Gutachten zu dem

Projekt RiskViz – Suchmaschine für industrielle Kontrollsysteme

Freie Universität Berlin, Fachbereich Mathematik und Informatik,
Secure Identity, Prof. Dr. Ing. Volker Roth

15. Oktober 2015

Arnd Böken
Rechtsanwalt und Notar

Assistentin: Ellen Kaiser
T +49 30 726111-475
F +49 30 7266111-333
a.boeken@gvw.com

Potsdamer Platz 8
10117 Berlin

Akten-Nr. 2840/2015 2AB

Berlin, den 15. Oktober 2015

Sehr geehrter Herr Professor Roth,

anbei erhalten Sie unser Gutachten zu dem Projekt RiskViz – Suchmaschine für industrielle Kontrollsysteme.

Für Rückfragen stehen wir gern zur Verfügung.

Mit freundlichen Grüßen

.....

Arnd Böken

Inhalt

1. Gegenstand der Untersuchung, Ergebnis in Kurzform, Haftung und Auftraggeber

1.1 Fragestellung

Gibt es rechtliche Vorgaben, die den Betrieb der Suchmaschine grundsätzlich entgegenstehen?

1.2 Untersuchungsgegenstand

Die Untersuchung bezieht sich auf das deutsche Internet, d. h. Server mit Standort in Deutschland. Sämtliche Fragen werden ausschließlich nach deutschem Recht beantwortet.

1.3 Ergebnisse in Kurzform

Scanning mithilfe der SCADACS Search Engine ist nach deutschem Recht nicht straf-bar, vorausgesetzt es werden keine Zugangssperren überwunden und das Scanning wird eingesetzt, um Sicherheitslücken aufzudecken und die Unternehmen anschlie-ßend zu warnen.

Scanning mit der SCADACS Search Engine ist nach zutreffender Auffassung in Deutschland datenschutzrechtlich zulässig, da keine personenbezogenen Daten erhoben werden. Es besteht allerdings das Risiko, dass Gerichte und Behörden es als rechtlich unzulässig ansehen, soweit natürliche Personen Inhaber der IP-Adressen sind. Es ist zu empfehlen, das Scanning solcher Adressen durch technische Maßnahmen auszuschließen.

Nach der Verfahrensbeschreibung zu dem Scanning-Verfahren besteht ein geringes Risiko einer unerwarteten Reaktion der Server auf Pre-Scanning und Scanning. Forscher und Hochschule sind verpflichtet, die Einhaltung von Sicherheitsregeln, anerkannter Standards und Empfehlungen zu prüfen sowie eine fachliche Risikobewertung vorzunehmen und in diesem Zusammenhang das Ausmaß möglicher Schäden sowie die Wahrscheinlichkeit von Schadenseintritten zu ermitteln und eine entsprechende Bewertung vorzunehmen. Vom Ergebnis dieser fachlichen Risikobewertung hängt die Zulässigkeit der einzelnen Forschungsmaßnahmen ab. Da ein gewisses Haftungsrisiko für eventuelle Schäden verbleibt, ist Voraussetzung für die Forschung, dieses Haftungsrisiko durch eine geeignete Versicherung abzudecken.

1.4 Begrenzung der Haftung

Die Haftung von Graf von Westphalen Rechtsanwälte Steuerberater Partnerschaft mbB (GvW), der Rechtsanwälte und sonstigen Mitarbeiter und Erfüllungsgehilfen wegen einer Verletzung unserer Berufspflichten unter jeglichem rechtlichen Gesichtspunkt, die im Zusammenhang mit unseren Leistungen entsteht, ist dem Mandanten gegenüber wie folgt begrenzt:

Die Haftung von GvW aus dem Mandatsverhältnis dem Mandanten sowie sämtlichen weiteren möglichen Anspruchsinhabern gegenüber ist für jeden Schadensfall insgesamt bis zum Höchstbetrag von EUR 10.000.000,00 (in Worten: Zehn Millionen) Dies gilt auch im Fall mehrerer Anspruchsteller; § 428 BGB gilt entsprechend.

Diese Haftungsbeschränkung gilt auch dann, wenn eine unmittelbar oder mittelbar mit dem Mandanten verbundene Gesellschaft oder Person Auftraggeber ist.

Die vorstehende Haftungsbeschränkung gilt nicht bei grob fahrlässiger oder vorsätzlicher Pflichtverletzung und bei Verletzung des Lebens, des Körpers oder der Gesundheit.

1.5 Auftraggeber

Dieses Gutachten wurde im Auftrag unserer Mandantin, der Freien Universität Berlin, erstellt und ist ausschließlich zur Verwendung durch die Freie Universität Berlin bestimmt. Zur Verwendung durch andere Personen ist dieses Gutachten nicht bestimmt. Dritte können hieraus keinerlei Ansprüche herleiten. GvW übernimmt Dritten gegenüber keine Haftung.

2. Sachverhalt

Grundlage unserer rechtlichen Beurteilung ist die Beschreibung von Johannes Klick und Jan-Ole Malchow, Technical Report 2013/1 Version 1 vom 3. September 2013 so-wie die erläuternde E-Mail von Professor Volker Roth vom 14. Oktober 2013 und die Dokumentation RiskViz Search Engine vom 30. Juni 2015.

Die sog. SCADACS Search Engine (SSE) wurde entwickelt, um industrielle Kontrollsysteme (industrial control systems, ICS) im Internet auffinden zu können. Zu diesem Zweck werden Bereiche von IP-Adressen gescannt und auf Dienste wie *HTTP(S), SNMP, Telnet, S7 Communication* sowie *Modbus* überprüft.

Das Scanning unterteilt sich in drei Prozessschritte:

(1) Vorbereitungsphase: Erstellen eines IP-Adressen-Pools
(2) Prescan-Phase: Prüfung, ob bestimmte Ports offen sind
(3) Scan-Phase: Herstellung einer Verbindung zu den offenen *services* und Erhalten einer gerätespezifischen Antwort/Darstellung

2.1 Die Vorbereitungsphase

SSE arbeitet mit einer Datei, die IP-Adressen enthält. Die Scanadressen müssen nicht einzeln eingegeben werden, sondern SSE verfügt über Funktionen, um einzelne IP-Adressen zu einer Liste über einen Adressraum auszudehnen.

2.2 Die Prescan-Phase

Im Rahmen des prescan-Prozesses sendet SSE TCP-SYN-Pakete an die ausgewählten IP Adressen:

Service	Packet Type	Src Port	Dst Port
HTTP	TCP-SYN	999	80
HTTPS	TCP-SYN	999	443
Telnet	TCP-SYN	999	23
S7 Com	TCP-SYN	999	102
Modbus	TCP-SYN	999	502
SNMP	UDP	999	161

Der prescan-Prozess nutzt sog. *C raw sockets*. Hierbei werden TCP-SYN-Pakete an die Netzwerkkarte gesendet. Schutzmaßnahmen werden hierbei nicht umgangen. Sobald SSE ein TCP-SYN-ACK-Paket als Antwort empfängt, wird dieses analysiert und auf die passenden TCP flags (SYN und ACK) sowie den Ziel-Port 999 hin überprüft. Wenn TCP-Pakete diese Anforderungen erfüllen, startet SSE den Scan-Prozess für die IP-Adresse.

