www.jusletter-it.eu

Agnes Balthasar / Matthias Wach / Alexander Balthasar

Sind Sicherheitslücken wirklich unvermeidlich? Technische, rechtsdogmatische und rechtspolitische Überlegungen

Sicherheitslücken bieten Nachrichtendiensten wie Kriminellen weitreichende Möglichkeiten, Daten zu ihren Zwecken abzuhören oder zu manipulieren; auf diese Herausforderung haben unsere Rechtsordnungen erst teilweise Antworten gefunden. Nicht zuletzt die grundrechtliche Dimension etwaiger Angriffe in Folge von Sicherheitslücken fordert jedoch ausreichende Effektivität des Rechtsschutz-Systems. Nach Darstellung der technischen Problematik will dieser Artikel nicht nur einen Überblick über die derzeitigen Schutzinstrumente bieten, sondern auch Impulse zu deren sinnvollen Weiterentwicklung aufzeigen.

Kategorie: Beiträge
Rechtsgebiete: Datenschutz; Datensicherheit
Region: Österreich

Zitiervorschlag: Agnes Balthasar / Matthias Wach / Alexander Balthasar, Sind Sicherheitslücken wirklich unvermeidlich? Technische, rechtsdogmatische und rechtspolitische Überlegungen, in: Jusletter IT 15. Mai 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1 Technischer Hintergrund

1.1 Einführung

[Rz 1] Wie auch der breiten Öffentlichkeit durchaus bekannt, werden Schwachstellen in Computerprogrammen von Kriminellen gerne dazu genutzt, Kommunikation sowie Computersysteme zu manipulieren, Zugriff auf Daten wie etwa Zugangsdaten, Kreditkartennummern etc. zu erlangen und in Folge Opfer zu schädigen. So stiegen laut Cybercrime-Report 2012[1] die Delikte im Bereich Cyberkriminalität in Österreich im Vergleich zum Jahr 2011 um mehr als 100% an, was sich nicht zuletzt auf sorglosen Umgang der Bevölkerung im Bezug auf die Internetnutzung zurückführen lässt.[2]

[Rz 2] Doch nicht nur Kriminelle, auch Nachrichtendienste nutzen Schwachstellen in Computerprogrammen extensiv aus, wie der Spiegel[3] und der Guardian[4] im Gefolge der «Snowden-Leaks» berichteten.

[Rz 3] Diese Dienste versuchen einerseits, verdeckte Einflussnahme auf Softwarehersteller auszuüben, um absichtlich Hintertüren, sogenannte «Backdoors», während der Softwareentwicklung einzuschleusen. Andererseits wird versucht, möglichst viele Informationen über in Software vorhandenen Sicherheitslücken zu sammeln, um fremde IT-Systeme zu überwachen oder zu manipulieren.

[Rz 4] So wurde unter anderen die «ANT»-Abteilung der NSA mit dem Ziel geschaffen, bestehende Lücken für Geheimdienstzwecke nutzbar zu machen sowie Backdoors zu entwickeln. Mittels

---

1 http://www.bmi.gv.at/cms/BK/publikationen/files/Cybercrime_Report2012_Web.pdf(Alle Internetquellen wurden, wenn nicht anders angegeben, am 7. März 2014 zuletzt abgerufen.).

2 http://oesterreich.orf.at/stories/2603429/.

3 http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

4 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

eines Katalogs[5], ähnlich dem eines Versandhauses, bietet ANT anderen NSA-Abteilungen bzw. befreundeten Diensten zahlreiche soft- wie hardwarebasierte[6] Infiltrationsmethoden an. Diese verschaffen den Nachrichtendiensten unzählige Möglichkeiten, welche unter anderem vom Kompromittieren von Personen[7], Erlangen geheimer Regierungsinformationen bis hin zu Industriespionage reichen.

1.2 Arten von Sicherheitslücken

[Rz 5] Oft ist es in der Praxis nicht möglich, zwischen absichtlich eingebauten Backdoors und aufgrund von Programmier- und Konfigurationsfehlern vorhandenen Sicherheitslücken zu unterscheiden. Dies ist vor allem auf Beweisprobleme zurückzuführen, würde doch kein Hersteller zugeben, sich nachrichtendienstlichem Druck gebeugt und wissentlich die Sicherheit der eigenen Produkte verwässert zu haben. Andererseits liegt es auch im Rahmen des Möglichen, dass einzelne Programmierer ohne Wissen ihres Arbeitgebers Backdoors in einem Programm hinterlassen. Die Komplexität und der Umfang heutiger Computerprogramme machen es schlicht unmöglich, jede einzelne Zeile eines Computerprogramms und jede noch so kleine Änderung am Programmcode auf deren Korrektheit hin zu prüfen.

[Rz 6] Betrachtet man den Problemkreis der unabsichtlich in einem Programm vorhandenen Fehler genauer, so kann vereinfacht dargestellt zwischen zwei Arten von Fehlern unterschieden werden:

[Rz 7] Viele Fehler sind durchaus im Vorfeld erkennbar und würden sich im Zuge einer eingehenden Qualitätskontrolle vermeiden lassen. So kommt es nicht selten vor, dass Sicherheitsprobleme so offensichtlich sind, dass sie von einem erfahrenen Anwender mit relativ simplen Mitteln zu erkennen sind.

