraussetzungen auch rechtlich als Ultima Ratio geboten sein.

I. Einführung

Vernetzung ist ein gängiges technisches Paradigma geworden, ein marktwirtschaftlicher und gesellschaftlicher Trend. Alles soll mit Rechnern ausgestattet und untereinander verbunden werden. Das erhöht die Zuverlässigkeit, die Geschwindigkeit und die Flexibilität der Prozesse. Und es spart Geld durch einen der prinzipiellen, mittelbaren Kerneffekte der Informationstechnik – man kann Personal reduzieren. Der Trend zeitigt überall und immer wieder neue Beispiele: Leitwarten zur Steuerung von 50 Kraftwerken über ein einziges Kontrollsystem, Smart Grids und das Cloud Computing sind einige jüngere Phänomene.

Ein Ende dieses Trends zur immer engeren Vernetzung war bislang nicht in Sicht. Das aber könnte sich ändern. Ein neuer Angreifer hat die Informationsgesellschaft betreten: Der militärische Hacker. Er hat Interesse an Infrastrukturen, an Wirtschaftsdaten, an Spionage, an Manipulation und an Sabotage. Er ist fähig dazu, seine Attacken gegen jede Variante der IT-Sicherheit auszuführen. Und er nutzt Vernetzung. Sein Erscheinen könnte eine radikale Trendwende provozieren. Die Entnetzung, der Antagonist zur Vernetzung, könnte schon bald Realität werden.

II. Vernetzung als Gefahr

1. Abhängigkeiten der Informationsgesellschaften

Technisierung produziert Abhängigkeit. Das ist eine bekannte Tatsache. In vielen Bereichen ist die Technik von einer Möglichkeit zu einer Notwendigkeit, zu einer conditio sine qua non geworden. Außerdem werden meist weitere Strukturen zu ihrem erfolgreichen Funktionieren benötigt. Warenaustauschsysteme, Steuerung und Verwaltung, verarbeitende und transportierende Großindustrie sind Beispiele. Eine Technologie evoziert so insgesamt – in der Einstellung auf die neuen Möglichkeiten, der Neubildung der Abläufe und in den umgebenden Komplementärsystemen – eine strukturelle Revolution – und gleichzeitig ein Netz von Abhängigkeiten. In einigen Fällen von Technologien mit hohem Bedarf an weiteren Strukturen sind Rückbildungen damit sehr schwierig. Es entstehen „lock-ins“[1] oder „Pfadabhängigkeiten“,[2] eine Hysterese. Die Strukturgeschichte des technischen Systems wird bedeutsam, indem sie strukturelle Änderungen verstellt.

Diese Geschichte der Evolution von Möglichkeit zu Notwendigkeit sowie von der Koevolution komplementärer Strukturen und entsprechender Pfadabhängigkeiten lässt sich für die vollvernetzte Informationsgesellschaft neu erzählen. Die informationstechnische Unterstützung von Prozessen ist sehr schnell sehr weit vorangeschritten.[3] Eine Strukturrevolution war anhängig. Alle informatisierten Prozesse finden in grundlegend neu strukturierten Formen, mit hohem Informationsaufwand, in hoher Geschwindigkeit und durchgeführt durch weit weniger spezifisch geschultes Personal statt, und sie werden ergänzt durch diverse neue technische und soziale Strukturen.

Diese technosozialen Abhängigkeiten sind für Militärs prinzipiell von hoher Relevanz. Sie suchen nach Abhängigkeiten in Gesellschaften, denn dies sind neuralgische Punkte, um sie zu schwächen und einen externen Willen aufzuzwingen.[4] Damit ist seit kurzem auch die vernetzte Informationstechnik im Visier.[5] Da die Abhängigkeiten hier sehr hoch sind, ist der „Cyberwar“ ein militärisch vernünftiges Szenario. Offene Fragen sind nun, was durch ihn bedroht ist, wie intensiv diese Bedrohung sein wird und wie man sich einrichten kann.

2. Ziele des Cyberwars

Die hohe Informatisierung und Vernetzung der Gesellschaft bieten dem Strategen viele Optionen. Das ist einer der Faktoren, die den Cyberwar militärisch so effizient machen. Besonders interessant sind die Optionen für Spionage und für Sabotage.

a) Spionage

Mit Cyberspionage lassen sich alle geschlossenen Informationen erreichen, die in informationstechnischen Systemen verwaltet werden. Die Komplexität der Systeme hilft dabei, den Angreifer zu verstecken.[6] Und sie ermöglicht die Sabotage der Originaldaten.[7] Die Schäden für die deutsche Wirtschaft durch Spionage sind schwer zu messen. Sie gehen aber bereits jetzt in die Milliarden. Das baldige Erblühen des Cyberwars wird diese bereits schwierige Lage für die Wirtschaft noch einmal drastisch verschlechtern.

b) Sabotage

Sabotage betrifft vor allem Infrastrukturen. Der Begriff der Infrastruktur ist dabei weiter zu verstehen als in seinem üblichen, katalogischen Sinne. Nicht nur Strom, Gas, Wasser, Finanzmärkte, Internet sind hierunter zu rechnen, auch lokale Infrastrukturen wie bestimmte Institutionen, wirtschaftliche Unternehmen, mi-

1 *W.B. Arthur*, „Competing Technologies, Increasing Returns, and Lock-In by Historical Events,“ in: The Economic Journal, 1989, Vol. 99, No. 394.
2 *P.A. David*, „Clio and the Economics of QWERTY,“ in: American Economic Review (American Economic Association) 75 (2), 1985, S. 332–337; s.a. *J. Beyer*, Pfadabhängigkeit, 2006.
3 *M. Castells*, Der Aufstieg der Netzwerkgesellschaft. Teil 1: Der Aufstieg der Netzwerkgesellschaft. 2003.
4 *B. Liddell Hart*, Strategy, 1954.
5 *S. Gaycken*, Cyberwar – Das Internet als Kriegsschauplatz, 2010.
6 *S. N. Pand/Vikram Mangl*, Protecting Data from the Cyber Theft – a Virulent Disease, in: Journal of Emerging Technologies in Web Intelligence, 2010, Vol. 2, No. 2, S. 152–155.
7 *Philip H. J. Davies*, „Intelligence, information technology, and information warfare“, in: Annual Review of Information Science and Technology, 2001, Vol. 36, Issue 1, S. 312–352.