2.3 Die Scan-Phase

2.3.1 Sammlung von Informationen über die Identität des betreffenden Geräteservices

Findet das SSE-System auf diese Weise einen offenen *port*, wird es versuchen, Informationen über die Identität des aktiven Services zu erhalten. Im Fall von *HTTP(S)* versendet SSE einen *HTTP get header* und wird den *HTTP response header* erhalten. Sehr oft enthält der *HTTP response header* Identifikationsinformationen wie den betreffenden server. SSE nutzt *curl* für HTTP(S)-Verbindungen.

Für einen *telnet-service* baut SSE eine telnet-Verbindung auf via netat und prüft diese für zehn Sekunden, bevor es die Sitzung beendet. Sämtliche Daten die während der *telnet*-Sitzung übermittelt werden, werden von SSE protokolliert.

Im Fall eines *SNMP-service* sendet SSE eine sog. *system description request* mittels OID 1.3.6.1.2.1.1.1 gemäß RFC 1157.

Für S7 Communication und Modbus nutzt SSE das Opensource-Tool PLC Scan. Dieses sendet eine sog. *protocol specific identification request* zu dem Gerät.

2.3.2 Scanning Rate

Ein kurzer Test auf einem *3 GHz quadcore System* mit vier GB RAM und einer Gigabit Netzwerkoberfläche hat gezeigt, dass SSE schon bei Einsatz auf einem einzigen CPU-Kern einen Prescan über tausende IP-Adressen pro Sekunde durchführen kann. Damit kann ein IPv4/0 Scan in 3,5 Stunden/port durchgeführt werden.

2.3.3 Tests

Tests haben gezeigt, dass einige Geräte TCP-SYN-ACK-Pakete als Antwort auf TCP-RST-Pakete des SSE senden. Jedes TCP-SYN-ACK-Pakete startet den Scan-Prozess für die betreffende IP-Adresse und das jeweilige Gerät von neuem. Die Ursache dieses Phänomens ist ungeklärt. Das Forscherteam geht allerdings davon aus, dass einige Geräte über schlecht implementierte TCP/IP *stacks* verfügen. An der Lösung dieses Problems wird derzeit gearbeitet.

2.3.4 Risiken

Es besteht das Risiko, dass ein mit dem Internet verbundenes Gerät auf eine Standard-Protokoll-Anfrage unerwartet reagiert. Dies hängt von der Implementierung oder der Qualität der eingesetzten Software ab. Das Forscherteam kann bisher keine Vorhersage über die Wahrscheinlichkeit des Eintritts einer solchen Reaktion treffen. Es hält diese aber für sehr unwahrscheinlich, da die meisten Verkäufer ihre Geräte auf ihre Standardverträglichkeit hin überprüfen würden. Das Forscherteam hat sich Siemens S7/300 und S7/1200, S7 Com-Geräte beschafft und überprüft, dass die Geräte durch das Scanning nicht beeinträchtigt werden und dass sie so wie erwartet auf die Scans antworten.

Weiterhin besteht ein geringes Risiko, dass ein Dritter mit gefälschten *prescan TCP-SYN-ACK* an das SSE-System antwortet, was einen Scan der betreffenden IP-Adresse auslösen würde. Dadurch könnte das SSE-System für DoS-Attacken missbraucht werden. Dieser Missbrauch lässt sich verhindern, indem SSE so konfiguriert wird, nur auf ACK Pakete zu antworten, die von Adressen stammen, an die zuvor Syn-Pakete gesandt wurden.

3. Strafbarkeit des Scannings?

3.1 Strafbarkeit nach § 202a StGB (Ausspähen von Daten)

Nach § 202a StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

Daten sind dann gegen unberechtigten Zugang besonders gesichert, wenn der Verfügungsberechtigte durch geeignete Schutzmaßnahmen sein Interesse zum Ausdruck gebracht hat, den Zugang zu den Daten zu erschweren (*Kargl*, in: *Kindhäuser/Neumann/Paeffgen*, Strafgesetzbuch, 4. Aufl. 2013, § 202 a, Rn. 9).

Zu der Frage, ob Portscanning nach § 202 a StGB strafbar ist, sind bisher in Deutsch-land keine gerichtlichen Urteile ergangen. Die Literatur geht ganz überwiegend davon aus, dass Portscanning nicht strafbar nach § 202 a StGB ist (*Bär*, in: *Wabnitz/Janovsky*, Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Auflage 2014, 14. Kap., § 202a StGB, Rn. 80; *Dietrich,* Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB, 2009, S. 133; *Ernst*, Hacker und Computerviren im deutschen Strafrecht, DS 2004, 14, 16; Rinker, Strafbar-keit und Strafverfolgung von „IP-Spoofing“ und „Portscanning“, MMR 2002, 663, 665).

Diese Ansicht ist zutreffend. § 202 a StGB setzt zum einen voraus, dass die Daten gegen einen unberechtigten Zugang besonders gesichert sind und der Täter die Zugangssicherung überwindet. Beide Voraussetzungen liegen beim Portscanning nicht vor. Daher sind die Handlungen in der „Prescanning“-Phase straffrei.

In der Scanningphase werden Datenpakete an die offenen Ports geschickt, damit die Anwendungsprogramme mit bestimmten Antworten reagieren, um sie zu identifizie-ren. Auch dieses „Scanning“ verschafft keinen Zugang zu Daten, die gegen unberech-tigten Zugang besonders gesichert sind, und erfolgt auch nicht unter Überwindung der Zugangssicherung. Auch hier besteht keine Strafbarkeit nach § 202a StGB.

3.2 Strafbarkeit nach § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)

Strafbar macht sich nach § 202c StGB unter anderem, wer Computerprogramme, deren Zweck die Begehung einer Straftat nach §§ 202a, 202b ist, herstellt, sich verschafft oder einem anderen zugänglich macht. Dies könnte bedeuten, dass sowohl der Besitz von SCADACS Search Engine als auch die Überlassung von SCADACS Search Engine an einen Dritten strafbar wäre.

Nach Auffassung des Bundesverfassungsgerichts ist aber bei der Auslegung und Zweckbestimmung des § 202c StGB die Entstehungsgeschichte der Norm maßgeblich zu berücksichtigen. § 202c StGB gehe auf Art. 6 Abs. 1 lit. a Nr. i des Übereinkommens des Europarats vom 23. November 2001 zurück, welcher sich ausdrücklich auf eine „Vorrichtung einschließlich eines PC-Programms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Art. 2 bis 5 umschriebene Tat zu begehen, beziehe. Entsprechend seien auch nach der Beschlussempfehlung des Rechtsausschusses nur PC-Programme gemeint, „die in erster Linie dafür ausgelegt oder hergestellt wurden, um damit eine Straftat nach den § 202a, § 202b StGB zu begehen.“ Das BVerfG ist in der Folge der Ansicht, dass bei der Auslegung des § 202c StGB von den Absichten des Programmentwicklers auszugehen sei, wobei aber zusätzlich eine äußerlich feststellbare Manifestation dieser Absichten erforderlich

sei (BVerfG, Beschluss vom 18. Mai 2009 - 2 BvR 2233/07, 2 BvR 2233-07, 1151, 1524/08 - CR 2009, 673).

