DATENSCHUTZFREUNDLICHER INFORMATIONSAUSTAUSCH ZWISCHEN CSIRTS

Erich Schweighofer / Vinzenz Heussler / Janos Böszörmenyi / Peter Kieseberg

Ao. Universitätsprofessor, Universität Wien, Arbeitsgruppe Rechtsinformatik (DEICL/AVR)
Schottenbastei 10-16/2/5, 1010 Wien, AT
Erich.Schweighofer@univie.ac.at, http://rechtsinformatik.univie.ac.at

Wissenschaftlicher Mitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
vinzenz.klaus.heussler@univie.ac.at; http://rechtsinformatik.univie.ac.at

Wissenschaftlicher Mitarbeiter, Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT und Doctoral Fellow, Hebrew University of Jerusalem
janos.boeszoermenyi@univie.ac.at

Senior Researcher und Forschungskoordinator, SBA Research
Favoritenstraße 16, 1040 Wien, AT
pkieseberg@sba-research.org; https://www.sba-research.org/

Schlagworte: ***NIS-Richtlinie, CSIRTs, Informationsplattform, Datenschutz***

Abstract: *CSIRTs müssen potentiell personenbezogene Daten über Sicherheitsvorfälle austauschen. Ohne eine Privacy By Design-Lösung könnte das Datenschutzrecht, der Schutz von Wirtschaftsgeheimnissen bzw. das Strafrecht verletzt werden. Es wird eine Informationsplattform der CSIRTs vorgeschlagen, wo in kodierter Form Sicherheitsvorfälle berichtet werden. Ohne Kenntnis weiterer personenbezogener Daten kann nur Quantität, Region und Branche der Angriffe herausgelesen werden. Mit weiteren Daten – vornehmlich aus eigenen Sicherheitsvorfällen – ist eine Ähnlichkeit zu anderen Vorfällen berechenbar.*

1. Einleitung

Daten, Information und Wissen sind der Rohstoff des Wissens- und Netzwerkzeitalters und werden gemeinhin als das «Öl des 21. Jahrhunderts» bezeichnet. Information ist jedoch, ganz im Unterschied zu Grund und Boden oder Industriegütern, beliebig vervielfältigbar. Der persönliche und wirtschaftliche Wert der Information wird durch jede Teilung, und somit bei jedem Informationsaustausch, beeinflusst. Dem Austauschen von Informationen sind daher in der virtuellen wie auch in der analogen Welt rechtliche Grenzen gesetzt. Was weitergegeben bzw. veröffentlicht werden kann, ergibt sich erst nach Prüfung der einschlägigen Rechtsvorschriften.

In Zusammenhang mit Sicherheitsvorfällen im Bereich der Netz- und Informationssicherheit ist es für eine effektive Bewältigung jedoch von Nöten, Informationen zu sammeln und auszutauschen, woraus sich u.a. datenschutzrechtliche Problemstellungen ergeben können. Eine besondere Rolle bei der Sammlung von relevanten Informationen und deren Austausch kommt den Computer Security Incident Response Teams (CSIRTs) zu, welche gleichsam einer Feuerwehr (Früh-)Warnungen ausgeben und im Falle von Sicherheitsvorfällen bei der Bewältigung mitwirken. Im Folgenden soll daher ein technischer Lösungsweg in Form einer Informationsplattform der CSIRTs vorgeschlagen werden, wo unter Berücksichtigung des Privacy By Design-Prinzips in kodierter Form Sicherheitsvorfälle berichtet werden.

2. NIS-Richtlinie

Zunächst soll auf den einschlägigen unionsrechtlichen Rahmen im Bereich der Sicherheit von Netz- und Informationssystemen (NIS) eingegangen werden. Die Europäische Union (EU) erachtete einen umfassenden Ansatz auf Unionsebene für erforderlich, um wirksam auf die Herausforderungen im Bereich der Sicherheit von NIS reagieren zu können. Vor diesem Hintergrund wurde die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen[1] (NIS-Richtlinie) erlassen. Die NIS-Richtlinie ist von den Mitgliedstaaten bis zum 9. Mai 2018 in nationales Recht umzusetzen.[2] Diese Umsetzung wird in Österreich durch ein in Ausarbeitung befindliches «Bundesgesetz über die Cybersicherheit» erfolgen.