litärische Basen oder sogar militärisches Gerät sollten so verstanden werden. Werden sie abgeschaltet, sind die durch sie gesicherten Prozesse verunmöglicht. Das ist häufig schnell katastrophal. Eine Abschaltung der Stromversorgung produziert auf Grund der dichten Abhängigkeit von Strom – alle anderen Infrastrukturen benötigen ihn – bereits nach 24 Stunden einen Abfall aller Leistungen.[8] Kurz darauf setzen katastrophale Zustände ein. Cyberangriffe auf kritische Infrastrukturen[9] sind auf Grund dieser mangelhaften Kompensationsmöglichkeiten besonders gefährlich. Sie können flächendeckende und dauerhafte Schäden anrichten.[10]

3. Die Relativität der IT-Sicherheit

Es stellt sich damit die Frage, ob Informationen und Infrastrukturen technisch geschützt werden können. Wie also steht es um die IT-Sicherheit? Sie behauptet, rudimentären Schutz zu bieten. Allerdings orientieren sich diese Behauptungen an den traditionellen Bedrohungen. Das waren abenteuerlustige Teenager und auf meist kleine Betrügereien ausgerichtete Cyberkriminelle.

Der neue militärische Angreifer verändert jedoch das gesamte Wertespektrum der IT-Sicherheit. Sicherheit ist relativ. Was bislang als sicher galt, muss gegenüber den mit wissenschaftlichem Know-how, mit hohen Ressourcen, mit großen Verbänden verschiedenster Experten und mit Nachrichtendiensten und all ihren Möglichkeiten operierenden Militärs neu evaluiert werden.[11] Der bisherige Stand aus Forschung und Erfahrung: Gegen diese außergewöhnlich starken Hacker existieren keine Schutzkonzepte.[12] Eine Einsicht, zu der unlängst auch das US-Militär gelangt ist. Cyberdefense wird dort nicht mehr als realisierbares Paradigma erachtet.[13]

4. Strafverfolgung und militärische Gegenschläge: Das Problem der mangelnden „Attribution"

Eine andere Variante des Schutzes wäre noch denkbar: Protektion durch den Staat. Einem potenziellen Angreifer müssen zur Abschreckung Strafverfolgung oder militärische Gegenschläge angedroht werden.

Dieses Abschreckungskonzept funktioniert jedoch im Cyberwar ebenfalls nicht. Hier kommt das sog. „Attributionsproblem" zum Tragen: Ein Cyberangreifer kann prinzipiell nicht identifiziert werden. Für viele Akteure ist dies eine nur schwer akzeptable Einsicht. Aber sie ist zwingend.[14] Denn ein Cyberangreifer hinterlässt keine Spuren, insbesondere dann nicht, wenn Nachrichtendienste im Spiel waren.[15] Schutz durch den Staat ist also im Cyberwar ebenfalls keine Option. Auch dies wird von führenden Militärs inzwischen anerkannt. Wie *William J. Lynn*, III., U.S. Deputy Secretary of Defense, sagt: „The bottom line is that we have to shift our cyber defence paradigm from assured retaliation to denial of benefit".[16]

Der Mangel an Attribution ist auch auf Grund einer weiteren damit eröffneten Option problematisch. Ein Cyberkrieger kann auch vollkommen unabhängig von konkreten Konflikten Operationen durchführen, um einen Gegner langfristig zu schwächen. Auch in Friedenszeiten muss also mit Angriffen gerechnet werden.

5. Paradigmenwechsel durch Stuxnet

Die vorstehenden Ausführungen wären bis vor kurzem hypothetisch gewesen. In der Diskussion wurde bislang zuweilen darauf verwiesen, dass Gefährdungen schlicht behauptet würden und Bedrohungspotenziale in hohem Maße prognostischer Natur seien.[17] Inzwischen gibt es allerdings einen eindrücklichen ersten Fall.

Im Sommer 2010 wurde mit Stuxnet ein Computervirus identifiziert, der offensichtlich für teils offene, teils automatisierte Angriffe auf Industriesteuersysteme der Fa. *Siemens* entwickelt wurde. Auf Grund der technischen Eigenschaften von Stuxnet wird ein außerordentlicher Aufwand vermutet.[18] Stuxnet ist so der erste offen bekannte, mit Sicherheit militärisch produzierte Hackerangriff der Geschichte. Er beweist das Interesse der Militärs an Infrastrukturen und Industrie, ihre Fähigkeiten und die systemischen Probleme des Schutzes.

Neben der trotz neuer Hinweise noch sehr spekulativen Interpretation eines gezielten Angriffs auf den Iran[19] weisen die technischen und der taktischen Merkmale vor allem auf eine Nutzung von Stuxnet als Waffentest. Dies ist sicherheitspolitisch bedeutsamer als eine weitere Facette des Irankonflikts. Denn es indiziert, dass diese Waffen inzwischen existieren, dass sie hochwirksam sind und dass möglicherweise weitere Tests folgen werden. Auch die *Europäische Agentur für Netz- und Informationssicherheit* (*ENISA*) hat Stuxnet als bemerkenswert herausgestellt und spricht von einem „Paradigmenwechsel" in der IT-Sicherheit. Die derzeitig geltende Philosophie zum Schutz kritischer Infrastrukturen müsse grundlegend überdacht werden.[20]

III. Entnetzung als technisch-organisatorisch gebotene Lösung

Die militärische Interessenlage, die Unmöglichkeit des Schutzes durch das klassische Instrumentarium der IT-Sicherheit und die Attacke durch Stuxnet führen bei vielen Akteuren zu Verunsicherung. Es muss dringend gehandelt werden, ohne dass konventionelle Konzepte in Anschlag gebracht werden könnten. Dabei ist die Konsequenz letztlich einfach: Der Ist-Zustand lässt sich nicht nachträglich retten. Er kann nicht länger beibehalten werden.

