Kurt Einzinger, Florian Skopik, Roman Fiedler

Keine Cyber-Sicherheit ohne Datenschutz

Datenschutzrechtliche Herausforderungen bei der Etablierung von nationalen CERTs

Bereits 18 Staaten Europas haben laut ENISA eine eigene nationale Cyber-Sicherheitsstrategie erstellt. Darin nehmen nationale Cyber-Lagezentren inzwischen eine zentrale Rolle bei der Abwehr von groß angelegten Cyber-Angriffen ein. Wurde die Informationssammlung und -verteilung über Sicherheitsvorfälle und Bedrohungen anfänglich vor allem im universitären und privaten Bereich von CERTs oder CSIRTs wahrgenommen, so ist in den letzten Jahren eine zunehmende Involvierung staatlicher Akteure festzustellen. Dadurch ergeben sich sehr spezielle rechtliche, insbesondere datenschutzrechtliche Problemstellungen. Der Beitrag geht auf diese Herausforderungen näher ein und beleuchtet exemplarisch sehr unterschiedliche Wege, die in Österreich, Deutschland und Dänemark eingeschlagen wurden.

Dr. Kurt Einzinger

ist Eigentümer der Netagentur netelligenz und Experte für Internet-Technologien, Internet-Sicherheit und Datenschutz und seit 1990 Mitglied des Österreichischen Datenschutzrates.
E-Mail: ke@netelligenz.at

Dr. Dr. Florian Skopik

arbeitet als Senior Scientist am Austrian Institute of Technology und leitet Projekte im Bereich Sicherheit kritischer Infrastrukturen.

E-Mail: florian.skopik@ait.ac.at

Roman Fiedler

ist Engineer am Austrian Institute of Technology und arbeitet in Projekten im Telehealth- und Security-Bereich.

E-Mail: roman.fiedler@ait.ac.at

1 Einleitung

Die Zahl und Komplexität von Cyber-Angriffen wächst seit Jahren rasant. Zunehmend werden sie zu einer Gefahr für die Industrie, aber auch für die Gesellschaft [1]. Konnten sich Organisationen bis in die 2000er Jahre mit allgemein erhältlichen Anti-Virenlösungen und präventiven Infrastruktur-Maßnahmen wie Netzsegmentierung und Firewalls noch hinreichend schützen, ist dies heute durch das Aufkommen zielgerichteter Attacken mit wirtschaftlichen Interessen nicht mehr ausreichend. Angriffe sind oft nicht mehr nur auf das möglichst schnelle Ausrichten eines breit angelegten Schadens ausgelegt, sondern werden in einer Vielzahl langsamer Schritte so ausgeführt, dass sich Opfer oft über Monate in Sicherheit wähnen. So haben Angreifer genügend Zeit, vertrauliche Firmendaten zu entwenden, ohne dass jemand Verdacht schöpft – ganz im Sinne klassischer Spionage.

Viele große Unternehmen haben daher ihr Sicherheitsparadigma bereits geändert: Man akzeptiert, dass Angriffe zu einem gewissen Grad gar nicht verhindert werden können – zu vielfältig sind die Angriffsmöglichkeiten in modernen hochkomplexen Netzen. Ist man jedoch Opfer eines Angriffs geworden, müssen dessen Auswirkungen möglichst schnell eingedämmt werden. Oberstes Ziel ist es daher Angriffe überhaupt erst einmal zu erkennen [1]. Zu diesem Zweck hat sich der Austausch diverser Sicherheits-sensitiver Informationen bewährt. Beispielsweise ist es durch regen Austausch sogenannter *Indicators of Compromise* (IOCs) möglich, nach Spuren von Schadsoftware im eigenen Netz zu suchen und so einen Angriff bereits in einer frühen Phase abzuwehren. Auch Informationen über *Command-Control*-Server, welche eine zentrale Rolle bei der Bekämpfung von Botnetzen

[2] spielen, aber auch Informationen über Spam-Absender, welche versuchen, Kunden auf gefälschte Internet-Banking-Seiten zu locken, oder Angreifer, welche zielgerichtete *Denial-of-Service*-Attacken durchführen, sind im internationalen Austausch für die Vermeidung erfolgreicher Angriffe unerlässlich.

Da nicht ausgeschlossen werden kann, dass es sich hierbei um personenbezogene Daten handelt, müssen die jeweiligen Bestimmungen des Datenschutzrechts eingehalten werden. Man ist sich weitestgehend einig, dass die Verwendung von personenbezogenen Daten minimiert werden muss, jedoch würde die gänzliche Vermeidung der Erhebung, Speicherung und Weiterverarbeitung personenbezogener Daten neuartige Ansätze in der Computer-Sicherheit verunmöglichen und dadurch womöglich genau das Gegenteil bewirken, nämlich die (Daten-)Sicherheit für alle verringern. Hier ist es erforderlich sehr gewissenhaft abzuwägen.