Allgemein legt die NIS-Richtlinie Maßnahmen fest, mit denen ein hohes gemeinsames Sicherheitsniveau von NIS in der EU erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.[3] Im Wesentlichen soll dieses hohe Level an Sicherheit von NIS durch eine Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten (strategische Koordination und operationelle Kooperation) sowie durch die Einführung verpflichtender Sicherheitsstandards, eines angemessenen IT-Risikomanagements und der Meldepflicht signifikanter Störfälle erreicht werden.

In Kapitel II der NIS-Richtlinie wird ein nationaler Rahmen für die Sicherheit von NIS normiert. Als Bestandteil dieses nationalen Rahmens sieht Art. 8 entsprechende Behörden vor. So haben die Mitgliedstaaten eine (oder mehrere) für die Sicherheit von NIS zuständige nationale Behörde(n) zu benennen («zuständige Behörde»),[4] deren Aufgabe die Überwachung der Anwendung der Richtlinie auf nationaler Ebene ist.[5] Ferner haben die Mitgliedstaaten eine für die Sicherheit von NIS zuständige nationale zentrale Anlaufstelle («zentrale Anlaufstelle» – Single Point of Contact) zu benennen,[6] welche als Verbindungsstelle zur grenzüberschreitenden Zusammenarbeit mit den Behörden der Mitgliedstaaten sowie mit der in Art. 11 genannten Kooperationsgruppe und dem in Art. 12 genannten CSIRTs-Netzwerk dient.[7]

Der nationale Rahmen für die Sicherheit von NIS umfasst gemäß Art. 9 weiters sogenannte Computer-Notfallteams (Computer Security Incident Response Teams – CSIRTs), wobei die Richtlinie unter dem Begriff CSIRT auch Computer Emergency Response Teams (CERTs) versteht.[8] Jeder Mitgliedstaat hat ein oder mehrere CSIRTs zu benennen. Dabei kann ein CSIRT auch innerhalb einer zuständigen Behörde eingerichtet werden. Die CSIRTs sind für die Bewältigung von Risiken und Vorfällen nach einem genau festgelegten Ablauf zuständig.[9]

Die Anforderungen an die CSIRTs werden insbesondere in Anhang I Nr. 1 beschrieben. Diese Anforderungen sind laut Anhang I angemessen und genau festzulegen und durch nationale Strategien und/oder Vorschriften zu stützen. So haben CSIRTs u.a. für einen hohen Grad der Verfügbarkeit ihrer Kommunikationsdienste zu sorgen, indem sie mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst Kontakt aufnehmen können. Die Kommunikationskanäle müssen zudem genau spezifiziert und den CSIRT-Nutzern («Constituency») und den Kooperationspartnern wohlbekannt sein. Ferner müssen aus Gründen der Betriebskontinuität CSIRTs auf eine Infrastruktur gestützt sein, deren Verfügbarkeit sichergestellt ist.

---

1 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 2016/194, 1.

2 Art. 25 Abs. 1 NIS-Richtlinie.

3 Art. 1 Abs. 1 NIS-Richtlinie.

4 Art. 8 Abs. 1 NIS-Richtlinie.

5 Art. 8 Abs. 2 NIS-Richtlinie.

6 Art. 8 Abs. 3 NIS-Richtlinie.

7 Art. 8 Abs. 4 NIS-Richtlinie.

8 Vgl. ErwG 34 NIS-Richtlinie.

9 Art. 9 Abs. 1 NIS-Richtlinie.

Auch die Aufgaben der CSIRTs werden in Anhang I geregelt. Demnach umfassen die Aufgaben der CSIRTs u.a. die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern. Des Weiteren haben sie zur Erleichterung der Zusammenarbeit die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken sowie Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen zu fördern.