Die unter Risiko stehenden Systeme müssen neu konzipiert werden. Absolute Sicherheit wird sich nicht erreichen lassen. Aber relative Sicherheit lässt sich entwickeln, wenn für die potenziellen militärischen Angreifer die Kosten maximiert werden und der Nutzen minimiert wird. Dazu gibt es zwei Wege. Um die Kosten zu maximieren, müssen neue und revolutionäre Konzepte für IT-Sicherheit entwickelt werden.[21] Die Sicherheit der Daten muss von Beginn jedes Entwicklungsprojekts an tief in jedes IT-gestützte System eingebaut werden, die Software muss weniger komplex, funktional schmaler und in ihrer Codebasis reduziert werden.

---

8 Vgl. *J. Birkmann/C. Bach/S. Guhl/M. Witting/T. Welle/M. Schmude*, State of the Art der Forschung zu kritischen Infrastrukturen am Beispiel Strom/Stromausfall, 2010, abrufbar unter: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_2.pdf.

9 Zum Begriff der kritischen Infrastrukturen s.u. IV.2.

10 *S. Gaycken/C. Demchak*, Security Resilience in the Emerging Global Socio-Technical Infrastructure, in: Journal of Contingencies and Crisis Management – JCCM, i.E.

11 *S. Gaycken/D. Talbot*, „Aufmarsch im Internet", in: Technology Review, 2010.

12 Vgl. etwa *M.C. Libicki*, Cyberdeterrence and Cyberwar, 2010.

13 Abrufbar unter: http://www.af.mil/shared/media/document/AFD-100727-053.pdf.

14 Vgl. auch *S. Gaycken*, The Necessity of (Some) Certainty – A Critical Remark Concerning Matthew Sklerov's Concept of „Active Defense", in: Journal of Military and Strategic Studies, 2010, Vol. 12, No. 2.

15 Vgl. *W.A. Owens/K.W. Dam/H.S. Lin*, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, 2010.

16 Abrufbar unter: http://www.securitydefenceagenda.org/Portals/7/2010/Events/Lynn/Lynn_Report.pdf.

17 S. etwa *Möllers/Pflug*, in: Kloepfer (Hrsg.) Schutz kritischer Infrastrukturen, S. 47.

18 S. hierzu etwa http://de.wikipedia.org/wiki/Stuxnet.

19 Etwa in der FAZ abrufbar unter: http://www.faz.net/s/RubCEB3712D41B64C3094E31BDC1446D18E/Doc~E8A0D43832567452FBDEE07AF579E893C~ATpl~Ecommon~Scontent.html.

20 *ENISA*, Press Release v. 7.10.2010, abrufbar unter: http://www.enisa.europa.eu.

21 Dieses Konzept einer „Hochsicherheits-IT" wird bald einer der zukünftigen Forschungsschwerpunkte an der *FU Berlin* werden.

Allerdings sind der Erhöhung der Kosten systembedingt enge Grenzen gesetzt. Es muss also auch dringend der Nutzen minimiert werden. Hier hilft nur der Abbau der Technik. Denn das, was die Angriffe auf die Rechnersysteme so attraktiv macht, sind die Kernfunktionen der vernetzten IT selbst: zentralisierte Steuerungen und Verwaltungen. Dies ist also der Auftritt der Entnetzung. Entnetzung bedeutet: Wichtige Rechner müssen vom Netz. Nur kleine, interne und physisch streng kontrollierte Netzwerke dürfen betrieben werden. Systeme müssen möglichst individuell, ohne technische Standards und auf keinen Fall interoperabel konzipiert werden. Außerdem sollte insgesamt wesentlich weniger IT zur Steuerung kritischer Prozesse oder zur Verwaltung kritischer Daten genutzt werden, wenn dies auch durch Personal oder andere Mechanismen erledigt werden kann.

Dies sind klare Folgerungen, die zwar radikal und teuer sind, aber unumgänglich sein werden. In den USA werden sie bereits umgesetzt. Die *Comprehensive National Cybersecurity Initiative* schrieb bereits vor Jahren die Verringerung der Verbindungen zwischen Behörden und externen Netzen auf die spektakuläre Zahl von insgesamt 100 fest.[22] Das ist eine Reduzierung auf unter 1,5% der Verbindungen im Vergleich zum bisherigen Stand, in dem bereits jede Verbindung auf ihre Sinnhaftigkeit geprüft war.

IV. Entnetzung als rechtlich gebotene Option zum Schutz kritischer IT-Infrastukturen

1. Vorrang der Prävention

Cyberwar-Angriffe sind dadurch gekennzeichnet, dass sich der Angreifer in aller Regel nicht ermitteln lässt. Das Problem der fehlenden Attribution bewirkt, dass einer Drohung mit reaktiven Maßnahmen nur geringe Abschreckungswirkung zukommt. Dies gilt zum einen für die Strafverfolgung, die bereits bei der „traditionellen" internationalen Internetkriminalität auf Schwierigkeiten stößt.[23] Jenseits des Strafrechts werden im Zusammenhang mit Cyberwar-Attacken auch das Recht auf Selbstverteidigung des Staates sowie ein Recht des Staats zu Präventivschlägen bei unmittelbar bevorstehenden Anschlägen („imminent threat") diskutiert.[24] Aber diese Überlegungen machen nur Sinn, wenn der Angreifer überhaupt identifizierbar ist.