Eine zentrale Stellung in der Informationsverteilung eines Staates bei Cyber-Sicherheitsvorfällen nehmen inzwischen die nationalen Cyber-Lagezentren und GovCERTs ein. Bereits 18 Staaten Europas haben laut ENISA (*European Network and Information Security Agency*) eine eigene nationale Cyber-Sicherheitsstrategie erstellt [3]. Für die Bekämpfung und Schadensminimierung von Attacken und Schadsoftware im Internet sind Zentren zur Informationssammlung und -verteilung über Sicherheitsvorfälle und Bedrohungen wesentlicher Bestandteil der nationalen Sicherheitsstrategien. Wurde diese Aufgabe anfänglich vor allem im universitären und privaten Bereich von CERTs (*Computer Emergency Response Team*) oder CSIRTs (*Computer Security Incident Response Team*) wahrgenommen, so ist in den letzten Jahren eine Zunahme der staatlichen (öffentlichen) Stellen im Sinne des Schutzes kritischer Informationsinfrastrukturen als öffentliche Aufgabe zu bemerken. Dadurch ergeben sich aber auch spezielle rechtliche, insbesondere datenschutzrechtliche Problemstellungen.

Insbesondere ist nicht auszuschließen, dass im Informationsfluss zwischen Betreiber, IT-Security-Firmen, CERTs und der Öffentlichkeit in Erfüllung der Aufgaben eines CERTs auch personenbezogene Daten enthalten sind, wodurch sich die Übermittlung und Verwendung dieser Daten derzeit in einem rechtlichen Graubereich befindet. Beispielsweise ist im österreichischen Datenschutzgesetz (DSG 2000) dafür keine Ausnahme bzw. Ermächtigung vorgesehen. Daher stellen sich etliche Fragen nach den datenschutzrechtlichen Grundlagen:

- Welche gesetzlichen (datenschutzrechtlichen) Grundlagen bestehen für die Verwendung von personenbezogenen Daten in einem CERT (Lagezentrum)?
- Welche gesetzlichen (datenschutzrechtlichen) Grundlagen bestehen für die Übermittlung von personenbezogenen Daten von einem privaten Betreiber (Firma) an ein CERT (Lagezentrum)?
- Welche gesetzlichen (datenschutzrechtlichen) Grundlagen bestehen für die Übermittlung von personenbezogenen Daten von einem Betreiber (Einrichtung) des öffentlichen Bereichs an ein CERT (Lagezentrum)?
- Welche gesetzlichen (datenschutzrechtlichen) Grundlagen bestehen für die Übermittlung von personenbezogenen Daten von einem CERT (Lagezentrum) zu anderen CERTs (Lagezentren) oder privaten Betreibern und Einrichtungen des öffentlichen Bereichs?

Darüber hinaus muss man die Frage nach der Rechtsgrundlage zum Betrieb eines nationalen CERTs stellen, welches im öffentlichen Bereich angesiedelt ist. In den meisten europäischen Rechtssystemen kann die öffentliche Hand nur auf Grundlage von Gesetzen tätig werden. Der Betrieb eines nationalen Cyber-Security Lagezentrums (oder CERTs) durch die öffentliche Hand bedarf also auch einer gesetzlichen Ermächtigung dafür.

In einer umfangreichen Studie der ENISA aus dem Jahre 2011 werden folgende mittelfristigen Empfehlungen an die Politik für die Verbesserung der gesetzlichen Rahmenbedingungen für CERTs ausgesprochen:

- *B.1 Address legal uncertainty concerning requests*
- *B.2 Designate national/governmental CERTs on a specific regulatory footing*
- *B.3 Ensure EU-level legislation takes account of scope of national/governmental CERTs*
- *B.4 Specify threshold for incidents requiring national/governmental CERT response-sharing*
- *B.5 Articulate why CERTs need to process personal data to Article 29 Working Party [4]*

Bis heute sind jedoch nur wenige dieser Empfehlungen entsprechend in nationales oder EU-Recht eingearbeitet worden. Dieser Artikel fasst die sehr unterschiedlichen Ausprägungen in Österreich, Deutschland und Dänemark exemplarisch zusammen.

2 Situation in Österreich

In Österreich bestehen derzeit einige wenige privatwirtschaftliche bzw. akademische CERTs und ein im Bundeskanzleramt angesiedeltes GovCERT, welches in enger Verbindung mit cert.at (man könnte von einem *Public Privat Partnership* sprechen) steht, betrieben von der österreichischen Domain-Registrierungs-Gesellschaft nic.at. Weitere „Lagezentren" im öffentlichen Bereich (Bundesministerium für Inneres – BMI, Bundesministerium für Landesverteidigung und Sport – BMLVS) sind in Aufbau. Es existieren derzeit keine eigenen gesetzlichen Regelungen dafür. Das wirft die Frage auf, inwieweit die bestehenden Gesetze betreffend der Tätigkeiten der einzelnen Ministerien die Einrichtung eines nationalen CERTs abdecken können. Dies wird zu klären sein, auch wenn die Zusammenarbeit zwischen den Ministerien im Großen und Ganzen auch heute schon gut funktioniert.