[Rz 8] Als Beispiel kann hier ein Sachverhalt angeführt werden, welcher im Dezember 2003 seinen Ausgang nahm[8]. So berichtete ein Benutzer von einem mysteriösen Dienst[9], welcher auf seinem Router[10] vorhanden sei. Es dauerte jedoch bis zum Jahresende 2013, also ca. 10 Jahre, bis dieser Meldung nähere Beachtung geschenkt wurde. In Folge der Enthüllungen eines Sicherheitsspezialisten kam zu Tage, dass genau jener Dienst, welcher sich auf Routern diverser Hersteller findet, ein angeblich vergessener Wartungszugang ist, mithilfe dessen die Konfiguration betroffener Geräte gelesen und manipuliert werden kann. Zu entdecken war diese Lücke mit einfachsten Mitteln, da für erfahrene Anwender mithilfe eines Portscans[11] leicht festzustellen ist, dass ein

5 http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

6 Dabei ist an speziell angepasste Hardware zu denken, deren Erscheinungsbild gewöhnlicher Hardware entspricht, die jedoch zusätzliche Spionagefunktionen enthält. So existieren z.B. Monitorkabel, die die Bildsignale per Funk an Überwacher übertragen oder USB-Sticks, welche über versteckte Funkmodule Daten übertragen.

7 http://heise.de/-2123236.

8 http://heise.de/-2084884.

9 Computer können viele verschiedene Netzwerkdienste anbieten, welche unter einem sogenannten «Port» erreichbar sind.

10 Router stellen Knoten in Netzwerken dar, ermöglichen die Nutzung eines einzelnen Internetanschlusses mit mehreren Geräten und sind heutzutage in fast jedem Haushalt zu finden. Sie bieten grundlegende Sicherheitsfunktionen und stellen oft zusätzlich Funktionen wie Wlan, Dateiserver, Druckerserver oder Telefoniedienste bereit.

11 Mithilfe eines Portscans kann festgestellt werden, welche Dienste von einem Netzwerkgerät bereitgestellt werden.

verdächtiger Dienst auf einem Gerät vorhanden ist. Es ist unverständlich, warum dieser nicht schon im Rahmen der Qualitätskontrolle entdeckt wurde. Die Vermutung, betroffene Hersteller hätten ihre Geräte nicht einmal den grundlegendsten Sicherheitstests unterzogen, liegt nahe.

[Rz 9] Diesen leichter erkennbaren Fehlern sind diejenigen gegenüberzustellen, die in der komplexen Logik und dem enormen Umfang[12] des Programmcodes versteckt sind und oft erst dann zu Tage treten, wenn diese dazu ausgenutzt werden, Angriffe auf IT-Systeme durchzuführen. Dies ist nicht zuletzt darauf zurückzuführen, dass die zahlreichen Einsatzmöglichkeiten moderner IT-Systeme es den Herstellern im Vorhinein schlicht unmöglich machen, alle Anwendungsszenarien zu bedenken bzw. zu testen und somit jeglichen Fehler im Vorfeld auszuschließen.

1.3 Folgen von Sicherheitslücken

[Rz 10] Je nach Beschaffenheit eines Sicherheitsproblems ergibt sich ein weiter Spielraum möglicher Gefährdungspotentiale, welche aufgrund von deren Diversität nur demonstrativ dargestellt werden können.

[Rz 11] Abhängig von der Art der Schwachstelle, der betroffenen Gerätekategorie sowie der betroffenen Software reichen die Möglichkeiten vom Überwachen aller Eingaben über das unbemerkte Aktivieren von integrierten Mikrophonen oder Kameras, dem Manipulieren von aufgerufenen Websites bis hin zur Möglichkeit, beliebige Daten zu kopieren und zu manipulieren. Um einen Eindruck von der Tragweite real möglicher Angriffe zu vermitteln, sollen nun drei Beispiele näher erläutert werden:

1. Immer wieder treten Lücken an Routern für Heim- oder Firmennetzwerke auf, die es ermöglichen, deren Konfiguration bzw. Software zu manipulieren. So nützten Kriminelle eine Lücke aus, konfigurierten ein betroffenes Gerät um und richteten innerhalb einer halben Stunde einen Schaden von ca. €{} 4'000.– an, indem sie die im Router integrierte Telefoniefunktion dazu nutzten, Mehrwertnummern anzurufen[13]. Bekannt wurde die Lücke, da die Betroffenen diesen Sachverhalt in Folge der hohen Telefonrechnungen zur Anzeige brachten. In weiterer Folge kam zu Tage, dass fast alle aktuellen Routermodelle eines bekannten Herstellers von dieser Schwachstelle betroffen waren und diese es auch ermöglicht hätte, die gesamte über die betroffenen Geräte abgewickelte Kommunikation zu belauschen.
2. Subtiler gelang es Angreifern in einem ähnlich gelagerten Fall, zahlreiche von einer Lücke betroffene Router derart zu manipulieren, dass diese den Netzwerkverkehr auf Zugangsdaten überwachten und diese an die Angreifer weiterleiten. Die Existenz dieser Lücke wurde erst in Folge von Recherchen eines IT-Fachmagazins entdeckt, besonders brisant war die Lücke für eine betroffene deutsche Anwaltskanzlei, da Zugangsdaten für alle Mail-Accounts der Kanzlei an Angreifer gelangten und somit die Vertraulichkeit jeglicher Kommunikation von vorherein nicht gewährleistet war.[14]
3. Über Monate unentdeckt blieb auch eine Lücke in jenem Teil des Programmcodes eines Betriebssystems, welcher für die korrekte Verschlüsselung von Websiteaufrufen zuständig ist. In Folge dessen waren Computer, Smartphones und Tablets, welche auf der gleichen Betriebs-

[12] Windows XP enthält beispielsweise 50 Millionen Textzeilen Programmcode.

[13] http://heise.de/-2110186.