Dementsprechend ist im Folgenden das Augenmerk vorrangig auf den Präventivbereich zu richten. Im Hinblick auf kritische IT-Infrastrukturen ist hier das Recht der IT-Sicherheit genauer zu betrachten. Maßgebliche Elemente der Prävention sind vor allem die Planung, Implementierung und fortlaufende Aktualisierung einer den Sicherheitsanforderungen entsprechenden Netz- und Systeminfrastruktur, sowie einer Notfallplanung[25] für den Fall eines Angriffs.

2. Kritische Infrastrukturen

a) Begriff

Der Begriff der „kritischen Infrastruktur" hat sich mittlerweile als juristische Kategorie etabliert.[26] Kritische Infrastrukturen sind Einrichtungen, Anlagen, Dienste und Systeme, auf die Staat und Gesellschaft existentiell angewiesen sind und deren Ausfall bzw. Störung zu gravierenden Schäden für das Gemeinwesen, Wirtschaft und Bevölkerung sowie für den Einzelnen führen würde.[27] Hierbei ist es unerheblich, ob die Infrastruktur privat oder öffentlich betrieben wird.[28]

In aller Regel sind IT-Infrastrukturen auf Grund ihres Vernetzungsgrads und der Folgen einer Störung ebenfalls kritische Infrastrukturen.[29] Teilweise wird hierfür auch der Begriff „Kritische Informationsinfrastrukturen" verwendet.[30]

Die *Bundesregierung* hat mit dem nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) drei strategische Ziele vorgegeben: Prävention, Reaktion und Nachhaltigkeit. Das Ziel Prävention soll durch das Etablieren von Schutzvorkehrungen in Verwaltungen und Unternehmen erreicht werden.[31] Die Erreichung der Ziele soll durch einen Umsetzungsplan für die *Bundesverwaltung* (UP Bund), einen Umsetzungsplan für die kritischen Infrastrukturen (UP KRITIS) und ggf. weitere Umsetzungspläne sichergestellt werden.[32]

Das *Bundesamt für die Sicherheit in der Informationstechnologie* (*BSI*) zählt u.a. folgende Sektoren zu den kritischen Infrastrukturen und benennt die jeweils zugehörigen kritischen IT-Systeme:[33]

- Transport und Verkehr (Luftfahrt, Seeschifffahrt, Bahn, Nahverkehr, Binnenschifffahrt, Straße, Postwesen): Leitstellen, Prozessleittechnik, Logistikmanagement, Verkehrsmanagement, Verkehrssicherheit, Navigation.
- Energie (Elektrizität, Kernkraftwerke, Gas, Mineralöl): Steuerung und Regelung der Energieerzeugereinrichtungen, von Einrichtungen der Energieübertragung und der Energieverteilung.
- Informationstechnik und Telekommunikation.
- Finanz-, Geld- und Versicherungswesen (Banken, Versicherungen, Finanzdienstleister, Börsen): Sicherheit der Kommunikation innerhalb und zwischen den Instituten, branchenspezifische Datenverarbeitungsprogramme, bargeldloser Zahlungsverkehr, Interbankenverkehr, Abrechnungssysteme.
- Versorgung (Gesundheit, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittelversorgung, Wasserversorgung, Entsorgung): Einsatzleitzentralen, Kommunikationsverbindungen, Datenbanken, Krankenhausmanagement, technische Leitstellen und Steuerungseinrichtungen, Medizintechnik.
- Behörden, Verwaltung und Justiz (Regierung, Behörden, Verwaltung, Behörden und Organisationen mit Sicherheitsaufgaben, Bundeswehr): Gesicherte Kommunikation, spezifische Informationssysteme, Datenbanken, Leitstellen und Lagezentren.

b) Verteilung der kritischen Infrastrukturen in Deutschland

Etwa 80% der kritischen Infrastrukturen in Deutschland befinden sich in privater Hand,[34] 20% sind dem öffentlich-rechtlichen Sektor zuzuordnen. Die Aufgabe des Schutzes kritischer Infrastrukturen stellt sich trotz der unterschiedlichen Verteilung für Staat und für private Unternehmen in gleicher Weise. Dies führt zu einer faktischen Verantwortungsteilung,[35] ohne dass damit allerdings etwas über die rechtliche Zuordnung der Verantwortlichkeiten ausgesagt ist. Aus der Aufteilung wird aber deutlich, dass im Hinblick auf Sicherheitsvorkehrungen nicht al-

22 Abrufbar unter: http://www.dhs.gov/files/programs/gc_1234200709381.shtm.
23 Zur „klassischen" Internetkriminalität *Gercke*, MMR 2008, 291.
24 Weiterführend *Schmidt-Preuss*, in: Kloepfer (o. Fußn.17), S. 79 ff.
25 Hierzu *Steger*, CR 2007, 137.
26 *Schmidt-Preuss* (o. Fußn. 24), S. 67.
27 Vgl. *Schmidt-Preuss* (o. Fußn. 24); s.a. die Definition in Art. 2a) der RL 2008/114/EG v. 8.12.2008, ABl. EG Nr. L 345, S. 75.
28 *Möllers/Pflug* (o. Fußn. 17), S. 47, 52.
29 *Möllers/Pflug* (o. Fußn. 17).
30 S. § 3 Abs. 1 Nr. 15 BSIG; Mitt. der *Kommission* über den Schutz kritischer Informationsinfrastrukturen „Schutz Europas von Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität v. 30.3.2009, KOM(2009) 149 endg.
31 *Helmbrecht*, in: Kloepfer (o. Fußn. 17), S. 39, 43.
32 *Helmbrecht* (o. Fußn. 31), S. 43.
33 Abrufbar unter: https://www.bsi.bund.de/cln_183/DE/Themen/KritischeInfrastrukturen/EinfuehrungundUeberblick/KRITISSektoren/kritissektoren_node.html.
34 *Schäuble*, in: Kloepfer (o. Fußn. 17), S. 21, 24.
35 *Kloepfer*, in: Kloepfer (o. Fußn. 17), S. 9, 17.

leine nur der Staat, sondern maßgeblich auch der privatwirtschaftliche Sektor gefordert ist.