Hervorgehoben sei hier weiters, dass die Mitgliedstaaten sicherzustellen haben, dass ihre CSIRTs Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben.[10]

3. Datenschutzproblematik

Um Bedrohungen für die Sicherheit der NIS beispielsweise durch Cyberangriffe effektiv bewältigen zu können, müssen Informationen gesammelt und ausgetauscht werden. Die Informationsgewinnung dient dabei dem Ziel, die Prävention und die Reaktion im Umgang mit Cyberbedrohungen zu unterstützen. Wenn z.B. einer Organisation bekannt ist, dass von einer bestimmten IP-Adresse Angriffe ausgehen bzw. dass bestimmte Angriffsmethoden genutzt oder bestimmte Ziele anvisiert werden, so könnte diese Information bei anderen Organisation zur Schadensverhinderung oder -minimierung beitragen.[11] Auch Logdaten, Spamfilter, Sperrlisten und andere Formen der Datenzusammenstellung können IP-Adressen enthalten. Dabei kann nicht ausgeschlossen werden, dass personenbezogene Daten verarbeitet werden. Gerade IP-Adressen können nach einer bedeutenden Entscheidung des EuGH im Jahr 2016 personenbezogene Daten darstellen.[12] Obgleich die NIS-Richtlinie das Erfordernis des Informationsaustausches erkennt, legt sie keine eigenen datenschutzrechtlichen Vorschriften fest.[13] Sie erwägt nur allgemein, dass sie in Einklang mit diversen Rechten und Grundsätzen, wie z.B. der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten oder der unternehmerischen Freiheit, steht und im Einklang mit diesen umgesetzt werden sollte.[14]

Da ein CSIRT sehr wahrscheinlich personenbezogene Daten, die es beispielsweise von einem Betreiber eines wesentlichen Dienstes in Erfüllung der Meldepflicht bei einem Sicherheitsvorfall gemäß der NIS-Richtlinie erhält, verarbeitet, bedarf das CSIRT einer rechtlichen Grundlage für das Verarbeiten dieser Daten. Noch ist die zentrale Rechtsgrundlage für das Datenschutzrecht in Österreich das Datenschutzgesetz 2000[15] (DSG), welches die europäische Datenschutzrichtlinie (DSRL)[16] umsetzt. Doch wurde am 27. April 2016 die Datenschutz-Grundverordnung (DSGVO)[17] beschlossen, die ab 25. Mai 2018 anzuwenden ist und das DSG ablösen wird. Die DSGVO sieht in Erwägungsgrund 49 vor, dass die Verarbeitung von personenbezogenen Daten durch CSIRTs ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellt, wie dies für die Gewährleistung

---

10 Art. 9 Abs. 3 NIS-Richtlinie.

11 Kuratorium Sicheres Österreich, KSÖ Rechts- und Technologiedialog – Whitepaper, Version 2, Wien 2016, S. 20.

12 EuGH 19. Oktober 2016, C-582/14, *Breyer/Deutschland*.

13 Vgl. Art. 2 NIS-Richtlinie sowie ErwGr. 72, welcher Folgendes besagt: «Der Austausch von Informationen über Risiken und Vorfälle in der Kooperationsgruppe und im CSIRTs-Netzwerk und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRTs könnte die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung sollte mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates und der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vereinbar sein. Bei der Anwendung dieser Richtlinie sollte je nach Einzelfall die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates gelten.»

14 Vgl. ErwGr. 75.

15 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000; DSG 2000), BGBl I 1999/165 i.d.F. BGBl I 2015/132.

16 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

17 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

der NIS unbedingt notwendig und verhältnismäßig ist. Ein solches berechtigtes Interesse wird auch Behörden, Betreibern von elektronischen Kommunikationsnetzen und -diensten sowie Anbietern von Sicherheitstechnologien und -diensten «zugestanden».