[14] http://heise.de/-1963578.

systemfamilie basierten, monatelang einem erhöhten Sicherheitsrisiko ausgesetzt, da deren Browser auch im Fall von Manipulation eine korrekte Verschlüsselung anzeigte. Obwohl die Lücke großen Wiederhall in der Fachpresse fand, wurden keine konkreten Angriffe bekannt, jedoch sind es genau solche Lücken, welchen es Nachrichtendiensten besonders leicht machen, auch verschlüsselte Kommunikation, beispielsweise den Zugriff auf Mailkonten, ohne Wissen der Betroffenen komplett mitlesen zu können. Auch Kriminelle könnten derartige Lücken dazu nutzen, besonders brisanten Datenverkehr zu manipulieren – so wäre es beispielsweise möglich gewesen, von betroffenen Geräten aus vorgenommenes Internetbanking derart zu manipulieren, dass Überweisungen nicht auf den vom Benutzer angegebenen Konten landen, sondern auf Konten der Kriminellen umgeleitet werden. Die Art der Lücke und die konkrete Ausgestaltung des Programmcodes, welcher diese verursachte, ließ in der Fachwelt die Vermutung aufkommen, es könnte sich hierbei auch um ein gezielt platziertes Backdoor handeln. Aufgrund der schon angesprochenen Beweisproblematik konnte dies bisher jedoch nicht zweifelsfrei belegt werden.[15]

1.4 Reaktionen auf Sicherheitslücken

[Rz 12] Sicherheitslücken sowie Backdoors sind nicht zuletzt deshalb besonders gefährlich, da sie im Gegensatz zu Fehlern an klassischen Waren je nach betroffener Software eine fast *unüberblickbare Menge an Anwendern* treffen. Dazu kommt, dass es aufgrund der Verbreitungswege von IT-Produkten für den Hersteller, z.B. im Gegensatz zu einem Autoproduzenten, oft *unmöglich* ist, alle Abnehmer seines Produktes über Sicherheitsrisiken zwecks deren Behebung direkt zu *informieren*.

[Rz 13] Natürlich liegen Fehler in der Natur jeder von Menschen erbrachten Arbeit – deren Vorhandensein lässt sich also nie komplett ausschließen. In Folge dessen stellt sich jedoch die Frage nach einer «machbaren» bzw. zumutbaren Reaktion auf diese Sicherheitsprobleme.

[Rz 14] Viele Nutzer sind bereits dahingehend sensibilisiert, Virenscanner und Firewalls auf den von ihnen genutzten Geräten zu installieren. Oft wird jedoch aus den Augen verloren, dass Sicherheitssoftware auf einem PC oder Smartphone nicht die restliche Infrastruktur vor Sicherheitsrisiken schützt – Router oder moderne Netzwerkdrucker sind vollwertige Computer, enthalten ebenfalls Sicherheitslücken und sind deswegen genauso attraktive Angriffspunkte wie klassische PCs. Diese Tatsache gewinnt durch die Entwicklung, herkömmliche Geräte wie Kühlschränke «smart» zu machen und mit dem Internet zu verbinden, an zusätzlicher Relevanz.

[Rz 15] Auch die beste Sicherheitssoftware kann nur wenig Schutz bieten, wenn nicht alle installierten Programme in Form von Aktualisierungen auf dem neuesten Stand gehalten werden. Zwar reagieren die meisten Hersteller zeitnahe auf entdeckte Lücken und bieten entsprechende Aktualisierungen an, betagte, offiziell nicht mehr unterstützte Produkte erhalten jedoch oft keinerlei Aktualisierungen mehr[16].

---

15 http://heise.de/-2121738, http://heise.de/-2121441sowie https://www.imperialviolet.org/2014/02/22/applebug.html.

16 Dies ist besonders dann problematisch, wenn veraltete Software noch im großen Maße eingesetzt wird, wie beispielsweise Windows XP. Aktuell (März 2014) wird noch fast jeder dritte PC mit Windows XP betrieben, Microsoft stellt die Unterstützung für dieses im Oktober 2001 erschienene Betriebssystem jedoch am 8. März 2014 ein, was zur Folge hat, dass Sicherheitslücken in Windows XP nicht mehr behoben werden (siehe http://heise.de/-2134738).

[Rz 16] Doch auch für den Fall, dass Aktualisierungen vorhanden sind, ergibt sich das Problem, dass derzeit nur Computer, Smartphones und Tablets über automatische Mechanismen verfügen, welche Aktualisierungen ohne Benutzerinteraktion vornehmen. Die meisten anderen Geräte, wie beispielsweise Router, können nur manuell durch den Benutzer aktualisiert werden. Dies bedeutet, dass der Benutzer einerseits Kenntnis von der Verfügbarkeit der Aktualisierung erlangen und andererseits jenes technische Know-How besitzen muss, um diese durchführen zu können.

2 (Grund-)Rechtliche Dimensionen

2.1 Zivil- und Strafrecht

[Rz 17] In rechtlicher Hinsicht stellen die hier dargestellten Sicherheitslücken zuallererst einmal Produkt-Mängel dar, die – innerhalb der regelmäßig im Vordergrund stehenden privatrechtlichen Beziehungen zwischen Hersteller, (Zwischen-)Händler und Endverbraucher – auf dem **Zivilrechtswege** geltend zu machen wären. Dabei ist jedoch schon aus der Perspektive des je einzelnen Endverbrauchers zu beachten, dass *Gewährleistungsansprüche* – die sich gegen den vom Endverbraucher selbst ausgewählten unmittelbaren Vertragspartner, d.h. den Verkäufer des Geräts bzw. gesonderter Software, richten – jedenfalls nur auf Mängelbehebung pro futuro bzw. Preisminderung bzw. Wandlung (d.h. Rückabwicklung des Vertrages[17]) gerichtet sind[18], nicht aber auch auf die Erstattung von *Mangelfolgeschäden*. Für diese haftet der unmittelbare Vertragspartner des Endverbrauchers nur bei *eigenem* Verschulden; ein solches wird freilich oft genug entweder bereits objektiv betrachtet nicht vorliegen[19] oder aber vom Endverbraucher schlicht nicht zu beweisen sein.