3. Rechtlicher Rahmen des Präventivschutzes kritischer IT-Infrastrukturen

a) EU-Ebene

Der präventive Schutz kritischer Infrastrukturen ist Gegenstand zahlreicher Initiativen der EU. Auf der Ebene der Rechtsetzung ist etwa die Richtlinie des *Rates* über die Ermittlung und Ausweisung kritischer Infrastrukturen aus dem Jahr 2008[36] zu nennen. Auf der Aktionsebene ist u.a. die Mitteilung der *Kommission* über den Schutz kritischer Informationsinfrastrukturen „Schutz Europas von Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität"[37] relevant. Auf operativer Ebene ist die *ENISA* zu erwähnen, die allerdings nur in beratender und informierender Funktion tätig ist und keine Vollzugsaufgaben ausübt.[38] Insgesamt liegt die Kernkompetenz für den Schutz kritischer IT-Infrastrukturen jedoch bei den Mitgliedstaaten, weshalb an dieser Stelle auf den EU-rechtlichen Rahmen nicht vertieft eingegangen werden soll.[39]

b) Recht der IT-Sicherheit in Deutschland

Der präventive Schutz kritischer IT-Infrastrukturen ist dem Recht der IT-Sicherheit zuzuordnen. Hierbei handelt es sich um eine heterogene Rechtsmaterie, die sowohl öffentlich-rechtliche als zivilrechtliche Normen mit unterschiedlichem Regelungsgehalt umfasst, deren gemeinsamer Nenner die Gewährleistung von Sicherheit in der Informationstechnik ist.[40] Eine gesetzliche Definition der IT-Sicherheit findet sich in § 2 Abs. 2 BSIG. Dort heißt es: „Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder

2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen."

Im Kontext von Cyberattacken sind die Schutzziele der Verfügbarkeit und Unversehrtheit von IT-Systemen relevant. Verfügbarkeit meint den Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung.[41] Aus dem Kriterium der Verfügbarkeit resultiert der Einsatz von Schutzprogrammen, Firewalls und vergleichbaren Sicherheitsvorrichtungen.[42]

Ein einheitliches Gesetz, das sämtliche Aspekte der IT-Sicherheit regelt, gibt es nicht.[43] Die Rechtsmaterie ist vielmehr stark zersplittert. Dass hierdurch der Problematik nur unzureichend Rechnung getragen wird, liegt auf der Hand. Deshalb erscheint es sinnvoll, den Vorschlag von *Spindler* aufzugreifen und über ein übergreifendes IT-Sicherheitsgesetz nachzudenken.[44]

c) Öffentlich-rechtliche Regelungen

Öffentlich-rechtliche Ansätze zu den Anforderungen an die IT-Sicherheit finden sich vor allem im TK-Recht, im Datenschutzrecht sowie im Wirtschaftsaufsichtsrecht. Im Folgenden soll mit § 109 TKG, § 9 BDSG und § 25a KWG auf die wichtigsten Normen und auf das in allen diesen Normen wiederzufindende Grundprinzip des Angemessenheitsvorbehalts eingegangen werden.

■ § 109 TKG

Gem. § 109 TKG[45] hat der Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zu treffen, um die im Gesetz genannten Schutzgüter zu schützen. Als technische Vorkehrungen sind alle Maßnahmen zu verstehen, die sich auf die Funktionsweise der technischen Einrichtung beziehen. Bei der Planung sind sämtliche in Betracht kommende Risiken einzubeziehen.[46]

Nach § 109 Abs. 2 Satz 4 TKG sind die Vorkehrungen und Maßnahmen angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht. Zwischen dem Aufwand, den der Verpflichtete zu treffen hat, und dem Nutzen für die Allgemeinheit darf kein Missverhältnis bestehen.[47]

Welche Schutzmaßnahmen angemessen sind, muss anhand des Einzelfalls entschieden werden; hierbei ist der Stand der technischen Entwicklung relevant.[48] Zu berücksichtigen ist weiter, dass es eine absolute Sicherheit nicht geben kann und eine extrem hohe Sicherheit für die Allgemeinheit oft nicht bezahlbar ist.[49] Allerdings dürfen Sicherheitsanforderungen nicht alleine an Rentabilitäts- oder Wirtschaftlichkeitsbetrachtungen festgemacht werden.

Zu den bislang üblichen und als angemessen betrachteten technischen Vorkehrungen zählen Firewalls,[50] Überbrückungsaggregate,[51] der Betrieb redundanter Systeme[52] sowie die Überwachung des eigenen Netzes mittels Intrusion-Detection-Systemen.

■ § 9 BDSG

Nach § 9 BDSG haben die verantwortlichen Stellen technische und organisatorische Maßnahmen zu treffen und Sicherheitsmaßnahmen zu ergreifen. Durch § 9 BDSG wird die IT-Sicherheit „in den Dienst" des Datenschutzes gestellt.[53]

Nach § 9 Abs. 2 BDSG sind nur solche Maßnahmen erforderlich, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Dies bedeutet allerdings nicht, dass auf erforderliche Maßnahmen von Vorneherein wegen des zu hohen Aufwands verzichtet werden darf.[54] Welche Maßnahmen konkret zu treffen sind, hängt von einer Analyse des Gefahrenpotenzials ab. Hierbei ist die Analyse ein dauerhafter Prozess, der eine ständige Beobachtung der Risiken erforderlich macht.[55] Dabei ist jedenfalls auch der aktuelle Stand der Technik zu berücksichtigen.[56]

Die Anlage zu § 9 BDSG konkretisiert die entsprechenden Maßnahmen. Hierzu gehört nach Ziff. 2 die Verhinderung der unbe-