Abseits von Meldepflichten besteht aber auch ein Interesse am freiwilligen Informationsaustausch, welchem die Absicht zugrunde liegt, das Verständnis von Unternehmen und Behörden zu Cybergefahren unabhängig von einem konkreten Anlassfall zu verbessern.[18] Hier stehen die gegenseitige Hilfe und der Erfahrungsaustausch im Umgang mit Gefahren und geeigneten Präventions- und Abwehrmaßnahmen im Vordergrund, und zwar schon bei Auffälligkeiten, die nicht das Ergebnis eines Angriffs oder einer technischen Störung sein müssen.[19] Als rechtliche Fragestellungen ergeben sich diesbezüglich u.a. folgende Aspekte: Werden hier personenbezogenen Daten ausgetauscht? Welchem Zweck dient der Austausch? Wer sind die Empfänger? Welche Datensicherheitsmaßnahmen werden beim Austausch ergriffen? Ein berechtigtes Interesse zum freiwilligen Austausch von personenbezogenen Daten zwischen CSIRTs oder Betreibern kritischer Infrastrukturen kann diesbezüglich nicht aus ErwGr. 49 DSGVO abgeleitet werden, zumal stets nur ein berechtigtes Interesse des jeweiligen Verantwortlichen angenommen wird.

Um einen solchen Informationsaustausch dennoch zu ermöglichen, können technische Lösungen angedacht werden, die den Grundsätzen für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO entsprechen. So sollen beispielsweise nur jene Daten ausgetauscht werden, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind («Datenminimierung»). Auch soll die Verarbeitung personenbezogener Daten in einer Weise stattfinden, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können («Pseudonymisierung»). Diese Maßnahmen können als Privacy by Design-Lösungen i.S.d. Art. 25 DSGVO verstanden werden.

4. Der Datenaustausch zwischen Geldwäschemeldestellen als Beispiel für eine datenschutzfreundliche Lösung?

Die Geldwäschemeldestellen (auf Englisch *Financial Intelligence Units*; «FIUs») der EU haben eine Technologie entwickelt, die zur Darstellung einer datenschutzfreundlichen Ausgestaltung des Informationsaustausches herangezogen werden kann. Das dezentrale Computernetzwerk der europäischen FIUs, «FIU.net», wurde im Jahr 2000 von der niederländischen FIU initiiert und nahm im Jahr 2002 den Betrieb auf.[20] Die Integration in die Strukturen von «EUORPOL», wo es heute zum Einsatz kommt, erfolgte mit Anfang des Jahres 2016.[21]

Von Udo Kroon, einem der Entwickler von FIU.net, wird die Technologie als umgekehrte «Cloud» («cloud inside out») bezeichnet, da es über eine dezentralisierte Architektur verfügt, in der die Informationen physisch jeweils bei der Stelle (Behörde) verbleiben, die sie zur Verfügung stellt. Diese Architektur hat aus datenschutzrechtlicher Sicht den Vorteil, dass Speicherung, Verarbeitung und Analyse der Daten lokal stattfinden und somit eine höhere Datensicherheit gewährleistet werden kann, u.a. da sie nicht übermittelt werden müssen. Für die Behörden ist dieses Modell attraktiv, weil sie für die Verarbeitung ihrer Daten die jeweils für sie geltenden (d.h. in diesem Zusammenhang: nationalen) Rechts- und Verwaltungsvorschriften anwenden können («flexibility by design»).[22]

---

[18] Diese Art des freiwilligen Informationsaustausches darf nicht verwechselt werden mit der freiwilligen Meldung i.S.d. Art. 20 NIS-Richtlinie, welche sehr wohl auf Sicherheitsvorfälle abstellt, aber auch Einrichtungen erfassen will, die nicht als Betreiber wesentlicher Dienste ermittelt wurden.

[19] Kuratorium Sicheres Österreich (Fn. 12), S. 25 f.

[20] Vgl. Wikipedia: https://nl.wikipedia.org/wiki/Gebruiker:FIU.NET (alle Internetquellen aufgerufen am 6. Februar 2017).

[21] Vgl. EUROPOL, EUROPOL joins forces with EU FIUs to fight terrorist financing and money laundering, https://www.europol.europa.eu/newsroom/news/europol-joins-forces-eu-fius-to-fight-terrorist-financing-and-money-laundering.

[22] Udo Kroon, Ma^{3}tch: Privacy AND Knowledge, 2013 IEEE International Conference on Big Data.

Grundlage für die Zusammenarbeit der Geldwäschemeldestellen der EU ist insbesondere der Beschluss 2000/642/JI des Rates.[23] Durch die 4. Geldwäsche-Richtlinie, der die EU-Mitgliedstaaten bis 26. Juni 2017 nachzukommen haben, soll diese Kooperation weiter vertieft werden. Der österreichische Gesetzgeber ist dieser Verpflichtung durch das Finanzmarkt-Geldwäschegesetz[24] bereits nachgekommen, wobei einige Bestimmungen erst am 26. Juni 2017 in Kraft treten werden.