Die Strafbarkeit nach § 202c StGB hängt also davon ab, welche Intention verfolgt wird. Wäre das Ziel der Untersuchung, die Informationen zu nutzen, um in fremde IT-Systeme einzudringen oder an Dritte weiterzugeben, die Sie für solche Zwecke missbrauchen, würde eine Strafbarkeit nach § 202 c StGB vorliegen. Wenn das Ziel dagegen darin besteht, Sicherheitslücken aufzudecken und einen Beitrag zur Prävention zu leisten, besteht keine Strafbarkeit nach § 202c StGB (allg. Auffassung, siehe nur *Weidemann*, in: von *Heintschel-Heinegg*, Beckscher Online-Kommentar StGB 2015, § 202c, Rn. 9 mit weiteren Nachweisen). So wie Sie uns informiert haben, dient die Forschung dazu, beispielsweise Sicherheitslücken aufzudecken und Risikoprävention zu betreiben, durch Erstellung von Risikolageberichten sowie der Schaffung von Möglichkeiten für Unternehmen, Informationen über Schwachstellen zu erhalten. Die Nutzung zielt daher nicht auf das Begehen von Straftaten ab. Daher ist der Besitz von SCADACS Search Engine nicht strafbar (zur Frage der Strafbarkeit einer Drittverschaffung s.u. 3.4.).

3.3 Strafbarkeit nach § 303a StGB und § 303b StGB

Wird das Scanning verwendet, um einen DoS-Angriff durchzuführen, liegt eine Straf-barkeit vor. Ein DoS-Angriff führt dazu, dass Daten unterdrückt werden, auch das zeitweilige Entziehen der Verwendungsmöglichkeit ist strafbar nach § 303a StGB (Datenveränderung). Die Strafbarkeit von Portscanning in Vorbereitung eines solchen Angriffs ergäbe sich dementsprechend aus § 303a Abs. 3 i.V.m. § 202c StGB. Weil die hier begutachteten Handlungen diese Intention gerade nicht verfolgen, sind sie straflos.

Bei einem Angriff auf eine Datenverarbeitung von wesentlicher Bedeutung liegt auch eine Strafbarkeit nach § 303b StGB (Computersabotage) vor (*Ernst*, Hacker und Computerviren im deutschen Strafrecht, DS 2004, 14, 17; *Rinker*, Strafbarkeit und Strafverfolgung von „IP-Spoofing“ und „Portscanning“, MMR 2002, 663, 665; *Hoeren*, Internetrecht, S. 530). Für das Portscanning gelten wegen des Verweises in § 303b Abs. 5 StGB auf § 202c StGB die Ausführungen zu § 303a StGB sowie § 202c StGB entsprechend (s.o.).

3.4 Überlassung an Dritte

Wird die SCADACS Search Engine einem Dritten überlassen und nutzt dieser die In-formationen für einen DoS-Angriff oder um Zugangssperren zu überwinden, so macht der Dritte sich strafbar.

Die Überlassung der SCADACS Search Engine an einen Dritten könnte eine nach § 27 StGB strafbare Beihilfe zu einer Tat gem. §§ 202a, 303a oder 303b StGB darstellen oder den Tatbestand der Drittverschaffung gem. § 202c StGB erfüllen. Letzteres wäre gegenüber einer Beihilfestrafbarkeit subsidiär (*Bosch*, in: *Satzger/Schluckebier/Widmaier*, StGB-Kommentar, 2. Auflage 2014, § 202c, Rn. 8).

Nach § 27 Abs. 1 StGB wird wegen Beihilfe bestraft, wer vorsätzlich einem anderen zu dessen vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat. Ein Hilfeleisten liegt in jeder Handlung, die die Herbeiführung des Taterfolges durch den Haupttäter objektiv fördert oder erleichtert (BGH NStZ 2007, 230 [232]). Der Vorsatz des Gehilfen muss dabei nicht nur den eigenen Tatbeitrag, sondern auch die Verwirklichung der Tat des Haupttäters umfassen.

Einerseits fördert die Weitergabe des Programms an Dritte eine durch diese begangene Straftat gem. §§ 202a, 303a oder 303b StGB. Denn jede Überlassung erhöht objektiv das Risiko einer Tatbegehung durch den Empfänger. Andererseits ist die Weitergabe des Programms eine berufstypische Handlung des Verfügungsberechtigten, da sie nicht ohne weiter gegen Regeln der Berufsausübung verstößt. In dieser Hinsicht ist sie strafrechtlich neutral, denn auch die Herstellung und Nutzung des Programms durch den Autor selbst ist straflos.

Die höchstrichterliche Rechtsprechung hat differenzierte Maßstäbe entwickelt, um die Grenze zwischen sozialadäquatem berufstypischen Verhalten und strafbarer Beihilfe zu ziehen (übersichtlich *Murmann*, in: *Satzger/Schluckebier/Widmaier*, StGB-Kommentar, 2. Auflage 2014, § 27, Rn. 6):

Die Rechtsprechung differenziert danach, ob einem erkennbar tatgeneigten Dritten Hilfe geleistet wird oder ob eine solche Tatneigung nicht erkennbar ist. Bestehen Anhaltspunkte dafür, dass ein Dritter die Mittel zu Straftaten verwenden will, so darf man ihm diese Mittel nicht zur Verfügung stellen. Andernfalls würde eine Solidarisierung mit dem erkennbar tatgeneigten Täter vorliegen und damit eine strafbare Beihilfe. Solche Anhaltspunkte können sich zum Beispiel daraus ergeben, dass der Dritte Ihnen seine Absicht mitteilt oder Sie auf andere Weise davon erfahren.

Bestehen solche Anhaltspunkte nicht, sondern besteht lediglich die allgemeine Möglichkeit, dass der Dritte die Gegenstände zur Begehung einer Straftat nutzt, so liegt keine strafbare Beihilfe vor (BGH, NStZ 2000, 34).

In der Praxis empfiehlt es sich, den Dritten vor Weitergabe schriftlich auf die Grenzen des zulässigen Handelns hinzuweisen und eine Verpflichtungserklärung einzuholen, wonach der Dritte die Software oder andere zur Verfügung stehende Gegenstände nicht zu diesen Zwecken nutzen wird.

Äußert er auf Befragen, dass er sie doch zu solchen Zwecken einsetzt oder ergeben sich sonst gewichtige Verdachtsmomente, so dürfen Sie ihm Software und andere Gegenstände nicht zur Verfügung stellen.

3.5 Ergebnis

Wir legen zu Grunde, dass das Scanning allein durchgeführt wird, um Sicherheitslücken zu suchen und Forschung zur Internetsicherheit zu betreiben, Risikolageberichte zu erstellen und Möglichkeiten zu schaffen, über die Unternehmen Informationen über Schwachstellen erhalten können. Wir gehen weiter davon aus, dass auch bei der Weitergabe der Software an Dritte diese Dritten belehrt werden und sich verpflichten, die Software allein zu diesen Zwecken einzusetzen.

Außerdem muss SSE so konfiguriert werden, nur auf ACK-Pakete zu antworten, die von Adressen stammen, an die zuvor SYN-Pakte gesandt worden waren. Das verhindert, dass das SSE-System für DoS-Attacken missbraucht wird.

Unter diesen Umständen besteht kein Risiko der Strafbarkeit bei der Entwicklung o-der dem Einsatz der SCADACS Search Engine.