2.1 Bundesministerium für Inneres (BMI)

Für die Errichtung eines CERTs innerhalb der Sicherheitsbehörden (BMI) sprächen sowohl deren gesetzlich festgeschriebenen Aufgaben der Gefahrenbekämpfung und Gefahrenerforschung als auch der vorbeugende Schutz von Rechtsgütern. Hierbei obliegt ihnen auch der besondere Schutz (Sicherheitspolizeigesetz SPG § 22 (1) 6).

Außerdem werden ihnen Auskunftsermächtigungen gegenüber Betreibern öffentlicher Telekommunikationsdienste und sonstigen Dienstanbietern gemäß E-Commerce Gesetz gewährt (SPG § 53 (3a)). Inwieweit man hiervon eine Ermächtigung zur Verarbeitung von personenbezogenen Daten im Rahmen eines Cyber-Security Lagezentrums (oder CERTs) innerhalb der österreichischen Sicherheitsverwaltung (BMI) ableiten kann, ist nicht eindeutig. So können diese Auskünfte nur auf Verlangen der Sicherheitsbehörden gegeben werden, was eine eigenmächtige Meldung von Providern an das Lagezentrum nicht einschließt.

Es könnte argumentiert werden, dass die Sicherheitsbehörden dieses Lagezentrum im Rahmen ihrer Tätigkeit zur Abwehr eines gefährlichen Angriffs und der Gefahrenerforschung (SPG § 16) betreiben und dafür das Verarbeitungsprivileg laut SPG § 53 in Anspruch nehmen können. Diese Konstruktion unterscheidet sich jedoch von den meisten anderen CERTs oder Lagezentren dadurch, dass durch die Amtswegigkeit (StPO § 2, siehe 3.4.) der Zweck eines solchen CERTs um die verpflichtende Strafverfolgung erweitert wäre. Dies hätte sicherlich Auswirkungen auf die Art der Tätigkeiten des CERTs, da die Schadensminimierung nicht allein im Vordergrund stünde, und es würde sich auch auf die Vertrauensbasis der Teilnehmer außerhalb der Sicherheitsverwaltung negativ auswirken.

Vor kurzem ist ein *Cyber Crime Competence Center* (C4) als nationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität, angesiedelt im Bundeskriminalamt entstanden. Es versteht sich als die nationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität und setzt sich aus technisch und fachlich hochspezialisierten Expertinnen und Experten aus dem Bundeskriminalamt (BK) als federführender Organisation sowie dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und dem Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK) des Bundesministeriums für Inneres zusammen [5]. Der Schwerpunkt ist hier eindeutig die Kriminalitätsbekämpfung im Cyberraum und erst in zweiter Linie die Sicherheit und Funktionalität der Informations-Infrastrukturen. Laut BMI wird zusätzlich zurzeit am Aufbau eines Cyber-Lagezentrums (CSC) gearbeitet.

Aus dem SPG kann keine Ermächtigung zur Verwendung und Übermittlung personenbezogener Daten abgeleitet werden. Private Betreiber (ISPs und Telcos) werden im SPG zwar zur Beauskunftung verpflichtet, allerdings nur auf Anfrage. Dadurch werden ISPs und Telcos nicht zur eigenständigen Informationsübermittlung bei Sicherheitsvorfällen in ihrem Bereich ermächtigt oder verpflichtet, noch wird eine datenschutzrechtliche Erlaubnis zur Übermittlung von Daten über *Incidents* erteilt, in denen personenbezogene Daten enthalten sind.

2.2 Bundesministerium für Landesverteidigung und Sport (BMLVS)

Im BMLVS wird gerade am Aufbau eines milCERTs gearbeitet. Mit der Bezeichnung „milCERT“ (*Military Computer Emergency Readiness Team*) soll die vorhandene Bereitschaft und nicht nur die Reaktion auf Sicherheitsvorfälle ausgedrückt werden. Laut Pressemeldungen besteht das milCERT aus IT-Sicherheitsexperten des Abwehramtes und des Führungsunterstützungszentrums. Das milCERT sieht sich als Teil des österreichischen CERT-Verbundes und dabei als das Koordinierungs- und Kompetenzzentrum für *Cyber Defence* im österreichischen Bundesheer. Es soll Informationen und Unterstützung für alle Kommanden und Dienststellen des BMLVS und nach Bedarf auch für andere Bundesdienststellen zur Verfügung stellen. Es soll die IKT-Sicherheit des BMLVS im Einsatz und während der Einsatzvorbereitung sicherstellen und die Cyber-Sicherheit Österreichs durch verschiedene Dienstleistungen unterstützen. Das milCERT ist jedoch nicht nachrichtendienstlich tätig.