[Rz 18] Nun gibt es genau deshalb überdies eine «*Produkthaftung*»[20], mit der derartige Schadenersatzansprüche – grundsätzlich auch verschuldensunabhängig – gegen den Hersteller oder auch den Importeur erhoben werden können. Sieht man näher zu, dann dürfte freilich auch dieses Institut in seiner **Effektivität an beachtliche Grenzen** stoßen:

[Rz 19] Schon das österreichische Produkthaftungsgesetz[21] schließt nicht nur seine Anwendbarkeit dann aus, wenn ein «Unternehmer» die betreffende «Sache überwiegend in seinem Unternehmen verwendet hat» (§ 2 Z 1), was gerade im hier behandelten Kontext den gesamten Bereich betrieblicher EDV diskriminiert, sondern verweigert einen Ersatzanspruch überdies, wenn «die Eigenschaften des Produkts nach dem Stand der Wissenschaft und Technik zu dem Zeitpunkt, zu dem es der in Anspruch Genommene in den Verkehr gebracht hat, nicht als Fehler erkannt werden konnten» (§ 8 Z 2), worauf sich wohl gerade IT-Hersteller gerne berufen werden.

---

17 Dies gilt in gleicher Weise – jedenfalls im österreichischen Recht – für eine allenfalls in Betracht kommende Anfechtung wegen eines *Irrtums*des Käufers über eine wesentliche Eigenschaft des Kaufgegenstandes, unter den weiteren Voraussetzungen des § 871 des österreichischen Allgemeinen Bürgerlichen Gesetzbuches (ABGB). Anderes gilt zwar für eine erfolgreiche Anfechtung wegen List bzw. Nötigung (vgl. § 874 ABGB) – diese Konstellationen können im hier gegebenen Zusammenhang aber außer Betracht bleiben.

18 Vgl. für Österreich § 932 ABGB.

19 Einem Verkäufer von IT-Hard- bzw. Software kann wohl kaum jemals zugemutet werden, in eigenständiger Weise, d.h. unter Außerachtlassung vom Hersteller gegebener Zusicherungen über die Qualität des Produkts, dessen Sicherheit zu überprüfen.

20 Vgl. für Österreich das Produkthaftungsgesetz, BGBl 1988/99.

21 Siehe vorige Fn.

[Rz 20] Dazu kommt freilich, dass die Geltendmachung von Produkthaftansprüchen im – bei IT-Produkten regelmäßig gegebenem – internationalen Bezug weder in materiellrechtlicher[22] noch in formellrechtlicher Hinsicht[23] für den Geschädigten ganz einfach sein dürfte.

[Rz 21] Prinzipiell sind Beeinträchtigungen der IT-Sicherheit natürlich auch **strafrechtlich** sanktionierbar (vgl. für Österreich etwa §§ 118a, 119a des Strafgesetzbuches [StGB][24]). Freilich stoßen gerade auch hier Verfolgungshandlungen regelmäßig an die Grenzen der jeweiligen **Zuständigkeit** der jeweiligen staatlichen Strafgerichtsbarkeiten.[25]

2.2 Die grundrechtliche Perspektive

[Rz 22] Dieser Befund limitierter Effektivität des gegenwärtigen zivil- wie strafrechtlichen Schutzes kontrastiert eigentümlich mit der grundrechtlichen Perspektive:

[Rz 23] Denn auch wenn im Einzelnen hinsichtlich der Rechtsnatur von «Information» noch vieles strittig ist[26] – auf *zivilrechtlicher* Ebene konkurrieren eine sachenrechtliche[27] und eine persönlichkeitsrechtliche[28] Perspektive – so ist doch klar, dass «Information» rechtlich gesehen keinesfalls eine «terra nullius» darstellt: in **grundrechtlicher** Hinsicht kommen hier – blickt man nur, parte pro toto, in die EU-Grundrechte-Charta (EUGRC) – vornehmlich in Betracht die Rechte auf Datenschutz (Art. 8), auf (geistiges) Eigentum (Art. 17 [Abs. 2]), aber auch jene auf Schutz der Privatsphäre als solcher (Art. 7) sowie auf Meinungsfreiheit (Art. 11)[29]; darüber hinaus kann man – wie das dBVerfG[30] – sichtlich auch ein Grundrecht auf «informationelle Selbstbestimmung» als Ausfluss des Rechts auf «freie Entfaltung der Persönlichkeit» (Art. 2 Abs. 1 des deutschen Grundgesetzes [dGG]) und damit letztlich als Ausfluss der «Würde des Menschen» überhaupt (Art. 1 Abs. 1 dGG; Art. 1 EUGRC) annehmen.

[Rz 24] Unter der Voraussetzung, dass sowohl die «rule of law»[31] im allgemeinen wie Art. 1 EMRK

---

22 Vgl. hiezu etwa Claudia Rudolf, Internationales Produkthaftungsrecht nach der Rom II-Verordnung, wbl 2009, 525 ff., insbesondere ihr Resümee.

23 Vgl. hiezu erst jüngst das Urteil des EuGH vom 16. Januar 2014, C-45/13, Kainz, Rz. 31, unter Berufung auf Vorjudikatur.

24 Bemerkenswerterweise sind diese Delikte allerdings nicht als reine Offizial-, sondern als *Ermächtigungsdelikte*ausgestaltet, was nicht auf ein übermäßiges öffentliches Interesse an der Strafverfolgung hindeutet.

25 Vgl. für Österreich §§ 64, 65 StGB.

26 Siehe näher jüngst Alexander Balthasar, Right of access to information? Prolegomena to a rising issue with due consideration of the legal nature of information, in: *Alexander Balthasar*, *Hendrik Hansen*, *Balázs Kőnig*, *Robert Müller-Török*, *Johannes Pichler*(Eds.), CEEeGov Days 2014, eGovernment: Driver or Stumbling Block for European Integration? Proceedings of the CEEeGov Days, May 8–9, 2014 Budapest (2014), 23 ff., 25 ff.

27 Ausgehend vom römischrechtlichen – und in § 285 ABGB grundsätzlich bewahrten – weiten Sachenbegriff des ABGB; vgl. Elisabeth Staudegger, Datenhandel – ein Auftakt zur Diskussion. Zur Zulässigkeit des Handels mit Daten aus Anlass der Weitergabe von «Gesundheitsdaten», ÖJZ 2014, 107 ff.