Die 4. Geldwäsche-Richtlinie nennt FIU.net sowohl in ihren Erwägungsgründen (56) als auch im operativen Teil (Art. 51, 53 und 56) explizit und verpflichtet die Mitgliedstaaten ihren Geldwäschemeldestellen, die Kommunikation über FIU.net nahe zu legen (Art. 56). Dies ist grundsätzlich zu begrüßen, denn der Austausch von Daten zwischen den EU-Geldwäschemeldestellen ist auf eine datenschutzfreundliche Basis zu stellen. Alle sogenannten «Verpflichteten»[25] und somit die bedeutendsten Berufsgruppen, die im Umgang mit Bargeld oder Wertgegenständen tätig sind, haben ungewöhnliche oder verdächtige Transaktionen an die FIU in ihrem Mitgliedstaat zu melden. Diese Meldungen werden von der FIU analysiert und bei Verdacht einer strafbaren Handlung an die Strafverfolgungsbehörden weitergeleitet. Insbesondere bei Kreditinstituten fallen aufgrund des Einsatzes von Software zur Erfüllung ihrer Sorgfaltspflichten (z.B. Identifikation, Abgleich der Daten von Kunden oder der wirtschaftlichen Eigentümer mit Überwachungslisten und Transaktionsüberwachung) sehr große Mengen von Daten für die Geldwäschebekämpfung an.[26]

Die Zahl der Verdachtsmeldungen ist in Österreich relativ gering.[27] Anders sieht es jedoch in einigen anderen EU-Mitgliedstaaten aus, hauptsächlich weil aufgrund unterschiedlicher Kriterien die Verdachtsmeldungen zu erstatten sind. Besonders viele Verdachtsmeldungen (237‘431 im Jahr 2015)[28] fallen z.B. in den Niederlanden an. In Anbetracht dieser Zahlen ist es verständlicher, weshalb ein System wie FIU.net und die Ma^{3}tch-Technologie entwickelt wurde.

«Ma^{3}tch» wurde auf das oben beschriebene FIU.net aufgebaut. Hierbei handelt es sich um einen Abgleich anonymisierter (in Hashwerte umgewandelter) Daten nach dem «Hit-/No-Hit-Prinzip». Die Daten werden nur als Codes ausgetauscht, wobei insbesondere personenbezogene Daten durch asymmetrische Verschlüsselung anonymisiert werden. Da alle Geldwäschemeldestellen das gleiche Verfahren verwenden, kommt es bei Vorliegen eines gleichen oder sehr ähnlichen Vorfalls zu einem gleichen bzw. ähnlichen Verschlüsselungscode mit positivem Abgleich. Aufgrund dessen wird ein Ermittlungsverfahren aufgrund ausreichender Verdachtsmomente gestartet und es werden die echten Daten zwischen den Geldwäschemeldestellen ausgetauscht. Dieses Verfahren entspricht den Prinzipien des «Privacy by Design» und der «Datenminimierung».

Durch die Ma^{3}tch-Technologie werden personenbezogene Daten in anonymisierte Filter verwandelt. Der Filter enthält allerdings nur einen Code aus vier Zeichen, der nicht zurückverfolgt werden kann. Balboni und Macenaite beschreiben dieses Verfahren als «hashing the hash», da es grundsätzlich nicht möglich ist, die Identität der Personen hinter dem Code herauszufinden (anonymous). Welche Informationen in den Filter aufgenommen werden, wie lange der Filter gültig ist und mit wem er geteilt wird, entscheidet die Behörde, die den Filter erstellt (autonomous). Teilt FIU A seine Filter mit FIU B, kann FIU B diese Filter mit seinen lokalen Informationen integrieren, erst zu diesem Zeitpunkt können Informationen gefunden werden.

---

23 Beschluss des Rates vom 17. Oktober 2000 über Vereinbarungen für eine Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen, ABl L 2000/271, 4.