Die Tätigkeiten der Angehörigen des BMLVS werden durch das Militärbefugnisgesetz geregelt. Bezüglich der Verarbeitung von Daten findet sich darin in MBG § 22 folgendes:

- *„(2a) Militärische Organe und Dienststellen […] dürfen von den Betreibern öffentlicher Telekommunikationsdienste jene Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses verlangen, die diese Organe und Dienststellen als wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr benötigen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.*"

Es stellt sich auch hier die Frage, inwieweit die Verwendung personenbezogener Daten im milCERT durch das Datenverarbeitungsprivileg im MBG gedeckt ist. Dazu müsste deren Tätigkeit als nachrichtendienstliche Aufklärung oder Abwehr definiert sein, was für die Akzeptanz in der CERT-Community und bei privaten und internationalen Teilnehmern nicht gerade förderlich wäre.

Eine Ermächtigung zur Übermittlung personenbezogener Daten an andere CERTs oder Cyber-Security-Zentren im In- oder Ausland ist im MBG nicht enthalten. Auf private Betreiber (ISPs und Telcos) wird im MBG nur insofern eingegangen, als dass sie zur Beauskunftung verpflichtet werden. Weder werden sie zur Informationsübermittlung an das milCERT bei Sicherheitsvorfällen in ihrem Bereich ermächtigt, noch wird eine datenschutzrechtliche Erlaubnis zur Übermittlung solcher Daten erteilt. Es ist somit möglich, dass das milCERT seinen Aufgabenbereich ausschließlich innerhalb der Organisationen des Landesverteidigungsministeriums finden wird.

2.3 Bundeskanzleramt (BKA)

Das Bundeskanzleramt ist laut dem Bundesministeriengesetz (BMG) mit folgenden Aufgaben, die in Bezug zur Tätigkeit eines CERTs stehen, betraut: (1) Koordination in Angelegenheiten der umfassenden Landesverteidigung; (2) anlassbezogene Koordination innerstaatlicher Maßnahmen zur Bewältigung überregionaler oder internationaler Krisen oder Katastrophen; und (3) Koordination in Angelegenheiten der Telekommunikation, Informationstechnologien und Medien.

Daraus ließe sich eine Legitimierung für die Führung eines nationalen CERTs ableiten. Vor allem der Koordinierungsaspekt, der zur urtümlichen Aufgabe des BKA zählt, wäre das gewichtigste Argument. Hervorgehend aus der Initiative *Computer Incident Response Coordination Austria* (CIRCA) des *Internet Service Provider Verbands* (ISPA) und des BKA wurden in Österreich im Jahr 2007 vom BKA und der *Internet Foundation Austria* (IPA) mit Unterstützung der Universität Wien das CERT.at und das GovCERT.at ins Leben gerufen. Im März 2008 wurde der operative Betrieb aufgenommen.

In seinem Leitbild sieht sich CERT.at als das österreichische nationale CERT. Als solches ist es Ansprechpartner für IT-Sicherheit im österreichischen nationalen Umfeld. Es ist vernetzt mit anderen CERTs und CSIRTs aus den Bereichen kritische IKT-Infrastrukturen und gibt auch Warnungen und Empfehlungen heraus. Bei Angriffen auf Rechner auf nationaler Ebene sieht sich CERT.at in einer koordinierenden Rolle und informiert dabei die jeweiligen Netzbetreiber und zuständige lokale Security Teams. Ausführliche Information zu CERT.at sind im RFC-2350-Format abrufbar [6]. Darin wird auch die Behandlung von (privaten) Nachrichten, Datenschutz und Vertraulichkeit angesprochen.

- *„4.2 Co-operation, interaction and disclosure of information CERT.at will cooperate with other organisations in the field of computer security. This cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. Nevertheless CERT.at will protect the privacy of reporters, partners and our constituents, and therefore (under normal circumstances) pass on information in an anonymised way only unless other contractual agreements apply. CERT.at operates under the restrictions imposed by Austrian law. This involves careful handling of personal data as required by Austrian Data Protection law, but it is also possible that – according to Austrian law – CERT.at may be forced to disclose information due to a court order."*

In Abwesenheit einer eigenen Datenschutzerklärung können diese Textstellen als eine solche aufgefasst werden.

Das GovCERT Austria ist das Government Computer Emergency Response Team für die öffentliche Verwaltung und die kritische Informations-Infrastruktur (KII) in Österreich [7]. Es wird in Personal- und Arbeits-Union mit CERT.at betrieben.

Es existieren keine gesetzlichen Ermächtigungen oder Verpflichtungen zur Meldung von Sicherheitsvorfällen an CERT.at bzw. GovCERT. Allerdings wurden mit der Novelle des Telekommunikationsgesetzes (TKG) im November 2011 spezielle Sicherheitsbestimmungen und Informationspflichten für Betreiber öffentlicher Kommunikationsdienste normiert. Dabei ist auf der einen Seite bei Sicherheitsverletzungen, die die Netzintegrität oder den Netzbetrieb verletzen, die Regulierungsbehörde (RTR) zu informieren (TKG § 16a (5)), die wiederum ausländische Regulierungsbehörden oder die ENISA verständigen kann. Falls Datenschutzverletzungen involviert sind, hat sich die Regulierungsbehörde mit der Datenschutzbehörde abzustimmen. Hierbei wird allerdings keine Ermächtigung zur Weitergabe personenbezogener Daten ausgesprochen.