28 Vgl. insbesondere Viktor Mayer-Schönberger, Information und Recht. Vom Datenschutz bis zum Urheberrecht (2001), insbes. 25 ff.

29 Dies insofern, als die Befürchtung, dass eigene Meinungsäußerungen einem anderen als dem vom Äußernden bestimmten Adressatenkreis zur Kenntnis gelangen könnten, diesen von der Äußerung selbst abhalten könnte.

30 Urteil vom 15. Dezember 1983, Az. 1 BvR 209 u.a., BVerfGE 65, 1; kritisch unlängst Walter Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit. Gutachten für den XVIII. Österreichischen Juristentag (2012), I/1, 85 ff.

31 Diese gehört mittlerweile gemäß Art. 2 EUV zu jenen Werten, auf die sich nicht nur die Union gründet, sondern die auch allen Mitgliedsstaaten gemeinsam sind; auf der Ebene des Europarates siehe Art 3 seiner Satzung. Aus der Perspektive das nationalen österreichischen Verfassungsrechts gebietet das rechtsstaatliche Bauprinzip hinreichende Effizienz des Rechtsschutzes (vgl. z.B. VfSlg 16.772/2002); siehe jedoch schon – denselben Grundgedanken artikulie-

im Besonderen den Staat nicht nur zur Respektierung von (Grund-)Rechten, sondern auch zu deren Gewährleistung verpflichten[32], ist der oben erzielte Befund mangelnder Effektivität nicht nur von rein rechtspolitischer, sondern auch bereits von **rechtsdogmatischer** Relevanz. Die nachfolgenden Ausführungen zielen daher darauf ab, Vorschläge, wie künftig dieser Gewährleistungspflicht besser entsprochen werden könne, zu erstatten, freilich vor dem Hintergrund bereits existierender derartiger Ansätze.

3 Bestehende Lösungsansätze

[Rz 25] Der Europäischen Union ist die Problematik sichtlich bereits seit Jahren bewusst, wie nicht nur eine Fülle unverbindlicher Rechtsakte[33], sondern auch das seit Jahren praktizierte Bestreben, die Problematik einer breiteren Öffentlichkeit näher zu bringen,[34] zeigt. Darüber hinaus sind insbesondere nachstehende vier Maßnahmen hervorzuheben.

3.1 ENISA

[Rz 26] Ein wichtiger Schritt war die Errichtung der europäischen Agentur ENISA (European Network and Information Security Agency), welche 2004 zunächst durch eine Verordnung[35] für einen Zeitraum von fünf Jahren gegründet wurde und ihren Sitz in Kreta hat. Ziel von ENISA ist es, zu einer hohen Netz- und Informationssicherheit innerhalb der Europäischen Union beizutragen und eine entsprechende Kultur zu entwickeln (EwGr 15). Dieses Mandat wurde in weiterer Folge, vor allem, weil die Bedeutung des Themas Internetsicherheit erkannt wurde, immer wieder verlängert (2008,[36] 2011[37]). Da die Bewertung[38] von ENISA einige Schwachstellen aufzeigte, wurde zur Modernisierung eine neue Verordnung[39] erarbeitet. Diese trat am 19. Juni 2013 in Kraft und verlängert ENISAs Mandat für weitere sieben Jahre; sie trifft strukturelle Änderun-

rend – § 19 ABGB.

32 Siehe näher nur Michael Holoubek, Grundrechtliche Gewährleistungspflichten (1997); Christoph Grabenwarter/Katharina Pabel, Europäische Menscenrechtskonvention, 5. Auflage (2012), § 19.

33 Für einen Überblick siehe: Vorschlag der Europäischen Kommission vom 7. Februar 2013 für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM(2013) 48 final, Punkt 1.2. der Begründung («Allgemeiner Kontext»).

34 Beispielsweise die Saferinternet Initiative, die von der Europäischen Kommission mitgetragen wird und vor allem Kinder, Jugendliche, Eltern und Lehrende bei einem sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien unterstützt (http://www.saferinternet.at) oder der 2012 ins Leben gerufene Europäische Cybersicherheitsmonat, in dessen Rahmen europaweit Veranstaltungen zum Thema Internetsicherheit abgehalten werden, um Internetnutzer für Gefahren des Internets zu sensibilisieren, zu informieren und Hilfestellungen anzubieten (http://cybersecuritymonth.eu).

35 Verordnung (EG) Nr. 460/2004vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl L 2004/77, 1.

36 Verordnung (EG) Nr. 1007/2008vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, ABl L 2008/293, 1.

37 Verordnung (EU) Nr. 580/2011vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer, ABl L 2011/165, 3.

38 Mitteilung der Kommission an das Europäische Parlament und den Rat vom 1. Juni 2007 über die Bewertung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), KOM(2007) 285 endgültig.

39 Verordnung (EU) Nr. 526/2013vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, ABl L 2013/165, 41.

gen, wie die Einrichtung einer Außenstelle in Athen (Art. 26 Abs. 4), und überträgt ENISA neue Befugnisse.

[Rz 27] ENISA hat zunächst einmal die Funktion einer Denkfabrik.[40] Sie soll als Forum[41] für den Austausch von Erfahrungen im Bereich der Netz- und Informationssicherheit dienen und Kontakte zu Organen, Einrichtungen und sonstigen Stellen der EU, staatlichen Behörden, der Wirtschaft und Verbraucherschutzorganisationen aufnehmen. Darüber hinaus wird ENISA beratend tätig, gibt beispielsweise Mitgliedstaaten und der EU fachkundige Ratschläge zur Verbesserung der Netz- und Informationssicherheit oder unterstützt bei der Analyse[42] von Sicherheitsproblemen.[43] Auf Aufforderung berät ENISA überdies die Kommission bei technischen Vorarbeiten für die Aktualisierung und Weiterentwicklung des EU-Rechts.[44]

3.2 EC3

[Rz 28] Seit Anfang 2013 besteht ein bei Europol in Den Haag angesiedeltes Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (European Cybercrime Center, EC3).