4. Datenschutzrechtliche Zulässigkeit

4.1 Anwendbares Recht

Die Verarbeitung personenbezogener Daten durch Berliner Hochschulen unterliegt gem. § 6b Abs. 4 des Berliner Hochschulgesetzes (BerlHG) dem Berliner Datenschutzgesetz (BlnDSG). Das BerlHG, die Studentendatenverordnung oder die Satzung der Hochschule enthalten keine vorrangigen Bestimmungen. Andere Regelungen der Freien Universität, die sich mit dem Datenschutz bei solchen Forschungsprojekten befassen, sind uns nicht bekannt.

Das BlnDSG wird auch nicht durch vorrangige Vorschriften des Telekommunikationsgesetzes (TKG) oder des Telemediengesetzes (TMG) verdrängt. Der Anwendungsbereich des TKG betrifft den Datentransport an sich. Bei dem Scanning-Projekt werden vorhandene Transportwege genutzt, aber nicht angeboten. Insoweit ist die Freie Universität Berlin lediglich Nutzerin eines bereits vorhandenen Transportweges und nicht dessen Betreiber. Telemedien sind alle Informations- und Kommunikationsdienste, also Online-Auftritte. Das bloße Versenden von Datenpaketen dient weder der Information Dritter noch der Kommunikation mit ihnen.

4.2 Erhebung von IP-Adressen

Das Berliner Datenschutzgesetz regelt den Schutz personenbezogener Daten bei einer Datenverarbeitung durch Behörden und sonstige öffentliche Stellen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, § 4 Abs. 1 BlnDSG.
Als personenbezogene Daten kommen hier die IP-Adressen der untersuchten industriellen Kontrollsysteme in Betracht.

4.2.1 Statische IP-Adressen

Bei statischen IP-Adressen ist weitgehend anerkannt, dass sie sich auf eine bestimmbare Person beziehen, sofern Inhaber eine natürliche Person ist. Der Inhaber lässt sich über die entsprechenden Datenbanken ohne größeren Aufwand feststellen (h.M.; siehe aber *Meyerdierks,* Personenbeziehbarkeit statischer IP-Adressen: Datenschutzrechtliche Einordnung der Verarbeitung durch Betreiber von Webseiten, MMR 2013, 705, 706 f.: unverhältnismäßiger Suchaufwand).

4.2.2 Dynamische IP-Adressen

Dagegen gehört die Frage, ob dynamische IP-Adressen einen Personenbezug haben, zu den umstrittensten Fragen des Datenschutzrechts (*Krüger/Maucher*, Ist die IP-Adresse wirklich ein personenbezogenes Datum? Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, 433, 434 ff.).
Bei dem Folgegutachten gehen wir von einem Umfang von 25-30 Seiten aus. Der Festpreis beträgt 11.000 Euro (+ USt.).

4.2.2.1 Absolute Theorie

Nach einer Auffassung kommt es darauf an, ob überhaupt jemand in der Lage ist, die IP-Adresse einer bestimmten Person zuzuordnen. Dabei muss es sich nicht um die verantwortliche Stelle handeln; es reicht, wenn ein Dritter hierzu in der Lage ist, sogenannte absolute Theorie (*Schaar*, Datenschutz im Internet, Kap. 3, Rn. 153, 174 ff.; Karg, MMR 2011, 345, 346, so auch Schweizer BVG, Urteil vom 27.05.2009, BeckRS 2009, 22471 unter J.2.2.1).

Nach dieser Ansicht sind dynamische IP-Adressen personenbezogene Daten. Das ist auch die Auffassung der Datenschutzbehörden. Der Internetzugangsprovider speichert, welchem Nutzer die IP-Adresse zugewiesen war. Mit Hilfe dieser Kenntnis lässt sich die Zuordnung leicht vornehmen.

4.2.2.2 Relative Theorie

Demgegenüber vertritt die überwiegende Auffassung einen relativen Ansatz. Danach kommt es darauf an, ob die verantwortliche Stelle mit einem verhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft, die Person bestimmen kann. Wenn man mit diesem relativen Ansatz auf die Kenntnisse, Mittel und Möglichkeiten der verantwortlichen Stelle abstellt, können dieselben Daten für eine Stelle – etwa den Zugangsanbieter – personenbezogen und für eine andere Stelle – etwa den Anbieter einer Webseite – nicht personenbezogen sein (vgl. BGH, Beschluss vom 28.10.2014, VI ZR 135/13 Rn. 25 ff.).

Nach dieser Ansicht scheidet bei dynamischen IP-Adressen ein Personenbezug regelmäßig aus, denn der Anbieter der Webseite kann den Inhaber der Adresse nur mit unverhältnismäßigem Aufwand identifizieren. Das gilt im Regelfall auch für den Betreiber von SCADACS. Anders als bei statischen IP-Adressen gibt es keine allgemein zugängliche Datei über die Zuordnung dynamischer IP-Adressen (BGH aaO Rn. 31). Der Zugangsanbieter des Internetnutzers hat zwar die Zuordnung gespeichert, er darf aber keine Auskunft über die Identität geben.

Diese Rechtsansicht ist zutreffend, da im Regelfall keine Möglichkeit besteht, von dem Internet-Service-Provider eine Auskunft über die Zuordnung von IP-Adressen zu bestimmten Anschlussinhabern zu erhalten. Richtigerweise ist entsprechend § 4 Abs. 3 Nr. 7 BlnDSG von der Anonymität der Nutzer auszugehen, da „die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können“. In dieselbe Richtung geht die mit der Datenschutzrichtlinie (RL 95/46/EG) konforme Auslegung; denn nach Art. 2 a) i.V.m Erwägungsgrund Nr. 26 S. 2 der Richtlinie sollen zur Beurteilung der „Bestimmbarkeit“ einer Person nur solche Mittel der Personenbestimmung berücksichtigt werden, die „vernünftigerweise“ entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten. Da für Außenstehende aber in der Regel gerade keine Möglichkeit existiert, vom Service-Provider Auskunft über die Zuordnung von IP-Adressen zu erhalten, stehen ihnen insofern von vornherein keine Mittel zur Verfügung, die vernünftigerweise – d.h. insbesondere ohne Rechtsbruch – zur Erreichung dieses Ziels eingesetzt werden könnten. Für Außenstehende ist die Person folglich unbestimmbar.

4.2.2.3 Ausblick

Wegen der bestehenden Rechtsunsicherheit hat der Bundesgerichtshof die Frage der dahingehenden Auslegung von Art. 2 a) der Datenschutzrichtlinie dem Europäischen Gerichtshof vorgelegt (BGH, Beschluss vom 28. Oktober 2014 – VI ZR 135/13 – ZUM 2015, 440). Dessen Entscheidung steht noch aus.

Es steht zu erwarten, dass mit der Einführung von ipv6 der Anteil statischer IP-Adressen zunehmen wird. Sofern sich aber standardmäßig privacy extensions durch-setzen werden, die eine Zuordnung von IP-Adressen unmöglich machen, spricht viel dafür, den Personenbezug zu verneinen. Diese Fragen müssen einer zukünftigen Untersuchung vorbehalten bleiben.

4.2.3 Kein Scannen von IP-Adressen natürlicher Personen

Rechtlich problematisch sind allein die Fälle, in denen die statische IP-Adresse einer natürlichen Person zusteht. Dies betrifft nur wenige Fälle.