24 Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt, BGBl I 2016/118.

25 Z.B. Kredit- und Finanzinstitute, Wirtschaftsprüfer, Steuerberater, Notare, Rechtsanwälte, Immobilienmakler, Gewerbetreibende und Anbieter von Glücksspieldiensten.

26 Schweighofer, Böszörmenyi, BILETA.

27 Gemeldet wurden 1’255 Verdachtsfälle im Jahr 2013, 1‘507 Verdachtsfälle im Jahr 2014 und 1‘755 Verdachtsfälle im Jahr 2015 (vgl. Bundesministerium für Inneres, Geldwäschejahresbericht 2015, S. 16, http://www.bmi.gv.at/cms/BK/publikationen/files/Web_Geldwsche_2015.pdf).

28 FIU-Netherlands, Annual Report 2015, S. 35, http://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/fiu_jaaroverzicht_2015_eng.pdf.

In einer Studie über *EU Financial Intelligence Units («FIUs») using the Ma³tch technology as additional feature to the existing exchange of information* wurde die Ma³tch Technologie aus der Sicht des Datenschutzes sehr positiv gesehen, weil damit die Prinzipien des Privacy by Design und der Datenminimierung erzielt werden, insbesondere weil personenbezogene Daten anonymisiert werden. Die Kodierung garantiert aber auch ein ausreichendes Matching von gleichen oder ähnlichen Fällen. Die Studie hat auf die Notwendigkeit von organisatorischen wie technischen Verfahren hingewiesen, damit der Datenschutz gewährleistet ist. Die Einführung war jedoch trotzdem von gewisser Verunsicherung gekennzeichnet und hat auch zu einer Anfrage im deutschen Bundestag geführt.[29]

Obwohl der Informationsaustausch über Ma³tch grundsätzlich positiv einzustufen ist, sollten die potentiellen Gefahren dieser Technologie nicht übersehen werden. Ma³tch kann viel mehr als nur den Austausch personenbezogener Daten in anonymisierter Form und über sichere Kanäle ermöglichen. Ma³tch soll auch Wissen generieren und unter anderem Profile erkennen und Verhaltensmuster vorhersagen. Auch die Analyse sozialer Netzwerke wird von den Entwicklern der Ma³tch-Technologie angestrebt.[30] Welche datenschutzrechtlichen Implikationen diese Anwendungsfelder haben könnten und inwiefern sie in der Praxis bereits verwendet werden, kann an dieser Stelle nicht mehr behandelt werden. Weiters muss darauf hingewiesen werden, dass bisher keine Sicherheitsüberprüfung dieser Technologie veröffentlicht wurde.

5. Definition und Modellierung des Sicherheitsvorfalls

Die NIS-Richtlinie sieht eine Meldepflicht für Betreiber wesentlicher Dienste[31] sowie Anbieter digitaler Dienste[32] vor, wenn ein Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit des bereitgestellten Dienstes hat. Die Meldung hat unverzüglich an die zuständige Behörde oder das CSIRT zu ergehen. Als Sicherheitsvorfall definiert die NIS-Richtlinie «alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben»[33]. Es werden einige Parameter demonstrativ aufgelistet, welche zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls zu berücksichtigen sind und die den breiten Begriff des Sicherheitsvorfalles folglich präzisieren. Die Parameter für Betreiber wesentlicher Dienste umfassen die Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer, die Dauer des Sicherheitsvorfalls sowie die geografische Ausbreitung.[34] Für Anbieter digitaler Dienste sind die Parameter die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, die Dauer des Sicherheitsvorfalls, die geografische Ausbreitung, das Ausmaß der Unterbrechung sowie die Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten,[35] wobei die Kommission bei Anbietern digitaler Dienste bis zum 9. August 2017 Durchführungsrechtsakte zu erlassen hat, um diese Parameter genauer zu bestimmen.[36] Für Betreiber wesentlicher Dienste wären der Begriff des Sicherheitsvorfalls und die Parameter auf nationaler Ebene näher festzulegen.