36 RL 2008/114/EG des Rates v. 8.12.2008, ABl. EG Nr. L 345, S. 75.
37 Mitt. der *Kommission* (o. Fußn. 30).
38 S. VO (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates v. 10.3.2004 zur Errichtung der *Europäischen Agentur für Netz- und Informationssicherheit*, ABl. Nr. 77 v. 13.3.2004, S. 1.
39 S. hierzu und zu völkerrechtlichen Fragen *Schmidt-Preuss* (o. Fußn. 24), S. 69 ff.
40 Vgl. *Heckmann*, MMR 2006, 280, 281.
41 *Heckmann* (o. Fußn. 40).
42 Vgl. *Heckmann* (o. Fußn. 40).
43 *Schmidl*, NJW 2010, 476, 477.
44 *Spindler*, MMR 2008, 7.
45 Auf die Sicherheitsanforderungen des PTSG wird vorliegend nicht weiter eingegangen; s. hierzu *Spindler*, in: Kloepfer (o. Fußn. 17), S. 85, 91 f.
46 *Bock*, in: Beck'scher TKG-Komm., 3. Aufl. 2006, § 109 TKG Rdnr. 19.
47 Vgl. *Bock* (o. Fußn. 46), Rdnr. 21.
48 *Spindler* (o. Fußn. 45), S. 90.
49 *Bock* (o. Fußn. 46).
50 *Bock* (o. Fußn. 46).
51 *Spindler* (o. Fußn. 45) m.w.Nw.
52 *Spindler* (o. Fußn. 45) m.w.Nw.
53 *Spindler* (o. Fußn. 45), S. 94.
54 *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 9 Rdnr. 7.
55 Vgl. *Spindler* (o. Fußn. 45), S. 95.
56 *Spindler* (o. Fußn. 45).

fugten Nutzung (Zugangskontrolle) sowie die Verhinderung unbefugter Veränderung oder Entfernung von Daten (Zugriffskontrolle). Die Verfügbarkeitskontrolle gem. Nr. 7 wurde als neue Sicherungsverpflichtung in den Katalog aufgenommen. Sie zielt auf den Schutz vor zufälliger Zerstörung ab.

Über § 11 Abs. 2 Satz 2 Nr. 3 BDSG gelten die vorgenannten Anforderungen explizit auch für die Auftragsdatenverarbeitung, also für Szenarien wie das Application Service Providing (ASP), das Outsourcing und das Cloud Computing. Nach § 11 Abs. 2 Satz 5 BDSG hat sich der Auftraggeber vor Erteilung des Auftrags und auch später regelmäßig davon zu überzeugen, ob die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden; das Ergebnis der Überprüfung hat der Auftraggeber zu dokumentieren. Diese Vorschrift macht deutlich, dass sich der Auftraggeber der Verantwortung für das Thema IT-Sicherheit nicht durch eine Auslagerung an einen Dritten entledigen kann.[57]

§ 25a KWG

Für Kreditinstitute ist die Informationstechnologie eine der wesentlichen Geschäftsgrundlagen; ein Ausfall der elektronischen Datenverarbeitung kann zu einem sofortigen Zusammenbruch des Instituts führen.[58] Dies gilt umso mehr, als mit fortschreitender Arbeitsteilung und Vernetzung mit Geschäftspartnern, Kunden, Börsen und anderen Institutionen (z.B. Aufsichtsbehörden) die Abhängigkeit von den IT-Systemen stark zugenommen hat.[59]

§ 25a KWG sieht die Verpflichtung zu einem angemessenen und wirksamen Risikomanagement vor. § 25a Abs. 1 Satz 2 Nr. 2 KWG setzt u.a. eine angemessene technisch-organisatorische Ausstattung des Instituts voraus und schließt spezifisch für IT-Systeme die Festlegung eines angemessenen Notfallkonzepts ein. Sofern wesentliche Aktivitäten und Prozesse auf ein anderes Unternehmen ausgelagert werden, sind nach § 25a Abs. 2 KWG ebenfalls angemessene Vorkehrungen zu treffen, um übermäßige zusätzliche Risiken zu vermeiden.[60]

Die Angemessenheit der Sicherheitsvorkehrungen ist anhand der vorgegebenen aufsichtsrechtlichen Ziele der Sicherung der anvertrauten Vermögenswerte, der Sicherung der ordnungsgemäßen Durchführung der Bankgeschäfte und Finanzdienstleistungen sowie der Vermeidung von Nachteilen für die Gesamtwirtschaft durch Missstände im Kredit- und Finanzdienstleistungswesen zu beurteilen.[61]

Die *Bundesanstalt für Finanzdienstleistungsaufsicht* hat mit einem Rundschreiben die Anforderungen nach § 25a Abs. 1 und Abs. 2 KWG i.S.v. Mindestanforderungen an das Risikomanagement (MaRisk) interpretiert.[62] Unter AT 7.1 ist spezifisch für die IT-Sicherheit gefordert, dass IT-Systeme (Hardware- und Softwarekomponenten) und die zugehörigen IT-Prozesse die Integrität, Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherzustellen haben. Zu diesen Zwecken ist bei der Ausgestaltung der IT-Systeme oder der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Als „gängige Standards" kommen insbesondere die BSI-Standards für den IT-Grundschutz in Betracht.[63] Nach AT 7.3 ist ein Notfallkonzept zu erstellen.

Für Outsourcing-Szenarien sieht AT 9 Nr. 2 eine Risikoanalyse dahingehend vor, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind. Bei wesentlichen Änderungen der Risikosituation ist die Risikoanalyse anzupassen.

Nach AT 2.2 hat sich die Geschäftsleitung regelmäßig und anlassbezogen einen Überblick über die Risiken des Instituts zu verschaffen. Nach AT 4.2 ist eine Risikostrategie festzulegen.