Das Bundesverfassungsgericht hat im Jahr 2012 darauf hingewiesen, dass bei dem Internetprotokoll v4 statische IP-Adressen im Regelfall nur an Institutionen und Großnutzer vergeben wurden, nicht aber an private Nutzer. Einzelkunden werden in aller Regel keine statischen IP-Adressen zugewiesen (s. BVerfG, Beschluss vom 24.01.2012, 1 BvR 1299/05, MMR 2012, 410, 413 Rn. 160).

Es kommt hinzu, dass Industriesteuerungen zum ganz überwiegenden Teil von Unternehmen eingesetzt werden, nicht aber von natürlichen Personen.

Wir würden empfehlen, diese Fälle durch eine technische Gestaltung auszuschließen. Hierbei ist Folgendes zu beachten:

Nach der Rechtsprechung des Bundesverfassungsgerichts liegt kein Eingriff in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung vor, wenn Kreditkartenunternehmen auf Veranlassung der Staatsanwaltschaft Kreditkartendaten maschinell auf bestimmte Suchkriterien prüfen. Voraussetzung ist, dass bei der Überprüfung ein Karteninhaber nicht als Treffer angezeigt wird, wenn die Suchkriterien nicht erfüllt wurden. Diese Personen wurden der Staatsanwaltschaft nicht übermittelt (s. BVerfG, Beschluss vom 17.02.2009, 2 BvR 1372, 1745/07, NJW 2009, 1405).

Gleiches gilt für die automatisierte Erfassung von Kraftfahrzeugkennzeichen. Wird das Kennzeichen nach der Erfassung mit dem Fahndungsbestand abgeglichen und werden die Daten in allen Fällen, in denen kein Treffer vorliegt, sofort spurlos und ohne die Möglichkeit, einen Personenbezug herzustellen gelöscht, so dass die Daten vollständig anonym bleiben, so greift dies nicht in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung ein. Dies gilt selbst dann, wenn nach einem sogenannten „unechten Treffer“ das System eine Meldung ausgibt und anschließend ein Polizeibeamter einen visuellen Abgleich des Kennzeichens vornimmt. Fällt der Abgleich negativ aus und löscht der Beamte den Vorgang dann umgehend, liegt auch hierin kein Grundrechtseingriff (BVerwG Urteil vom 22.10.2004,

6 C 7.13, BeckRS 2015, 40279, Rn. 27 ff.). Ein Grundrechtseingriff liegt dann vor, wenn ein „echter“ Treffer vergeben ist und die Daten dann weiterverarbeitet werden.

Die beiden Beispiele zeigen den Weg, auf dem sich mit Hilfe der Gestaltung einer automatisierten Erfassung die Beeinträchtigung von Betroffenenrechten vermeiden lässt.

Bei SCADACS ließe sich in ähnlicher Weise sicherstellen, dass unter keinen Umständen personenbezogene Daten verarbeitet werden. Dazu muss sichergestellt werden, dass Treffer von statischen IP-Adressen, die natürlichen Personen zugeordnet sind, ausgeschlossen werden.

Das könnte dadurch geschehen, dass bereits vor dem Scanvorgang geprüft wird, welche statischen IP-Adressen natürlichen Personen zugeordnet sind. Diese könnten dann von Pre-Scanning und Scanning ausgenommen werden.

Eine zweite Lösung bestünde darin, dass nach dem Pre-Scan bei allen Treffern maschinell überprüft wird, ob die jeweilige statische IP-Adresse einer natürlichen Person zugeordnet ist. Ist dies der Fall, muss gleichzeitig maschinell sichergestellt werden, dass die IP-Adresse aus dem Bestand gelöscht wird und keine weitere Verarbeitung erfolgt.

Aus rechtlicher Sicht wäre der Abgleich mit der RIP-Datenbank vor Beginn des Scan-vorgangs vorzuziehen, da solche IP-Adressen dann gar nicht erst gesucht werden und keinerlei Datenverarbeitung erfolgt. Sollte die zweite Lösung aus technischer Sicht vorteilhaft sein, wäre sie rechtlich ebenfalls vertretbar. Auf jeden Fall müssten die technischen Abläufe zum Löschen und die weiteren Abläufe in einer Organisationsanweisung festgelegt werden.

Eine weitere Möglichkeit, rechtliche Bedenken wegen der Verarbeitung von IP-Adressen auszuschließen, wäre die Kürzung von IP-Adressen. Dieses Verfahren setzt beispielsweise Google Analytics ein. Wird das letzte Oktett gelöscht, so ist es objektiv unmöglich, die IP-Adresse irgendwann einem konkreten Nutzer zuzuordnen. In diesem Fall entfällt bei sämtlichen Ausfällen der Personenbezug.

4.3 Persönliche oder sachliche Verhältnisse einer Person

In diesem Zusammenhang stellt sich die weitere Frage des Personenbezugs der mit der IP-Adresse verbundenen Information, ob speziell die durch Pre Scan und Scan erhaltenen Informationen personenbezogen sind.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, s. § 3 Abs. 1 BDSG.

Zu den persönlichen und sachlichen Verhältnissen gehören körperliche und geistige Eigenschaften und Merkmale einer Person, ihre sozialen, wirtschaftlichen und sonstigen Beziehungen zur Umwelt, aber auch ihre privaten Aktivitäten und Beziehungen.

Als isolierte Ziffernfolge „ohne jeden Kontext“ ist die IP-Adresse kein personenbezogenes Datum: Als Identifizierungsmerkmal mit Personenbezug wirkt sie erst, wenn sie bestimmte in den typischen Verwendungskontext der IP-Adresse fallende Angaben (etwa über den Besuch bestimmter Internetseiten, s.o.) repräsentiert. Ein Personenbezug setzt dementsprechend die Verwendung der IP-Adresse „im Kontext“ voraus (vgl. dazu Dammann, in: Simitis, Bundesdatenschutzgesetz, 7. Aufl. 2011, § 3, Rn. 10; BGH, Beschluss vom 28. Oktober 2014 – VI ZR 135/13 – ZUM 2015, 440, 442). Außerhalb des Kontexts der Verwendung einer IP-Adresse durch den betreffenden Nutzer kommt ihre Einordnung als personenbezogenes Datum hingegen nicht in Betracht.

Die Frage des Personenbezugs von IP-Adressen wird ganz überwiegend im Zusammenhang mit Webanalytics gestellt, also der Auswertung des Besucherverhaltens einer Website. Der Betreiber der Website erhält durch den Webserver die Information, welcher Nutzer mit welcher IP-Adresse die Seite besucht und wie er sich auf der Seite verhält. Im vorliegenden Fall ist es umgekehrt. Der Betreiber der Search Engine hat einen Bestand von IP-Adressen und untersucht, welche Ports auf Servern offen sind und welche Anwendungsprogramme dort laufen.

Einzelangaben über persönliche oder sachliche Verhältnisse einer Person liegen vor, wenn die erhobenen Daten auf ein Nutzerverhalten verweisen und nicht ausschließlich auf technische Zusammenhänge. Erst dann nämlich handelt es sich um Informationen mit unmittelbarem Bezug zur Person des Betroffenen (vgl. *Gola/Schumerus*, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 3, Rn. 5).