3 Situation in Deutschland

In Deutschland wird CERT-Bund (*Computer Emergency Response Team für Bundesbehörden*) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben, welches durch ein eigenes BSI-Gesetz (BSIG) schon 1991 errichtet wurde. Das BSI ist eine Bundesoberbehörde und untersteht dem Bundesministerium des Innern. Dem BSI wurden mit der Novellierung des BSI-Gesetzes 2009 weitergehende Aufgaben und Befugnisse eingeräumt.

Aufgabe des BSI ist die Förderung der Sicherheit der Informationstechnik (§ 3 (1) BSIG). Darüber hinaus wurde das Bundesamt als zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in Angelegenheiten der Sicherheit der Informationstechnik gesetzlich (§ 4 BSIG) eingerichtet und verpflichtet, alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen zu sammeln und auszuwerten und die Bundesbehörden unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge zu unterrichten. Gleichzeitig werden alle anderen Bundesbehörden verpflichtet, solche Informationen dem BSI unverzüglich mitzuteilen, soweit andere Vorschriften dem nicht entgegenstehen. (§ 4 (3) BSIG)

Durch das neue IT-Sicherheitsgesetz [8] wird das BSIG wesentlich erweitert. Dadurch soll die Entwicklung hin zur nationalen Informationssicherheitsbehörde nachvollzogen werden. Dazu werden nun die kritischen Infrastrukturen einbezogen und das BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes definiert. Kritische Infrastrukturen im Sinne des Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind (§ 2 (10) BSIG). Sie werden mittels Rechtsverordnung durch das Bundesministerium des Innern näher bestimmt (§ 10 (1) BSIG).

Die Betreiber kritischer Infrastrukturen werden verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Dabei ist der Stand der Technik zu berücksichtigen (§ 8a BSIG). Darüber hinaus werden die Betreiber zur Meldung von Sicherheits- oder Störvorfällen verpflichtet. Das Bundesamt ist die zentrale Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik (§ 8b BSIG).

Werden dabei personenbezogene Daten erhoben, verarbeitet oder genutzt, ist eine über die im Gesetz definierte (§ 8b Abs. 6 BSIG-E) hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig; § 5 BSIG ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

Im § 5 des BSIG wird das BSI ermächtigt Protokolldaten (Steuerdaten die zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind (§ 2 (8) BSIG)), die beim Betrieb von Kommunikationstechnik des Bundes anfallen, zu erheben und automatisiert auszuwerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist. Des Weiteren darf das BSI die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten (§ 5 (1) BSIG). Die automatisierte Auswertung dieser Daten muss unverzüglich erfolgen und nach erfolgtem Abgleich müssen sie sofort und spurlos gelöscht werden. Diese Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten (§ 5 (1) BSIG).

Eine darüber hinausgehende Verwendung personenbezogener Daten ist nur zulässig bei Verdacht auf ein Schadprogramm oder wenn sie Hinweise auf ein Schadprogramm enthalten können und die Daten zur Überprüfung des Verdachts notwendig sind. Sollte sich der Verdacht bestätigen, ist die weitere Verarbeitung der Daten zulässig, soweit dies der Abwehr des Schadprogramms oder anderer dient (§ 5 (3) BSIG). Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen. Falls aus im Gesetz angeführten Gründen von einer Benachrichtigung abgesehen wird, so wird der Fall dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vorgelegt.

Das BSI kann personenbezogene Daten zur Verfolgung einer Straftat (mittels eines Schadprogramms oder von erheblicher Bedeutung) an die Strafverfolgungsbehörden, zur Abwehr einer Gefahr für die öffentliche Sicherheit oder für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert an die Polizeien des Bundes und der Länder und zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen an das Bundesamt für Verfassungsschutz übermitteln (§ 5 (5) und (6) BSIG).

Personenbezogene Daten, die vom BSI im Rahmen seiner Befugnisse erhoben wurden, sind unverzüglich zu löschen, sobald sie für die Erfüllung der Aufgaben, für die sie erhoben worden sind, oder für eine etwaige gerichtliche Überprüfung nicht mehr benötigt werden (§ 6 BSIG). In § 4 (5) BSIG wird festgehalten, dass die Vorschriften zum Schutz personenbezogener Daten unberührt bleiben. Demnach bleiben die Rechte des Betroffenen nach dem Bundesdatenschutzgesetz (BDSG) auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) auch vollinhaltlich für alle personenbezogenen Daten, die das BSI verwendet, bestehen (vgl. § 6 (1) BDSG).