Angemessenheitsvorbehalt

Allen vorgenannten Normen (§ 109 TKG, § 9 BDSG und § 25a KWG) ist gemeinsam, dass sie eine – zumindest implizite – Verpflichtung zur fortlaufenden Analyse der Gefährdungssituation vorsehen und für den Fall, dass auf Grund der gewonnenen Erkenntnisse eine Reaktion erforderlich ist, Handlungspflichten auferlegen. Allerdings stehen entsprechende Maßnahmen unter einem Angemessenheitsvorbehalt. Angemessenheit bedeutet, dass die Maßnahmen geeignet, erforderlich und verhältnismäßig sein müssen.

Eine Entnetzung kommt unter dem Gesichtspunkt der Erforderlichkeit nur für kritische IT-Infrastrukturen in Betracht. Diesbezüglich ist zu prüfen, ob den drohenden Gefahren nicht auch mit anderen Mitteln begegnet werden kann als mit einer Entnetzung von Systemen. In Betracht kommt die Optimierung traditioneller Sicherheitsvorkehrungen sowie die redundante Auslegung der Systeme, sodass im Angriffsfall keine Daten verloren gehen und ein schneller Wiederanlauf möglich ist. Bei der Verhältnismäßigkeitsprüfung ist abzuwägen, ob der Schutz der betreffenden Schutzgüter Vorrang vor anderen schutzwürdigen Belangen hat. Hierbei ist zum einen zu berücksichtigen, dass auch im Hinblick auf überragend wichtige Rechtsgüter keine absolute Sicherheit geschaffen werden kann. Zum anderen ist zu bewerten, dass eine Entnetzung auch zu einer Destabilisierung bestehender Infrastrukturen führen kann, bewährte Prozesse und Geschäftsmodelle in Frage stellt und getätigte Investitionen entwertet. Hieraus folgt, dass allenfalls eine schrittweise, in einem ausreichenden Zeitraum zu bewerkstelligende Entnetzung sachgerecht sein kann. Die Kosten der Maßnahmen sind ebenfalls zu berücksichtigen; dieser Gesichtpunkt hat aber jedenfalls dann in den Hintergrund zu treten, wenn die Maßnahme für den Schutz wichtiger Schutzgüter unumgänglich ist.[64] Insgesamt stellt die Entnetzung damit die Ultima Ratio aller Sicherheitsvorkehrungen dar.

d) Zivilrechtliche Regelungen zur IT-Sicherheit in Unternehmen

Im erörterten Kontext stehen die Pflichten in Bezug auf das IT-Risk-Management i.R.d. Unternehmensorganisation im Vordergrund. Für nahezu alle kommerziellen Nutzer von IT-Infrastrukturen können Pflichten verallgemeinert werden, die sich aus allgemeinen handels- und gesellschaftsrechtlichen Pflichten ableiten.[65] Die IT-Sicherheit ist ein maßgeblicher Aspekt der IT-Compliance.[66]

Früherkennung von Risiken durch Risk-Management

Nach § 91 Abs. 2 AktG ist der Vorstand einer Aktiengesellschaft verpflichtet, geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Verpflichtung erschöpft sich nicht in der bloßen Früherkennung, sondern erstreckt sich auf die Einführung und Aufrechterhaltung von Risiko-Vermeidungsstrategien. Hier-

57 S. *Niemann/Paul*, K&R 2009, 444, 450.
58 *Braun*, in: Boos/Fischer/Schulte-Mattler, Kreditwesengesetz, 3. Aufl. 2008, § 25a KWG Rdnr. 455.
59 *Braun* (o. Fußn. 58).
60 Hierzu *Gennen/Schreiner*, CR 2007, 757.
61 *Braun* (o. Fußn. 58), Rdnr. 456.
62 Rundschreiben 15/2009 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk; Geschäftszeichen BA54-FR 2210-2208/0001 v. 14.8.2009.
63 *Spindler* (o. Fußn. 45), S. 97.
64 In diesem Zusammenhang werden bei einer Inanspruchnahme Privater Entschädigungspflichten diskutiert; vgl. *Möllers/Pflug* (o. Fußn. 17), S. 63 f.
65 *Spindler* (o. Fußn. 45), S. 110.
66 *Nolte/Becker*, IT Compliance, BB Special 5 zu BB 2008, Heft 25, S. 23.

aus wird gefolgert, dass ein Unternehmen nicht nur eine angemessene IT-Ausstattung mit zweckbezogenen adäquaten IT-Systemen unterhalten muss, sondern auch den sicheren und zuverlässigen Betrieb dieser IT-Systeme zu gewährleisten hat.[67] Die Anforderungen im Einzelnen lassen sich weitgehend aus den Branchenstandards und dem Stand der Technik ableiten.[68] Das Risk-Management gehört nicht nur in Aktiengesellschaften, sondern auch in Gesellschaften mit anderen Rechtsformen zu den Geschäftsführerpflichten. Dies gilt namentlich für die GmbH gem. § 43 GmbHG, wobei hier je nach Zuschnitt der jeweiligen Gesellschaft (kleine und mittlere Unternehmen) zu differenzieren ist.[69]

■ Reaktion auf erkannte Risiken

Auf erkannte Risiken ist angemessen zu reagieren; für den Bereich der Aktiengesellschaft gelten diesbezüglich die §§ 76, 93 AktG.[70] Die §§ 91, 93 AktG enthalten zwar kein konkretes Pflichtenprogramm, das den Verantwortlichen als Leitlinie dienen könnte. Die „übliche Sorgfalt" der Unternehmensführung umfasst aber jedenfalls auch das Erkennen und Bekämpfen von IT-Risiken.[71]