Beim Scanning sprechen die besseren Gründe gegen einen Personenbezug der Daten. Im Vordergrund steht, den Zustand eines technischen Systems zu ermitteln. Natürlich geht der Zustand im Endeffekt darauf zurück, wie der Betreiber des Servers irgendwann einmal die Einstellungen vorgenommen hat. Das ändert aber nichts daran, dass nicht diese Nutzerhandlungen ermittelt werden sollen, sondern schlicht der Zustand des technischen Systems. Die Gegenansicht ist allerdings durchaus vertretbar. Rechtsprechung zu der Frage existiert nicht.

4.4 Ergebnis

Nach zutreffender Ansicht verarbeitet SCADACS Search Engine im Regelfall keine personenbezogenen Daten. Bei dynamischen IP-Adressen fehlt es bereits an einer bestimmbaren Person. Es ist zu empfehlen, statische IP-Adressen, die natürlichen Personen zustehen, vom Scanning auszunehmen. Die Eigenschaften der Ports und die Anwendungsprogramme sind außerdem keine Angaben über persönliche oder sachliche Verhältnisse einer Person.

Allerdings verbleibt eine gewisse Rechtsunsicherheit. Zum einen bejahen die Datenschutzbehörden auch bei dynamischen IP-Adressen den Personenbezug, zum anderen liegt bisher keine Rechtsprechung zu der Frage vor, ob Angaben über Ports und Anwendungsprogramme einen Personenbezug haben.

5. Schutz von Eigentum und Vermögen Privater

5.1 Mit Forschungsvorhaben verbundene Risiken

Die bisherige Forschung hat ergeben, dass Pre-Scanning und Scanning in bisher nicht vollständig geklärten Fällen zu einem Ausfall von Servern führen können. Dies könnte Schäden an Geräten herbeiführen, die durch die entsprechende ICS gesteuert werden.

Staatliche Forschungsvorhaben dürfen keine unerlaubten Risiken für Rechtsgüter Privater mit sich bringen. Wer eine Gefahrenquelle schafft, hat eine Verkehrssicherungspflicht, § 823 ff., 839 BGB i. V. m. Art. 34 GG. Er muss die notwendigen und zumutbaren Vorkehrungen treffen, um eine Schädigung anderer möglichst zu verhindern und einen Sicherheitsgrad zu erreichen, den die in dem entsprechenden Bereich herrschende Verkehrsauffassung für erforderlich hält.

Der Forscher muss Sicherheitsvorschriften, anerkannte Standards oder Empfehlungen einhalten. In Bereichen, in denen Forschung betrieben wird, reicht die Beachtung existierender Sicherheitsstandards nicht aus, weil sie vielfach veraltet sind (vgl. BGH, Urteil vom 03.06.2008, VI ZR 223/07, NJW 2008, 3775, 3776, Rn. 9, 18). Vielmehr ist von Forschern zu erwarten, dass sie den aktuellen Stand von Wissenschaft und Technik kennen, Veröffentlichungen weltweit verfolgen und die gesammelten Erfahrungen berücksichtigen (Over, aaO S. 37 f.).

Eine Schädigung des Eigentums und Vermögens Privater verletzt deren Grundrechte. Bereits in der Gefährdung der grundrechtlichen Schutzgüter Privater durch den Staat kann ein

Grundrechtsverstoß liegen (BVerfGE 49,80 □141□; 66, 39 □57 f.□. Daher muss der Forscher eine fachliche Risikobewertung durchführen. Das bedeutet nicht, dass keinerlei Risiken eingegangen werden dürfen. Die Universität ist Träger des Grundrechts der Forschungsfreiheit nach Art. 5 Abs. 3 GG (BVerfGE 15, 256). Forschung dient der Gewinnung neuer Erkenntnisse, damit sind auch Risiken verbunden, Sie schließt das Grundrecht begriffsnotwendig mit ein (Wagner, Forschungsfreiheit und Regulierungsdichte, NVwZ 1998, 1235, 1238; vgl. zu dem Ansatz auch Over, aaO, S. 36 ff. 230).

Der Gesetzgeber hat für bestimmte besonders gefährliche Bereiche, wie z. B. die Gentechnik oder die Atomtechnik, Spezialgesetze geschaffen. Für Forschung von Hochschulen im Bereich der Internetsicherheit gibt es keine Spezialgesetze. Hier muss direkt auf verfassungsrechtliche Maßstäbe zurückgegriffen werden. Konflikte bei der Freiheitsausübung – hier zwischen Eigentums- und Wissenschaftsfreiheit – sind durch Herstellung praktischer Konkordanz zu begegnen (s. Dreier, in: ders., GG-Kommentar, Bd. I, 3. Aufl. 2013, Vorb. Rn. 120). Um zu prüfen, ob mit dem Forschungsvorhaben unerlaubte Risiken für Rechtsgüter Privater verbunden sind, muss das Forschungsinstitut eine fachliche Risikobewertung vornehmen.

5.2 Verkehrssicherung und Risikobewertung

Der Forscher unterliegt somit im Ergebnis zwei Anforderungen. Zum einen muss er die Sicherheitsvorschriften, anerkannten Standards und Empfehlungen in seinem Fachgebiet ermitteln und auf Aktualität prüfen, entsprechend dem Stand der Wissenschaft und Technik, und diese Vorgaben einhalten.

Zum zweiten muss er eine fachliche Risikoprüfung vornehmen und hierbei Ausmaß der Risiken sowie die Wahrscheinlichkeit des Schadenseintritts ermitteln und diese bewerten.

5.2.1 Verkehrssicherungspflichten

Auf Grund Ihrer Fachkompetenz haben Sie einen Überblick über die Sicherheitsvorschriften, anerkannten Standards und Empfehlungen in Ihrem Fachgebiet und deren Aktualität nach dem Stand der Wissenschaft und Technik.

In unserer Stellungnahme vom 16. Dezember 2013, insbesondere S. 13ff. hatten wir auf einige Punkte hingewiesen, die uns aufgefallen waren. Selbstverständlich sind Sie mit den Standards, Empfehlungen, Sicherheitsvorschriften in Ihrem Fachgebiet wesentlich besser vertraut. Auf Grund der technischen Zusammenhänge können Sie dies auch besser beurteilen.

Einen Punkt bitten wir gesondert zu berücksichtigen: Wir hatten der Studie des BSI aus dem Jahr 2003 entnommen, dass Portscans zur Phase 2 eines Penetrationstests gehören, sogenannter „passiver Penetrationstest“. Das BSI empfiehlt bereits vor dieser Phase eine Vorbereitung und genaue Abstimmung mit dem Auftraggeber, um hierbei auch die resultierenden Risiken zu besprechen und zu dokumentieren. Darin liegt eine Empfehlung des BSI, keine Portscans durchzuführen, ohne zuvor den Inhaber der Anlage informiert und seine Einwilligung eingeholt zu haben.

Dem liegt eine differenzierte Risikobewertung zu Grunde. In der Studie „Durchführungskonzept für Penetrationstests“ 2003 sieht das BSI als einziges Risiko einer verdeckten Durchführung von Portscans, dass der Portscan entdeckt werden könnte (BSI, Studie „Durchführungskonzept für Penetrationstests“, S. 57). Bei einer offensichtlichen Durchführung von Portscans sieht das BSI offenbar keine Risiken. Gleiches gilt für die Identifikation von Anwendungen und Diensten. SSE ermittelt in der Scanphase die laufenden Anwendungen. Auch hier sieht das BSI offenbar keine Risiken (aaO, S. 59). Ein Risiko sieht das BSI erst dann, wenn versucht wird, Informationen über das Betriebssystem, den Patchlevel-Stand und die Hardware der Systeme zu ermitteln. Hier soll das Risiko bestehen, dass die überprüften Systeme abstürzen oder in ihrer ordnungsgemäßen Funktionsfähigkeit beeinträchtigt werden könnten (aaO, S. 60).