[Rz 29] Das Zentrum soll strafrechtliche Ermittlungen der Mitgliedstaaten gegen illegale Online-Tätigkeiten organisierter krimineller Gruppen (z.B. im Zusammenhang mit Online-Finanztätigkeiten, Cyberattacken auf kritische Infrastrukturen und sexueller Ausbeutung von Kindern im Internet) unterstützen, eine gezielte Schulung von Strafverfolgern, Richtern und Staatsanwälten gewährleisten, sowie EU-weite Lösungen fördern. Erfahrungen und Informationen sollen gebündelt, Forschung und Entwicklung erleichtert und Bedrohungsanalysen und Frühwarnungen erstellt werden.[45] EC3 soll auch mit anderen Einrichtungen, darunter auch ENISA[46] zusammenarbeiten.[47]

[Rz 30] Auf nationaler Ebene ist beispielsweise in Österreich ein Cyber Crime Competence Center (C4) im Aufbau, in dessen Rahmen Experten des Bundeskriminalamtes, des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung sowie des Bundesamtes zur Korruptionsprävention und -bekämpfung zusammenarbeiten sollen.[48] Es soll als zentrale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität fungieren, eine Schnittstelle zu den Zentralstellen

---

40 http://heise.de/-1796599.

41 http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_de.htm.

42 So hat ENISA bei einer kürzlich veröffentlichen Analyse aktueller Betrugsfälle bei online abgewickelten Finanzgeschäften unzureichende Sicherheitsvorkehrungen auf Seiten der Dienstleister festgestellt (http://heise.de/-2090273, http://heise.de/-1928312). Auch hat die Agentur Ende letzten Jahres einen Ratgeber zum Aufbau von Computer Emergency Response Teams für Sicherheitslücken in industriellen Kontrollsystemen herausgegeben (http://heise.de/-2060774). Ebenso gab ENISA Empfehlungen zu Krypto Verfahren ab (http://heise.de/-2043356). Letztes Jahr publizierte ENISA eine Studie, in welcher sie vor Datenrisiken beim Cloud Computing warnt (http://heise.de/-1803684).

43 http://heise.de/-1843357.

44 http://europa.eu/legislation_summaries/information_society/internet/l24153_de.htm.

45 Pressemitteilung der Europäischen Kommission vom 9. Januar 2013 über ein Europäisches Zentrum zur Bekämpfung der Cyberkriminalität.

46 Mit dieser könnte es aber in Zukunft aufgrund unzureichender Aufgabenabstimmung zu Konflikten kommen, siehe http://www.sicherheitsmelder.de/xhtml/articleview.jsf;?id=8AD00DCD440D.htm.

47 https://netzpolitik.org/2013/europaische-union-rustet-polizeibehorden-gegen-cyberkriminalitat-piraterie-und-hacktivismus/.ENISA und EC3 haben zwar ein breites Aufgabenspektrum, sind aber nicht für Cyberspionage zuständig, weshalb sie auch nicht rund um den aktuellen Spionageskandal eingebunden sind, wie deren Sprecher auf Anfrage von EU-Abgeordneten im Rahmen der Untersuchungen der NSA-Affäre mitteilten (http://heise.de/-2061583).

48 http://derstandard.at/1304552207833/.

in anderen Ländern sowie zum EC3 und zum bei Interpol eingerichteten Digital Crime Center (IDCC) bilden[49] und bis Ende 2014 personell massiv (von 15 auf 49 IT-Spezialisten) aufgestockt werden.[50]

3.3 CERT

[Rz 31] Darüber hinaus wurden IT-Notfallteams, sogenannte Computer Emergency Response Teams (CERT), auf öffentlichem und privatem Sektor errichtet. Sie sammeln Informationen zu Sicherheitsproblemen und geben Warnungen, Tipps und Einschätzungen der aktuellen Sicherheitslage heraus. Darüber hinaus kommt ihnen beratende, koordinierende und unterstützende Rolle beim Auftreten konkreter Sicherheitsprobleme zu, über deren Existenz diese entweder durch Verständigung betroffener Stellen, Eigenrecherche oder Meldungen von dritter Seite Kenntnis erlangen.[51] In der 2010 beschlossenen Digitalen Agenda für Europa[52] verpflichtete sich die Kommission, ein CERT für die EU-Institutionen zu schaffen und sprach sich deutlich dafür aus, dass die Mitgliedstaaten ihrerseits solche IT-Notfallteams einrichten. Nach einem einjährigen Pilotprojekt wurde 2012 das CERT-EU zu einer ständigen Einrichtung[53] erhoben, die die EU-Institutionen in enger Zusammenarbeit mit deren IT-Sicherheitsteams bei Angriffen auf die Netz- und Informationssicherheit unterstützen soll.[54] Auch soll sie enge Kontakte zu den CERT in den Mitgliedstaaten pflegen und unter anderem auch mit ENISA und EC3 zusammenarbeiten.[55]

[Rz 32] In Österreich besteht schon seit 2008 ein vom Bundeskanzleramt in Kooperation mit nic.at gegründetes IT-Notfallteam (CERT.at) für den Unternehmens- und eines (GovCERT.gv.at) für den Behördenbereich. Freilich ist deren Kapazität auch aufgrund der personellen Strukturen begrenzt. Derzeit besteht z.B. das Team CERT.at aus neun Personen.[56]

---

49 Cybercrime Report des Bundeskriminalamts 2012 (FN 1).

50 http://futurezone.at/digital-life/cybercrime-steigt-in-oesterreich-um-112-prozent/24.591.463.

51 Bericht Internet-Sicherheit Österreich 2013 vom November 2013, 10 ff., siehe https://www.cert.at/static/downloads/reports/cert.at-jahresbericht-2013.pdf.

52 Mitteilung der Europäischen Kommission vom 19. Mai 2010 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine digitale Agenda für Europa, KOM(2010) 245 endgültig.