Die Unternehmensleitung hat unter den zur Beseitigung des Risikos verfügbaren Maßnahmen i.R.d. von der Rechtsprechung anerkannten zulässigen Risikos eine Auswahl zu treffen.[72] Die Absicherung der IT-Systeme gegen externe Angriffe gehört in jedem Fall zu einem risikoangemessenen IT-Betrieb.[73] Kommerzielle Nutzer müssen, abhängig auch von der Größe ihrer IT-Infrastruktur, Maßnahmen zur Sicherung ihrer IT-Systeme ergreifen. Dazu gehören jedenfalls die primäre Abwehr, die sekundäre Überprüfung durch Suchprogramme sowie die notwendige Aktualisierung der Programme.[74]

Im Rahmen der Entscheidungsfindung sind die einzelnen Aspekte, die für und die gegen eine Entnetzung sprechen, sorgfältig gegeneinander abzuwägen. Im Grundsatz sind in diesem Zusammenhang ähnliche Überlegungen anzustellen wie bei der oben erörterten Angemessenheitsprüfung.[75]

4. Berücksichtigung der Entnetzung als Sicherheitsoption

a) Risikoanalyse

Nach allen vorstehend erörterten Normen sind die Verantwortlichen – jedenfalls implizit – zur Analyse von Bedrohungsszenarien verpflichtet. Auf Grund des sich abzeichnenden und von der *ENISA* festgestellten Paradigmenwechsels müssen nunmehr auch Cyber-Angriffe der Stuxnet-Kategorie in die IT-Sicherheitsstrategie einbezogen werden.

b) Risikobekämpfung

Es liegt auf der Hand, dass eine vollständige Entnetzung von Systemen nur als Ultima Ratio[76] für besonders kritische IT-Infrastrukturen in Betracht kommt. Gleichwohl werden künftig folgende Gesichtspunkte zu berücksichtigen sein:

- Die bisher geltenden Sicherheitsstandards werden sich nach der Erfahrung mit Stuxnet generell erhöhen.[77]
- Im Hinblick auf die zu betrachtenden Netze bzw. Systeme ist zu bewerten, ob es sich hierbei um kritische Infrastrukturen handelt.
- Bei kritischen Infrastrukturen ist zu hinterfragen, ob eine über den gegenwärtig bestehenden Vernetzungsgrad hinausgehende weitere Vernetzung (z.B. mit weiteren Drittsystemen) sinnvoll und erforderlich ist und ob sich hierdurch die Risiken erhöhen.
- Bei der Auslagerung kritischer IT-Anwendungen (ASP, Outsourcing, Cloud Computing) sind die Sicherheitsvorkehrungen der jeweiligen Anbieter sowie die Sicherheit der Netzverbindungen zu diesen Anbietern zu hinterfragen.
- Bei kritischen Systemen sind vor einer Entnetzung Alternativen zu prüfen, die den Sicherheitsstandard auf das erforderliche Maß erhöhen, z.B. Aktualisierung und Erweiterung der bisherigen Sicherheitsvorkehrungen, insbesondere von Firewalls, und Implementierung redundanter Systeme.
- Bei der „Entnetzung" selbst sind ebenfalls abgestufte Herangehensweisen denkbar. So werden teilweise sog. „Air Gap"-Systeme eingesetzt. Als Air Gap („Luftspalt") wird ein Prozess bezeichnet, der zwei IT-Systeme voneinander physisch und logisch trennt, aber dennoch die Übertragung von Daten zulässt. Das Air Gap wird eingesetzt, um zwei oder mehr unterschiedlich vertrauenswürdige Rechnernetze voneinander zu isolieren, die jedoch Daten des jeweils anderen Systems verarbeiten müssen. Der Einsatzzweck ähnelt dem einer Firewall. Bei der Isolation der Systeme voneinander kann u.a. sichergestellt werden, dass die Datenübertragung nur in einer Richtung erfolgt und dass selbst bei Übertragung von Malware kein Rückkanal zur Verfügung steht, der z.B. die Übertragung von vertraulichen Inhalten ermöglichen könnte.[78] Das Verfahren wird im Hinblick auf militärische Netzwerke, Regierungsnetzwerke sowie im Hinblick auf besonders kritische Systeme wie z.B. bei Kraftwerken, in der Luftfahrt und im medizintechnischen Bereich diskutiert.[79]

Dr. Sandro Gaycken
ist Technik- und Sicherheitsforscher an der Freien Universität Berlin. Schwerpunkte seiner Forschung sind Cyberwarfare, Cybersecurity, Sicherheit und Technik, Datenschutz sowie gesellschaftliche und ethische Folgen der Informationstechnik.

Dr. Michael Karger
ist Rechtsanwalt, Fachanwalt für Informationsrecht, Fachanwalt für Verwaltungsrecht und Partner bei Wendler Tremml Rechtsanwälte, München.

67 *Nolte/Becker* (o. Fußn. 66), S. 24.
68 *Nolte/Becker* (o. Fußn. 66), S. 24.
69 *Spindler* (o. Fußn. 45), S. 111.
70 *Spindler*, in: MüKo zum Aktiengesetz, 3. Aufl. 2008, § 91 AktG Rdnr. 24.
71 *Trappehl/Schmidl*, NZA 2009, 985, 986.
72 *Spindler* (o. Fußn. 45), S. 110.
73 *Nolte/Becker* (o. Fußn. 66), S. 24.; vgl. auch *BITKOM*-Leitfaden „Sicherheit für Systeme und Netze im Unternehmen", 2. Aufl., S. 22 f.
74 *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, 2007, S. 167.
75 S.o. IV.3. c).
76 S.o. IV.3. c).
77 Zu den aktuell gültigen IT-Sicherheitsstandards s. den vom *BITKOM* und vom *Deutschen Institut für Normung e.V.* herausgegebenen „Kompass der IT-Sicherheitsstandards", Version 4.0, August 2009, abrufbar unter: www.bitkom.de.
78 Vgl. http://de.wikipedia.org/wiki/Air_Gap.
79 Vgl. http://en.wikipedia.org/wiki/Air_Gap (Computing).