Diese Ausführung des BSI zur Risikobewertung können Sie besser beurteilen als wir. Wir empfehlen, dass Sie Kontakt mit dem BSI aufnehmen und dort klären, inwieweit sich die Empfehlung aus dem Jahr 2003 vor Penetrationstests die Einwilligung der Betroffenen einzuholen, auch auf Ihr Scanning erstreckt, also die Anfangsphasen eines Penetrationstests.

Zum anderen müssen Sie auf Grund Ihrer Fachkompetenz prüfen, ob die Risikobewertung aus dem Jahr 2003 noch zutrifft oder ob auf Grund neuerer Erkenntnisse, beispielsweise auf Grund der Artikel von Durumeric/Wustrow/ Halderman sowie Klick und Malchow, oder auch neuer Artikel eine andere Risikobewertung erfolgen muss.

Es geht darum, wie groß die Risiken sind, dass das Scanning zu einem Schaden an der Anlage oder sonst beim Betreiber der Anlage führt. Das vom BSI genannte Risiko, dass das Portscanning entdeckt wird, ist kein Riskiko eines Schadenseintritts. Portscanning ist nicht rechtswidrig und daher ist auf Grund einer Entdeckung nichts zu befürchten.

Dabei müssen Sie auch prüfen, ob es weitere Standards, Empfehlungen oder Sicherheitsvorschriften gibt, die von Bedeutung sind.

5.2.2 Fachliche Risikobewertung

Staatliche Forschungsvorhaben dürfen keine unerlaubten Risiken für Rechtsgüter Privater mit sich bringen. Das bedeutet nicht, dass keinerlei Risiken eingegangen werden dürfen. Das Grundrecht auf Forschungsfreiheit schließt auch Risiken mit ein. Dieses Grundrecht ist mit den Grundrechten Privater in Einklang zu bringen.
Die notwendige Risikobewertung muss in drei Schritten erfolgen (BVerfG, Beschl. v. 18. Februar 2010 – 2 BvR 2502/08 –, juris, Rz. 12). In einem ersten Schritt ist festzustellen, welche Risiken sich nach Wissenschaft und Technik aus dem Forschungsvorhaben ergeben können und welche Schäden hier eintreten können. Dabei hat die forschende Stelle auf Grund ihrer Fachkenntnis eine sorgfältige und umfassende Prüfung vorzunehmen, die alle relevanten Aspekte einbezieht.

In einem zweiten Schritt ist dann zu überprüfen, wie hoch die Wahrscheinlichkeit für bestimmte Schäden ist. Auch hier hat die forschende Stelle alle ihr zur Verfügung stehenden Erkenntnisse einzusetzen.

In einem dritten Schritt ist dann eine Bewertung vorzunehmen, inwieweit die Risiken hingenommen werden können. Je größer das mit der Forschung verbundene Schadenspotenzial ist, desto niedriger ist die Schwelle hinsichtlich der Schadenswahrscheinlichkeit anzusetzen, deren Überschreitung nicht mehr hinnehmbar ist. Geht es etwa um ein Schadensereignis „apokalyptischen Ausmaßes“, so muss nach dem Stand von Wissenschaft und Technik „praktisch ausgeschlossen“ sein, dass das betreffende wissenschaftliche Vorhaben dieses Ereignis hervorruft. „Unentrinnbare Restrisiken“, wie sie großexperimentelle Grundlagenforschung mit sich bringen, sind in Kauf zu nehmen (BVerfG v. 18. Februar 2010, aaO, Rz. 14).

Hintergrund des gewisse Risiken erlaubenden Maßstabs ist der unbestreitbare gesamtgesellschaftliche Nutzen wissenschaftlicher Forschung (hierzu *Britz*, in: Dreier, GG-Kommentar, Bd. I, 3. Aufl. 2013, Art. 5 III [W], Rn. 17 m.w.N.).

Zu der Größe des Schadenspotentials und zur Wahrscheinlichkeit der Schadenseintritte können wir nichts sagen, es handelt sich hier um rein technische Fragen, die Sie beurteilen können.

Die notwendige Bewertung lässt sich erst durchführen, wenn bekannt ist, welches Schadenspotential droht und wie groß die Wahrscheinlichkeiten für Schäden sind. Bei der Bewertung ist von einem hohen Allgemeininteresse an der Forschung auszugehen, denn es geht um den Schutz einer wichtigen Infrastruktureinrichtung. Der hohe Stellenwert der Möglichkeit störungsfreier Internetnutzung ist in der Rechtsprechung mittlerweile

anerkannt, die darin ein Wirtschaftsgut von großer Bedeutung für die individuelle Lebensführung erblickt (BGH NJW 2013, 1072, 1074). Das umfangreiche BSI Kompendium zur ICS-Security vom November 2013 verdeutlicht die Bedeutung des Schutzes von industriellen Steuerungssystemen. Mehrere Presseberichte aus dem Jahr 2013 zeigen, wie schlecht an das Internet angebundene Steuerungseinrichtungen abgesichert sind. Sie zeigen auch, wie langsam Sicherheitslücken geschlossen werden.

5.3 Zuständigkeit für die Risikobewertung

Die Pflicht zur Durchführung der fachlichen Risikobewertung trifft die Körperschaft, hier die Hochschule, die in diesem Bereich von dem Präsidenten vertreten wird (vgl. § 52 Abs. 1 BerlHG). Der Forscher hat daran mitzuwirken, da er fachkundig ist. Ein enges Zusammenwirken liegt auch im Interesse aller Beteiligten, denn der beamtete Forscher trägt nach § 36 BeamtStG i. V. m. § 93 Abs. 1 BerlHG, 2 Abs. 2 S. 2 LBG Berlin die volle persönliche Verantwortung für die Rechtmäßigkeit seines Handelns.

5.4 Ergebnis der fachlichen Risikobewertung

Wenn die Prüfung ergibt, dass lediglich begrenzte Sachschäden drohen und dass die Eintrittswahrscheinlichkeit hierfür zudem nur sehr gering ist, also ein unentrinnbares Restrisiko, wenn zudem festgestellt wird, dass die Durchführung der Forschung keine Sicherheitsvorschriften, Standards oder Empfehlungen verletzt, so ist die Forschung rechtmäßig und darf durchgeführt werden.

Kommt die Prüfung dagegen zum Ergebnis, dass die drohenden Schäden hoch oder unkalkulierbar sind oder die Schadenswahrscheinlichkeit eher hoch ist und letztlich nicht nur unentrinnbare Restrisiken bestehen, so wäre die Durchführung der Forschungsmaßnahmen rechtlich unzulässig. Gleiches gilt auch, wenn die Forschung Sicherheitsvorschriften, anerkannte Standards oder Empfehlungen verletzt.