Durch das neue IT-Sicherheitsgesetz wird auch das deutsche Telekommunikationsgesetz geändert. Damit werden die Betreiber öffentlicher Telekommunikationsnetze oder -dienste dazu verpflichtet, der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die zu beträchtlichen Sicherheitsverletzungen führen oder führen können (§ 109 (5) TKG). Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das BSI weiter. Im § 100 TKG werden die Dienstanbieter ermächtigt, soweit erforderlich Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Hinzugefügt wird nun, dass dies auch für Störungen gilt, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können (§ 100 (1) TKG).

Eine spezielle Ermächtigung des BSI zur Übermittlung personenbezogener Daten an andere CERTs oder Cyber-Security-Zentren im In- oder Ausland ist im BSIG jedoch nicht enthalten. Es darf Warnungen an die Öffentlichkeit vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen aussprechen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen (§ 7 BSIG).

4 Situation in Dänemark

In Dänemark wurde im Juni 2011 mit dem *Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats etc.* [9] die Tätigkeiten der *National IT and Telecom Agency* im Bereich IT-Warnzentrale rechtlich abgesichert. Wie der Name des Gesetzes besagt, werden damit klare gesetzliche Richtlinien für die Verwendung von personenbezogenen Daten im Rahmen des Dänischen GovCERTs gezogen. Es definiert auch das Mandat und die Kompetenzen desselben [4]. En-

de 2011 wurde die Dänische Telekom Regulierungsbehörde (*National IT and Telecom Agency*), welche bis dahin dem Ministerium für Wissenschaft, Technologie und Innovation unterstand, aufgelöst und ihre Agenden der *Danish Business Authority* und der *Danish Agency for Digitisation* übertragen. Das Internet-Warnsystem für die Regierung wurde in Richtung Militär verschoben. Ein *Center for Cyber Security* wurde innerhalb des *Danish Defence Intelligence Services* eingerichtet.

Die Platzierung des Dänischen GovCERTs innerhalb des militärischen Nachrichtendienstes löste einige Diskussionen über die Sinnhaftigkeit bzw. Problematik dieser Verknüpfung aus. Insbesondere werden dadurch Probleme bei der Zusammenarbeit des GovCERTs mit privaten Stakeholdern deutlich [10].

- *Nevertheless, one concrete securitizing measure is GovCERT, which is placed under CFCS, as mentioned earlier. In trying to secure parts of the Danish infrastructure and Danish authorities, GovCERT is the only area where an actual effort and strategy for cooperation with private companies is made (p64). (…) This clearly shows that the placement and function of CFCS pose problems for the attractiveness of GovCERT, as they are dealing with classified information while at the same time being placed under FE. (p 65)*

(CFCS = *Centre for Cyber Security*, FE = *Danish Defence Intelligence Services*, Dänisch: *Forsvarets Efterretningstjeneste*)

Im Juni 2014 wurde der *Danish Centre for Cyber Security Act* (CFCSA) erlassen, worin die Aufgaben und Kompetenzen des Centers festgeschrieben werden. Demnach hat das Center die Aufgabe Sicherheitsvorfälle, die innerhalb des Verteidigungsministeriums und anderer verbundener Behörden und der Wirtschaft auftreten, zu entdecken, zu analysieren und zur Bekämpfung beizutragen. Das CFCS wird ermächtigt, sowohl Inhaltsdaten als auch Verkehrsdaten der angeschlossenen Behörden und Firmen zu verarbeiten, wenn es zur Erreichung eines hohen Grades der Informationssicherheit der Gesellschaft dient (CFCSA § 4). Zusätzlich werden die Aktivitäten des CFCS von den sie einschränkenden Bestimmungen des *Public Administration Act* und des *Act on Processing of Personal Data* ausgenommen (CFCSA § 8) – wobei der *Act on Processing of Personal Data* auf die Tätigkeiten der Nachrichtendienste der Polizei und der Verteidigung ohnehin nicht angewendet werden darf (APPD § 2 (11)) [11].

Jede Art von Verwendung personenbezogener Daten im CFCS wird im Materiengesetz CFCSA in den Kapiteln 6 und 7 geregelt. So wird die Ermittlung personenbezogener Daten auf spezifische, explizite und berechtigte Zwecke eingeschränkt und jede spätere Verwendung darf nicht mit diesen Zwecken inkompatibel sein (CSCFA § 9). Im § 10 wird aufgeführt, unter welchen Bedingungen die Verwendung von personenbezogenen Daten durch das CFCS stattfinden darf und für sensible Daten (über Rasse oder ethnische Abstammung, politische Einstellungen, religiöse oder philosophischen Glauben, Gewerkschaftsmitgliedschaft und Gesundheitsdaten oder das Sexualleben betreffend) werden nochmals eingeschränkte Bedingungen getroffen (CFCSA § 11, § 12). In den anschließenden Bestimmungen wird auf eine gute Datenhaltung eingegangen, die es ermöglicht, falsche oder irreführende Daten schnell und verpflichtend auszubessern (CFCSA § 13) und den Personenbezug nur solange aufrecht zu erhalten wie nötig (CFCSA § 14). Im Kapitel 7 (§ 15-17) finden sich Bestimmungen zur Analyse, Beauskunftung und Löschung der Daten. Den Abschluss bilden Paragrafen über die Datensicherheit (CFCSA § 18) und die Aufsichtsbefugnisse des Finanzaufsichtsbehörde (*Finanstilsynet*) über das *Center for Cyber Security* (CFCSA §19-24).