53 http://cert.europa.eu/cert/plainedition/en/cert_about.html.

54 http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/cert-eu-zu-staendiger-einrichtung-erklaert/.

55 http://www.heise.de/tp/artikel/38/38276/.

56 Siehe Fn. 51.

3.4 Richtlinienvorschlag der Kommission

[Rz 33] Anfang 2013 veröffentlichte die Kommission gemeinsam mit der Hohen Vertreterin für Außen- und Sicherheitspolitik eine Cybersicherheitsstrategie[57] sowie einen Richtlinienvorschlag,[58] der die Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit zum Ziel hat. Hierzu sieht sie dreierlei Maßnahmen vor:

- Erstens sollen die Mitgliedstaaten ein *Mindestniveau an nationalen Kapazitäten* schaffen, die sich mit der Netz- und Informationssicherheit befassen. So sollen zuständige Behörden und CERT geschaffen sowie nationale Netz- und Informationssicherheitsstrategien bzw. Kooperationspläne erarbeitet werden.
- Zweitens sollen die unionsweit errichteten zuständigen Behörden in weiterer Folge miteinander eng *kooperieren*.
- Drittens *verpflichtet* die Richtlinie nach dem Muster der Rahmenrichtlinie für die elektronische Kommunikation[59] gewisse *Unternehmen* in besonders betroffenen Sektoren sowie die *öffentliche Verwaltung* dazu, einerseits *Risiken zu bewerten und geeignete, angemessene Maßnahmen* zur Gewährleistung der Netz- und Informationssicherheit zu ergreifen und andererseits den zuständigen Behörden alle Sicherheitsvorfälle *zu melden*, welche ihre Netze, Informationssysteme und kritischen Dienste ernsthaft beeinträchtigen.

4 Weiterführende Ansätze

[Rz 34] Ohne die bisherigen Initiativen gering zu achten, meinen wir doch, dass noch mehr getan werden könnte; abschließend daher drei weiterführende Vorschläge:

4.1 Ausbau des Einsatzes und Hebung des Niveaus von Verschlüsselungsmethoden

[Rz 35] Zwar hilft die Verschlüsselung von Kommunikation nicht in jedem Fall, sprich dann nicht, wenn die Geräte bzw. Programme, von welchen die Datenübertragung ausgeht, selbst von Sicherheitslücken betroffen sind. Verschlüsselung kann aber insbesondere das Belauschen von Übertragungen an allen anderen Geräten oder Übertragungsmedien innerhalb der Kommunikationskette, wie beispielsweise von Lücken betroffener Router oder das «Anzapfen» von Glasfaserverbindungen, verhindern, weswegen der Trend, Verschlüsselung auf breiter Basis einzusetzen, sehr zu begrüßen ist.[60]

---

57 Gemeinsame Mitteilung der Europäischen Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik vom 7. Februar 2013 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN(2013) 1 final.

58 Vorschlag der Europäischen Kommission vom 7. Februar 2013 für eine Richtlinie des europäischen Parlament und des Rates über Maßnahmen zur Gewährleistung einer hohen Netz- und Informationssicherheit in der Union COM(2013) 48 final.

59 Richtlinie 2002/21/EGvom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl L 2002/108, 33.

60 So verschlüsselt beispielsweise Google seit den Enthüllungen rund um Edward Snowden die interne Kommunikation zwischen dessen Datenzentren, da diese bisher eine wichtige Quelle für die NSA war, siehe http://www.zdnet.de/88168876/prism-google-verschlusselt-datenflusse-zwischen-rechenzentren/.

[Rz 36] Dabei kommt es jedoch entscheidend auf den Einsatz effektiver, sicherer Verfahren an. Im Rahmen des Projekts «Bullrun» verfügt die NSA über Methoden, gewisse im Rahmen von SSL/TLS und damit HTTPS[61] genutzte Verschlüsselungsarten abzuhören.[62] Beispielsweise sei hier die im April 2014 bekannt gewordene «Heartbleed» Lücke[63] genannt, die lange Zeit unentdeckt blieb und zumindest ein halbes Jahr vor deren Bekanntwerden nachweislich ausgenutzt wurde, um verschlüsselte Kommunikation zu belauschen[64]. Um solchen Gefahren zu begegnen, muss neben dem grundsätzlichen Einsatz von Verschlüsselung und der ständigen Überprüfung der benutzten Verfahren sowohl auf Benutzerseite als auch auf Seiten der Betreiber sichergestellt werden, stets aktuelle Softwareversionen einzusetzen.

4.2 Steigerung der Produktsicherheit und Einführung wirksamer Kontrollmechanismen

[Rz 37] Wie bereits angesprochen, könnten schon im Vorfeld bestimmte Sicherheitslücken durch eine *verstärkte und effektivere Qualitätssicherung* vermieden werden. Es sollten also bereits die Hersteller verpflichtet werden, laufend Qualitätskontrollen nach eng festgelegten Maßstäben vorzunehmen. Mit Blick auf dennoch auftretende Sicherheitslücken müssten *umfassende Meldepflichten* geschaffen werden, um die ehestmögliche Information der Benutzer, Hersteller sowie Behörden sicherzustellen.[65] In weiterer Folge sollten Hersteller verpflichtet werden, *zeitnahe Aktualisierungen* bereitzustellen, welche möglichst ohne Zutun der Nutzer eingespielt werden sollten. Zur Überwachung bzw. Durchsetzung (einschließlich der Sanktionierung[66]) dieser Maßnahmen wäre die Schaffung einer Behördenstruktur in der *Art* der Telekom-Regulierungsbehörden[67] oder Datenschutzbehörden[68] notwendig, welche bereits bestehende Einrichtungen wie CERT und ENISA[69] *tunlichst integrieren* sollten.[70]

[Rz 38] Die Schaffung einer derartigen Struktur ist im Grundsatz schon im Richtlinienvorschlag[71]

---

61 SSL/TLS bzw. dessen Implementierung in HTTP Secure ermöglicht verschlüsselte Kommunikation zu Webseiten unter Heranziehung diverser kryptografischer Verfahren.