In einem Sicherheitsvorfall sind mehrere Dimensionen für die Betreiber eines CSIRT relevant, von denen einige datenschutzrechtlich schwierige Komponenten aufweisen. Zusätzlich ist auch wichtige Information enthalten, die zwar datenschutzrechtlich gesehen harmlos, für die Betreiber der jeweiligen Infrastruktur aber sehr schützenswert sind. Dies betrifft vor allem interne Abläufe sowie natürlich das Faktum einer (möglichen) Verwundbarkeit durch einen Angriff selbst.

---

29 Deutscher Bundestag, Drucksache 18/6239, 2. Oktober 2015. Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE.

30 Kroon (Fn. 23).

31 Art. 14 Abs. 3 NIS-Richtlinie.

32 Art. 16 Abs. 3 NIS-Richtlinie.

33 Art. 4 Z 7 NIS-Richtlinie.

34 Art. 14 Abs. 4 NIS-Richtlinie.

35 Art. 16 Abs. 4 NIS-Richtlinie.

36 Art. 16 Abs. 8 NIS-Richtlinie.

Im Rahmen von noch unveröffentlichten Analysen wurden die folgenden relevanten Informationspartikel identifiziert:

- ***Absenderinformationen***: Absender und Sektor einer kritischen Infrastruktur, Kontaktinformationen.
- ***Angriffsinformationen***: Systemlevel, betroffene Komponenten, Spezifität des Angriffs (Targeted Attack oder allgemeiner Ansatz), ähnliche Ziele, Beschreibung des Angriffs (wenn vorhanden), CVE-Link (wenn Angriff schon bekannt) oder Link zu einer Angriffssoftware (falls bekannt).
- ***Angreiferinformationen***: IP(s), Benutzernamen (intern und extern); speziell im Fall von DDOS-Angriffen (u.U. mit Amplification) kann die Liste der betroffenen IPs stark anwachsen; zusätzlich werden den IPs Zeitstempel zugewiesen, die das Intervall angeben, in dem Angriffe von der jeweiligen IP festgestellt werden konnten; E-Mail-Adressen im Fall von Phishing.
- ***Schadensinformationen***: Potentieller bzw. eingetroffener Schaden an den Komponenten; Schätzung der ökonomischen und technischen Auswirkungen auf das Unternehmen; Informationen, welche kritischen Infrastrukturen von dem System abhängen.

Zur Codierung wird auf den STIX[37]-Standard zurückgegriffen, der grundsätzlich dafür ausgelegt ist, Informationen so zu kodieren, dass sie interoperabel sind. Dadurch lässt sich die Kommunikation zwischen verschiedenen Parteien, kritischen Infrastrukturen und CSIRTs relativ einfach bewerkstelligen.

Während die meisten Informationen nicht generell heikel in Hinblick auf die DSGVO sind, ist dies bei den IP-Adressen und E-Mail-Adressen anders. Hier ist es möglich, bei den IPs, zumindest in Zusammenspiel mit dem Zeitintervall, Nutzer eindeutig zu identifizieren, weshalb es sich wohl um personenbezogene Daten handelt, auch wenn für die Identifizierung einer Person im Fall von dynamischen IP-Adressen zusätzlich noch die Hilfe des Providers benötigt wird.

Das Prinzip von Ma^{3}tch kann natürlich auch für IP-Adressen und E-Mail-Adressen angewandt werden, indem die Hashes ausgetauscht werden. Auch hierbei kann zuerst auf eine reduzierte Form zurückgegriffen werden, die erst bei Übereinstimmung vollständig verglichen wird.

Zusätzlich sieht unser Systemvorschlag vor, dass Aggregate, bspw. zur Veröffentlichung, zur Verfügung stehen. Das Hauptproblem hinter Aggregaten ist das Problem dynamischer Datenbereiche, d.h. stehen zwei Versionen X_0 und X_1 zu zwei unterschiedlichen Zeitpunkten t_0 und t_1 zur Verfügung, so muss darauf geachtet werden, dass nicht bspw. durch Differenzbildung Personen identifiziert werden können.