Auch ein solches Ergebnis würde nicht bedeuten, dass das Gesamtprojekt unzulässig wäre. Verboten wären die Maßnahmen, die das Risiko eines Schadens mit sich bringen oder gegen die Sicherheitsstandards etc. verstoßen. Demgegenüber wären andere Forschungsmaßnahmen erlaubt, für die das nicht gilt. Wir haben die Hinweise so verstanden, dass das Risiko möglicherweise darin besteht, die Reaktionen der Steuerungsanlagen schwer vorhersagen zu können, weil die dort verwendete Firmware nicht bekannt ist. Sofern es ohne Inkaufnahme der Risiken möglich ist, wäre es dann eine sinnvolle Maßnahme, zunächst diese Zusammenhänge näher aufzuklären, beispielsweise durch Erwerb solcher Steuerungsgeräte und Erforschen der Reaktion auf die Übermittlung von Datenpaketen.

5.5 Haftungsrisiken und Risikovorsorge

5.5.1 Verbleibende Risiken

In unserer Stellungnahme vom 16. Dezember 2013 sind wir zu dem Ergebnis gekommen, dass die Universität im Falle eines Schadenseintritts für den entstandenen Schaden haften würde. Wegen der Einzelheiten nehmen wir Bezug auf die dortigen Ausführungen.

Wie eben dargelegt, ist die forschende Stelle zur Durchführung einer fachlichen Risikobewertung verpflichtet und muss Verkehrssicherungspflichten einhalten.

Wenn die fachliche Risikobewertung dazu führt, dass die drohenden Risiken angesichts der geringen Eintrittswahrscheinlichkeit so gering sind, dass nur noch von unentrinnbaren Restrisiken gesprochen werden kann, und wenn die Verkehrssicherungspflichten eingehalten werden, so ist die Durchführung der Forschung rechtmäßig. Das könnte man einer Haftung entgegenhalten.

Allerdings verbleibt aus praktischer Sicht ein Problem, wenn später doch ein Schaden eintritt, mit dem niemand gerechnet hatte. Dann zeigen sich möglicherweise Risiken, die vorher nicht bekannt waren und die Bewertung stellt sich im Nachhinein als unzutreffend heraus. Man muss in solchen Fällen damit rechnen, dass ein erhebliches Risiko besteht, zu Schadenersatz verurteilt zu werden. Nach dem Eintritt von Schäden sieht die Lage häufig völlig anders aus, letztlich hängt die Einschätzung dann von einem Gutachten ab und der Ausgang eines Gutachtens ist in einem solchen Fall schwer vorherzusagen.

Daneben bestehen im Staatshaftungsrecht auch noch mögliche andere verschuldensabhängige und –unabhängige Ansprüche. Außerdem kann unabhängig von der Frage, ob die Forschung generell rechtmäßig ist, immer der Fall eintreten, dass bei der Durchführung bestimmte Fehler gemacht werden und die konkrete Maßnahme dann rechtswidrig und schuldhaft war.

Aus praktischer Sicht bleibt also ein Haftungsrisiko. Wir werden im Laufe des Projekts diese Fragen noch einmal im Detail untersuchen. Aus heutiger Sicht besteht aber ein solches Risiko.

5.5.2 Pflicht zur Risikovorsorge

Wegen des verbleibenden Haftungsrisikos besteht für den Forscher und die Hochschule die Verpflichtung, eine angemessene Risikovorsorge für die Hochschule und die Beteiligten zu treffen. Beamte und angestellte Forscher sind verpflichtet, ihrem Dienstherrn bzw. Arbeitgeber keinen Schaden zuzufügen und dies auch nicht in der Form, dass sie das Eigentum Dritter verletzen, die dann Schadenersatzansprüche gegen den Dienstherrn haben. Der Beamte trägt nach § 36 BeamtStG i. V. m. § 93 Abs. 1 BerlHG, § 2 Abs. 2 S. 2 LBG Berlin die volle persönliche Verantwortung für die Rechtmäßigkeit seines Handelns.

Außerdem sind Forscher und Hochschule an das Haushaltsrecht gebunden, insbesondere § 37 Abs. 1, 105 Abs. 1 Nr. 2 LHO Berlin. Das Haushaltsgeld verbietet überplanmäßige Ausgaben. Dies gilt nach § 37 Abs. 2 LHO Berlin auch für Maßnahmen, durch die Verpflichtungen entstehen können, für die Ausgaben im Haushaltsplan nicht veranschlagt sind. Dazu gehören auch Maßnahmen, die zu einer Haftung führen, für die der Haushaltsplan keine entsprechenden Mittel vorsieht. Dies gilt auch hier, da der Betrieb einer solchen Anlage immer ein Haftungsrisiko begründet. Das lässt sich vermeiden, indem eine Versicherung abgeschlossen wird, die das Risiko der Inanspruchnahme abdeckt.

Die Entscheidung darüber, in welchem Umfang Versicherungsschutz erforderlich ist, hat die Hochschule zu treffen. Es bietet sich an, diese Fragen im Zusammenhang mit der fachlichen Risikobewertung zu klären, die nach dem oben Gesagten erforderlich ist.

Wie sich aus dem Haushaltsplan ergibt, verfügt die Freie Universität über eine Haftpflichtversicherung, vgl. Haushaltsplan 2014/2015, Titel 54020. Allerdings müsste geklärt werden, ob der Versicherungsschutz gerade auch die hier bestehenden Risiken umfasst. Das gilt vor allem deshalb, weil nach dem Musterversicherungsbedingungen für die Haftpflichtversicherung Haftpflichtansprüche wegen Schäden aus dem Austausch und der Übermittlung elektronischer Daten ausgeschlossen sind, vgl. Ziff. 7.15. Weiter kommt hinzu, dass neben Haftpflichtansprüchen auch sogenannte verschuldensunabhängige Aufopferungsansprüche entstehen können und daher geklärt werden muss, ob die Versicherung auch solche Ansprüche abdecken würde. Das gilt auch für Ansprüche gegen die Forscher persönlich.

6. Kontakt

Berlin
Potsdamer Platz 8
10117 Berlin
T + 49 30 726111-0
F + 49 30 726111-333
berlin@gvw.com

Düsseldorf
Königsallee 61 – Köblick
40215 Düsseldorf
T + 49 211 56615-0
F + 49 211 56615-123
duesseldorf@gvw.com

Frankfurt am Main
Ulmenstrasse 23-25
60325 Frankfurt/Main
T + 49 69 8008519-0
F + 49 69 8008519-99
frankfurt@gvw.com

Hamburg
Poststrasse 9 – Alte Post
20354 Hamburg
T + 49 40 35922-0
F + 49 40 35922-123
hamburg@gvw.com

München
Sophienstraße 26 – Lenbach Gärten
80333 München
F + 49 89 6890 77-100
T + 49 89 6890 77-0
muenchen@gvw.com

Brüssel
227, Rue de la Loi, Level 4
1040 Brüssel
T + 32 2 4033-659
F + 32 2 4033-750
bruessel@gvw.com

Istanbul
Kanyon Ofis Binası Kat. 6
Büyükdere Cad. No. 185
34394 İstanbul
T + 90 212 381 80 00
F + 90 212 381 80 48
istanbul@gvw.com

Shanghai
Chong Hing Finance Center, Room 906
288 West Nanjing Road
200003 Shanghai
T +86 21 6322-3131
F +86 21 6322-2430
shanghai@gvw.com