62 Siehe jüngst etwa Alexander Prosser, Die Handysignatur im Lichte aktueller Entwicklungen, in: *Erich Schweighofer/Franz Kummer/Walter Hötzendorfer (*Hrsg.), Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, 256 ff.

63 Die Heartbleed-Lücke fand sich in der populären SSL-Implementierung OpenSSL, welche von zahlreichen Anbietern eingesetzt wird, siehe dazu weiterführend http://heise.de/-2166861(zuletzt abgerufen am 27. April 2014).

64 http://heise.de/-2167934(zuletzt abgerufen am 27. April 2014)

65 Gelegentlich finden sich Bedenken, Meldepflichten an staatliche Stellen könnten sich (aus Sicht der betroffenen Unternehmen) existenzgefährdend auswirken (Vertrauensverlust bei Kunden infolge Publikwerden der Sicherheitslücken), siehe http://www.wienerzeitung.at/themen_channel/wz_digital/digital_news/587388_Alle-15-Sekunden-ein-Cyber-Angriff.html. Aus unserer Sicht wäre derartigen – keineswegs immer unberechtigten – Bedenken aber viel eher durch eine strikte Einhaltung der Amtsverschwiegenheit Rechnung zu tragen.

66 Hier kommen sowohl administrative Maßnahmen (Warenverkehrsverbote für den Bereich des Binnenmarktes) wie der Einsatz des (Verwaltungs-)Strafrechts in Betracht.

67 In Österreich: RTR-GmbH bzw. Telecom-Control-Kommission.

68 Etwa nach dem Beispiel der französischen «Commission nationale de l'informatique et des libertés» (CNIL).

69 Hinsichtlich dieser Agentur verwundert deren wiederholte Befristung (siehe oben Fn. 35 bis 39), zumal dadurch die Verfolgung längerfristiger Strategien naturgemäß erschwert wird.

70 Dabei wäre u.E. eine *Bündelung von Aufgabengebieten bei einer geringen Anzahl von Stellen*einem bloßen Kooperationsgebot, das sich an eine immer größere Anzahl konkurrierender Stellen richtet, vorzuziehen, zumal dadurch wohl Synergieeffekte erzielt und Kompetenzkonflikte vermieden würden.

71 Siehe Abschnitt 3.4.

vorgesehen, allerdings müsste die derzeit noch nach Art. 3 Abs. 8 i.V.m. ErWG 24 vorgesehene – auch[72] unseres Erachtens nicht gerechtfertigte – *Ausnahme von Soft- wie Hardwareherstellern gestrichen* werden, um die Anwendung auch im Bereich der hier in Rede stehenden Sicherheitslücken und Backdoors zu gewährleisten, zumal derzeit ja auch die Rahmenrichtlinie[73] nur Telekommunikationsunternehmer, nicht aber Hard- und Softwarehersteller, verpflichtet.[74]

[Rz 39] Hinsichtlich solcher Maßnahmen ist freilich eine unionsweit enge Abstimmung unabdingbar; u.E. wäre daher, nach dem Muster des gegenwärtigen Vorschlages einer Datenschutz-Grundverordnung[75], durchaus zu erwägen, nicht, wie derzeit vorgesehen, lediglich eine Richtlinie, sondern eine *Verordnung* anzuvisieren.

4.3 Reduzierung der Abhängigkeit von nicht-europäischen Herstellern

[Rz 40] Die Effektivität des in Punkt 4.2. skizzierten verwaltungspolizeilichen Systems stiege natürlich in dem Maße, in dem nicht nur Zwischenhändler, sondern auch relevante Hersteller dieser Rechtsordnung vollumfänglich unterlägen. Mittelfristiges Ziel der europäischen Politik sollte es daher sein, darauf hinzuwirken, dass sich der Anteil europäischer Hersteller am europäischen Markt signifikant erhöhe.[76]

Mag. iur. Agnes Balthasar ist Universitätsassistentin am Institut für Europarecht, Internationales Recht und Rechtsvergleichung der Universität Wien. Kontakt: agnes.balthasar@univie.ac.at
Mag. iur. Matthias Wach ist Projektkoordinator im Bereich Derivatprodukte bei Wallstreetdocs Ltd. und besucht derzeit den Universitätslehrgang für Informations- und Medienrecht an der Universität Wien. Kontakt: matthias@wach.at
Priv.-Doz. Mag. phil. Dr. iur. Alexander Balthasar ist Leiter des Instituts für Staatsorganisation und Verwaltungsreform im österreichischen Bundeskanzleramt und lehrt Verfassungsrecht und Allgemeine Staatslehre an der Karl-Franzens-Universität Graz. Kontakt: alexander.balthasar@bka.gv.at

---

72 Vgl. bereits die Stellungnahme des Europäischen Datenschutzbeauftragten vom 14. Juni 2013, Rz. 45 und 80.

73 Siehe oben Fn. 59.

74 Art. 1 Abs. 1 dir cit, vgl. auch Punkt 1.1 des aktuellen Richtlinienvorschlages.

75 COM(2012) 11 final.

76 Derartige Bemühungen würden das Ansinnen, Daten europäischer Nutzer möglichst innerhalb Europas zu belassen sowie innereuropäischen Datenverkehr in keinem Fall über Drittstaaten zu leiten, sinnvoll ergänzen, da dadurch nicht nur eine europäische Kontrolle über Daten bzw. den Datenverkehr selbst, sondern auch über die dabei verwendeten Geräte gesichert werden könnte. Zur Initiative zum innereuropäischen Datenverkehr siehe beispielsweise http://www.focus.de/finanzen/news/europaeischer-netz-verbund-kalter-krieg-im-internet-will-merkel-microsoft-und-google-aus-europa-vertreiben_id_3624645.html.