6. Datenschutzfreundliche Kodierung von Identifikatoren

Grundsätzlich wird jeder Identifikator für sich alleine kodiert, um eine bessere Abdeckung und Erkennung von Gemeinsamkeit zu erhalten. Dabei muss bei zusammengesetzten Identifikatoren darauf geachtet werden, dass die Teile getrennt kodiert werden, da sonst der Match extrem erschwert wird (bspw. «Name» bestehend aus «Vorname(n)» und «Nachname(n)» →Bei Verwendung einer kryptograpischen Hashfunktion H lässt H(«Vorname»||«Nachname») keine Rückschlüsse auf («Nachname»||«Vorname») zu («||» beschreibt in diesem Zusammenhang die Verknüpfung von Texten).

Der grundsätzliche Ansatz besteht darin, dass nicht die Daten ausgetauscht, bzw. in einem gemeinsamen Datenpool (je nach Sichtweise) gespeichert werden, sondern wie im Fall von Ma^{3}tch lediglich verschlüsselte Versionen. Dabei können sowohl (sichere) kryptographische Hashfunktionen als auch ein gemeinsamer public key eingesetzt werden. Der zugehörige private key wird hingegen zur de-Anonymisierung eingesetzt.

Wichtig ist auch die Festlegung von Gültigkeitsbereichen für manche Aspekte: Während sich Namen nur selten ändern, ist dies im Fall dynamischer IP-Adressen anders. Diese sind nur in einem bestimmten Zeitraum einer bestimmten Person zugeordnet, außerhalb dieses Zeitraums daher anderen Personen, die somit bei reinem

[37] Der Standard ist verfügbar unter https://stixproject.github.io/.

Austausch der IP-Adresse zu Unrecht verdächtigt werden würden. Um diesem Aspekt vorzubeugen, muss ein Zeitintervall mitgegeben werden, das die Gültigkeitsdauer eingrenzt. Dieses wird nicht verschlüsselt, da ein Abgleich sonst nicht (oder unter dem Einsatz homomorpher Verfahren nur sehr langsam) möglich ist.

Erzeugen zwei Nutzer den gleichen Hashwert, so haben sie ein gemeinsames Merkmal angetroffen. Allerdings kann dies auch Probleme aufwerfen: So könnte einer der Beteiligten versuchen, alle gültigen Werte der Urbildmenge (bspw. Einwohner) zu hashen und damit herauszufinden, ob ein Einwohner in einem Fall beteiligt war, ohne selbst einen derartigen Vorfall gehabt zu haben. Dazu sind zwei (alternative) Möglichkeiten vorgesehen, um dies zu unterbinden:

- Organisatorisch: Die Partner tracken mit, ob andere Partenr eine unüblich große Zahl an systematischen Abfragen durchführen.
- Technisch: Anstatt dem Hash der ganzen Information, wird nur ein Teil gehasht zur Verfügung gestellt. Der weitere Austausch erfolgt mittels eines Nonce-basierten Challenge & Response-Verfahrens, d.h. der Anfragende muss beweisen, dass er n Stellen der Information kennt. Ein wesentlicher Aspekt ist auch noch das Thema der Nachvollziehbarkeit, das technisch so gestaltet werden muss, dass auch im Fall eines Zugriffs auf die Audit&Control-Informationen aller Partner keine Information errechnet werden kann.

7. Schlussfolgerungen

CSIRTs müssen potentiell personenbezogene Daten über Sicherheitsvorfälle austauschen. Ohne eine Privacy By Design-Lösung könnte das Datenschutzrecht, der Schutz von Wirtschaftsgeheimnissen bzw. das Strafrecht verletzt werden. Es wird eine Informationsplattform der CSIRTs vorgeschlagen, wo in kodierter Form Sicherheitsvorfälle berichtet werden. In diesem geschlossenen Benutzerkreis können CSIRTs anonymisierte bzw. pseudoanonymsierte Daten problemlos austauschen, die für die Kenntnis der Sicherheitslage und Bedrohungsszenarien wesentlich sind, aber den Datenschutz und den Schutz von Wirtschaftsgeheimnissen nicht verletzen. Die Kenntnis der gleichen personenbezogenen Daten führt zu einem «Hit» in der Plattform und bedeutet letztlich eine gewollte Kooperation der Betroffenen in der Bekämpfung des Cyberangriffs. Damit wird ein wesentlicher Beitrag zur Herstellung der Cybersicherheit geliefert.