Während also die ausführlichen Datenschutzregelungen des *Danish Centre for Cyber Security Act* viele datenschutzrechtliche Problematiken beim Betrieb von nationalen CERTs entschärfen, birgt die Eingliederung des CERTs in das Verteidigungsministerium insbesondere in den militärischen Nachrichtendienst wieder Probleme anderer Art. Dadurch erhält die Tätigkeit des CERTs eine militärische Färbung, die in der notwendigen Zusammenarbeit und dem damit verbundenen Vertrauensverhältnis mit privaten und zivilrechtlichen Organisationen als auch mit ausländischen CERTs behindernd sein kann.

5 Eine Europäische Perspektive

In Brüssel wird schon seit einiger Zeit die *Network and Information Security (NIS) Directive* [12] verhandelt, die Ende 2015 abgeschlossen sein könnte. Ziel der Richtlinie ist die Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS). Diese soll erreicht werden, indem die Mitgliedstaaten verpflichtet werden, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit untereinander zu verbessern, und indem die Betreiber kritischer Infrastrukturen und die öffentlichen Verwaltungen verpflichtet werden, geeignete Schritte zur Beherrschung von Sicherheitsrisiken zu unternehmen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden. Dafür sieht die NIS-Richtlinie für alle Mitgliedstaaten die Verpflichtung vor, ein Mindestniveau nationaler Kapazitäten zu schaffen, indem sie für die NIS zuständige Behörden einrichten, IT-Notfallteams (CERTs) bilden und nationale NIS-Strategien und nationale NIS-Kooperationspläne aufstellen. Auch soll dafür gesorgt werden, dass sich eine Kultur des Risikomanagements entwickelt und dass ein Informationsaustausch zwischen privatem und öffentlichem Sektor stattfindet. Unternehmen in den oben erwähnten besonders betroffenen Sektoren und öffentliche Verwaltungen sollen verpflichtet werden, die Risiken, denen sie unterliegen, zu bewerten sowie geeignete und angemessene Maßnahmen zur Gewährleistung der NIS zu ergreifen. Sie werden verpflichtet, den zuständigen Behörden alle Sicherheitsvorfälle zu melden, welche ihre Netze und Informationssysteme wie auch die Kontinuität kritischer Dienste und die Lieferung von Waren ernsthaft beeinträchtigen. Ebenso wird die notwendige Legalisierung der Verwendung von personenbezogenen Daten in diesen Sicherheitsstrukturen angesprochen. Die Mitgliedstaaten werden aufgefordert, eine Verarbeitung von personenbezogenen Daten, die notwendig ist, um die mit dieser Richtlinie verfolgten Ziele des öffentlichen Interesses zu erreichen, in einzelstaatliches Recht umgesetzter Form zu genehmigen.

Sollte also die Richtlinie in dieser Form in Kraft treten, dann sind die Europäischen Gesetzgeber gefordert, die jeweiligen Datenschutzbestimmungen betreffend der Verwendung von personenbezogenen Daten für Zwecke der Cyber-Security und in CERTs entsprechend anzupassen oder sie in eigenen neuen Materiengesetzen klar und umfassend zu regeln.

6 Schlussbetrachtung und Ausblick

Österreich, Deutschland und Dänemark sind unterschiedliche Wege gegangen. Während in Österreich keine legislativen Maßnahmen zum Betrieb eines nationalen CERTs vorgenommen wurden, haben sowohl Deutschland als auch Dänemark eigene gesetzliche Bestimmungen für die Tätigkeiten ihrer GovCERTs und für die datenschutzrechtliche Umgebung derselben erlassen – allerdings in gänzlich verschiedener Weise:

- In Deutschland wurde das BSI eingerichtet, welches sich im Zuge der Erkenntnis der Notwendigkeit eines nationalen CERT zum Schutze der Informations-Infrastruktur als Vehikel anbot. Obwohl dem Innenministerium zugehörig, ist das BSI als eigene Bundesoberbehörde von der Sicherheitspolizei klar getrennt und sind klare Regeln für den Umgang mit personenbezogenen Daten gesetzlich auferlegt. Allerdings beschränkt sich sein Wirkungsbereich überwiegend auf die deutschen Bundesbehörden und seit dem IT-Sicherheitsgesetz auch auf kritische Infrastrukturen.
- In Dänemark wurde das ursprünglich beim Telekom Regulator angesiedelte GovCERT in den nachrichtendienstlichen Bereich des Verteidigungsministeriums verschoben. Mit dem erst seit kurzem (Juni 2014) verabschiedeten *Danish Centre for Cyber Security Act* (CFCSA) wurde dies auch in einem eigenen Materiengesetz nachvollzogen.

In beiden Gesetzeswerken werden die datenschutzrechtlichen Rahmenbedingungen für das Verwenden von personenbezogenen Daten innerhalb des CERTs festgeschrieben. Gesetzliche Ermächtigungen oder Verpflichtungen für die Übermittlung von Meldungen werden in der deutschen Variante für Bundesbehörden ausgesprochen. Auch sind die Bundesbehörden unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge zu unterrichten. In der dänischen Variante wird von „angeschlossenen" Behörden oder Firmen gesprochen, ohne anzuführen, welcher Art (technisch oder organisatorisch) die Verbindung ist. Wenn Behörden angeschlossen sind, können mit Zustimmung sogar Inhaltsdaten und Verkehrsdaten übermittelt werden. Also eine sehr weitreichende Ermächtigung, die unter dem Vorbehalt der Verteidigung bzw. Gefahrenabwehr steht.

Die Übermittlung von Informationen, die personenbezogene Daten enthalten können, an andere in- oder ausländische CERTs oder Sicherheitseinrichtungen (z. B. ENISA) wird in beiden Gesetzen nicht explizit angesprochen.

Österreich ging einen pragmatischen Weg. Die Zusammenarbeit zwischen BKA und ISPs führte zur Einrichtung eines nationalen CERTs, welches privatwirtschaftlich geführt wird und den öffentlichen Bereich mitbetreut. Für die Verwendung von personenbezogenen Daten gibt es keine gesetzlichen Ausnahmen, vielmehr wird mit der Österreich-eigenen Datenkategorie „indirekt personenbezogen" argumentiert, deren Verwendung nicht so stark geschützt ist. Für die Übermittlung von *Incident*-Informationen mit personenbezogenen Daten an das CERT existieren auch keine datenschutzrechtlichen Ausnahmen. Durch die immer stärker werdende Bedeutung von nationalen CERTs und die Bestrebungen auf europäischer Ebene (ENISA, NIS-Richtlinie) ist es unumgänglich, die datenschutzrechtlichen Rahmenbedingungen für die Übermittlungen und Verwendung von personenbezogenen Daten in und an CERTs zu regeln.

In Österreich stehen zwei grundsätzlich unterschiedliche Wege offen, um die datenschutzrechtlich instabile Situation von CERTs und Cyber-Lagezentren in den Griff zu bekommen. Die einfachste und umfassendste Lösung wäre wohl eine Anpassung bzw. Änderung der gesetzlichen Rahmenbedingungen. Dies könnte entweder durch ein eigenes Cyber-Sicherheits-Gesetz (lex specialis) mit einem ausführlichen Datenschutzteil oder durch die Novellierung des DSG2000 und des TKG geschehen. Als zweite Möglichkeit – ohne legistische Maßnahmen – wäre die Konstruktion eines vertraglichen Auftraggeber-Dienstleister-Verhältnisses zwischen Telekom-Unternehmen, ISPs oder Infrastruktur-Unternehmen und dem CERT anzudenken, worin die datenschutzrechtlichen Fragen geregelt werden. Eine Anpassung der AGBs der Telekom-Unternehmen oder ISPs in Richtung Einverständnis des Kunden zur Datenweitergabe an ein Lagezentrum für Sicherheitszwecke wäre zusätzlich förderlich.

Danksagung

Recherchen zum Artikel wurden im Zuge des Forschungsprojekts CIIS durchgeführt. CIIS wird im österreichischen Sicherheitsforschungsprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie finanziell unterstützt.

Literatur

[1] Ponemon Institute: *Cost of Cyber Crime Study: United States – Benchmark Study of U.S. Companies*, October 2013

[2] Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A.: *A multifaceted approach to understanding the botnet phenomenon*. In: Proceedings of the 6th ACM conference on Internet measurement, 2006 (pp. 41-52).

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[4] ENISA: *A flair for sharing – encouraging information exchange between CERTs, A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe*, November 2011.

[5] https://www.onlinesicherheit.gv.at/nationale_sicherheits-initiativen/meldestellen/71347.html

[6] RFC 2350: http://cert.at/about/rfc2350/rfc2350.html

[7] http://www.govcert.gv.at/home/index/index.html

[8] http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html?nn=3446780

[9] Folketinget: *Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats etc.*, 2011 https://www.govcert.dk/gcdata/uk_version_l197.pdf

[10] Sofia Lisa Dinesen, Heidi Bruvik Sæther: *Cyber Security: Securitizing cyber threats in Denmark*. Denmark 2013. http://studenttheses.cbs.dk/bitstream/handle/10417/3949/sofia_lisa_dinesen_og_heidi_bruvik_saether.pdf

[11] The Act on Processing of Personal Data, http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/

[12] Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, Brüssel 7.2.2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf