Kurt Einzinger, Florian Skopik

Über die datenschutzrechtliche Problematik in CERTs/ CSIRTs-Netzwerken

Die NIS-Richtlinie verlangt die Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk) und verpflichtet die Mitgliedstaaten, zentrale Anlaufstellen und CSIRTs zu errichten. Doch weder in der NIS-Richtlinie noch in der DSGVO oder der Datenschutz-Richtlinie für die Strafverfolgung und Justiz sind ausdrückliche gesetzliche Ermächtigungen für die Verarbeitung und Übermittlung von personenbezogenen Daten zwischen Unternehmen und CSIRTs und innerhalb des CSIRTs-Netzwerks enthalten.

1 Einleitung

Advanced Persistent Threats und State-sponsored Hacks stellen neue Formen der Bedrohung für Organisationen dar, deren Geschäfte maßgeblich über das Internet abgewickelt werden. Aber auch „low profile"-Angriffe, welche sich vorgefertigter Tools und Schadsoftware bedienen, werden immer ausgefeilter – denn auch die Angriffsflächen moderner hochkomplexer IKT Infrastrukturen wachsen von Jahr zu Jahr. Das Kompromittieren von Webseiten, Attackieren von Diensten oder Ausspionieren vertraulicher Firmeninformationen steht bei diesen Angriffen im Mittelpunkt. Die Motivation dazu ist oft vielfältig geprägt und umspannt von der Erlangung wirtschaftlicher Vorteile bis hin zur Schädigung aus politischen oder religiösen Motiven mannigfaltige Facetten. Je wichtiger das Funktionieren digitaler Dienste für unsere Gesellschaft wird, desto eher gelangen diese Dienste auch ins Visier von Wirtschaftskriminellen, Spionen, Terroristen und staatsfeindlichen Gruppierungen. Um diesen Bedrohungen angemessen zu begegnen, haben viele Staaten umfangreiche nationale Cybersicherheitsstrategien erarbeitet und umgesetzt. Waren bis vor kurzem überwiegend privatrechtlich geführte Computer Emergency Response Teams (CERTs bzw. CSIRTs) alleiniges Mittel, um organisationsübergreifend für Sicherheit zu sorgen, haben Staaten nun bereits sehr intensiv damit begonnen, ihre Rolle beim Schutz nationaler kritischer Infrastrukturen und essentieller Dienste vor Cyber-Bedrohungen einzunehmen. Cyber Security Centers und Cyber Defense Centers werden von staatlichen Institutionen zunehmend genutzt, um den anfänglich genannten Bedrohungen angemessen zu begegnen. Eine der Hauptaktivitäten ist dabei die enge Vernetzung aller Beteiligten, v.a. auch bestehender CERTs bzw. CSIRTs, und der rege Informationsaustausch über aktuelle Bedrohungen, sowie der – bis zu einem gewissen Grad verpflichtende – Informationsaustausch über Sicherheitsvorfälle.

Die Europäische Union hat mit der Erlassung der NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) und der daraufhin in den Mitgliedstaaten begonnenen Umsetzung in nationales Recht einen wichtigen Grundstein für die Etablierung der zur Gewährleistung der Cybersicherheit erforderlichen Strukturen geschaffen. Ein wichtiger Meilenstein dabei ist die Einrichtung sog. NIS-Behörden. Gleichzeitig bringt aber dieser wichtige Schritt eine ganze Reihe neuer Herausforderungen mit sich – nicht nur für wenige, sondern für alle Unternehmen, die entweder kritische Infrastrukturen betreiben oder aber digitale Dienste bereitstellen. Naturgemäß gibt es, wie bei allen weitreichenden Veränderungen der Rahmenbedingungen, Unsicherheiten in Bezug auf die Umsetzung der Richtlinie und folglich Realisierung der zuvor genannten NIS-Behörden zum Informationsaustausch. Während ihre Rollen grob in der NIS-Richtlinie umrissen sind, ist noch weitgehend unklar, wie weit die Kompetenzen im Detail gehen sol-

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

len und v.a. wie die Ausgestaltung ihrer Arbeit im Alltag aussehen wird. Die Schnittstellen zwischen Organisationen und staatlichen Einrichtungen, die Art der ausgetauschten Informationen, die dafür erforderlichen Prozesse auf Seiten der Organisationen, aber auch des Staates werden derzeit breit diskutiert.

Durch den regen Austausch sicherheitsrelevanter Informationen zwischen Unternehmen und dem Staat sollen dabei Cyber-Lagebilder auf nationaler Ebene entstehen, um die Erkennung, Analyse und Bewältigung von Cyberangriffen zu unterstützen. Während die Umsetzung dieser Vision im Großen und Ganzen intuitiv erscheint, ist die konkrete Ausgestaltung dieser Vernetzung noch weitgehend offen. In diesem Kontext ist auch die verschärfte Datenschutzproblematik durch Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) zu sehen. Die daraus resultierenden Spannungen aufgrund des für die Gewährleistung der Sicherheit erforderlichen Informationsaustauschs zwischen Organisationen einerseits und des Datenschutzes von potentiell personenbezogenen Daten andererseits sollen im vorliegenden Artikel näher beleuchtet werden.

2 CERTs und CSIRTs

In der Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) wird als eine Maßnahme zur Erreichung dieses Sicherheitsniveaus die Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk — Computer Security Incident Response Teams Network) (Art. 1 lit c NIS-Richtlinie) und die Pflicht für die Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und CSIRTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen, (Art 1 lit e NIS-Richtlinie) definiert.

Jedoch sind weder in der NIS-Richtlinie, noch in der Datenschutz-Grundverordnung (DSGVO) oder der Datenschutz-Richtlinie für die Strafverfolgung und Justiz (Richtlinie 216/680) ausdrückliche gesetzliche Ermächtigungen für die Verarbeitung und Übermittlung von personenbezogenen Daten innerhalb und zwischen CSIRTs, Unternehmen und anderen Stellen enthalten.

Die NIS-Richtlinie macht es sich diesbezüglich überhaupt sehr einfach. In Art. 2 über die Verarbeitung personenbezogener Daten gemäß der NIS-Richtlinie verweist sie lediglich auf die mittlerweile schon „alte" Richtlinie 95/46/EG, die mit Wirkung vom 25. Mai 2018 aufgehoben sein wird, weshalb Verweise auf diese Richtlinie zukünftig als Verweise auf die DSGVO gelten werden (Art. 94 DSVGO). Diesem Verweis nach erfolgt die Verarbeitung personenbezogener Daten nach Maßgabe der Richtlinie 95/46/EG und die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union nach Maßgabe der Verordnung (EG) Nr. 45/2001 (Art. 2 NIS-Richtlinie). Dieser Artikel enthält somit nur Verweise auf Rechtsakte, die selbstverständlich Geltung haben.

Im Erwägungsgrund 34 der NIS-Richtlinie wird bezüglich CERTs/CSIRTs ausgeführt, dass die Mitgliedstaaten über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen sollten. Daher sollten die Mitgliedstaaten gewährleisten, dass sie über gut funktionierende CERTs/CSIRTs verfügen, die die grundlegenden Anforderungen zur Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Vorfällen und Risiken und einer effizienten Zusammenarbeit auf Unionsebene erfüllen.

Damit alle Arten von Betreibern wesentlicher Dienste und von Anbietern digitaler Dienste diese Fähigkeiten und diese Zusammenarbeit nutzen können, sollten die Mitgliedstaaten sicherstellen, dass diese von einem eingerichteten CSIRT abgedeckt sind. Wegen der Bedeutung der internationalen Zusammenarbeit zur Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch diese Richtlinie geschaffenen CSIRTs-Netzwerk an internationalen Kooperationsnetzen beteiligen können (Erwägungsgrund 34 NIS-Richtlinie).

Ein weiterer Erwägungsgrund der NIS-Richtlinie spricht davon, dass bei Sicherheitsvorfällen der Schutz personenbezogener Daten häufig nicht mehr gewährleistet sei. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um Verletzungen des Schutzes personenbezogener Daten aufgrund von Sicherheitsvorfällen zu begegnen (Erwägungsgrund 63 NIS-Richtlinie). Allerdings wird die Problematik der gesetzeskonformen Verarbeitung und Übermittlung personenbezogener Daten zwischen den betroffenen Unternehmen und Behörden hierbei auch nicht weiter angesprochen.

Lediglich im Erwägungsgrund 72 wird das Erfordernis der Verarbeitung personenbezogener Daten beim Austausch von Informationen über Risiken und Vorfälle in der Kooperationsgruppe und im CSIRTs-Netzwerk und bei der Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRTs erwähnt (Erwägungsgrund 72 NIS-Richtlinie). Diese Verarbeitung sollte dann mit der Richtlinie 95/46/EG und der Verordnung (EG) Nr. 45/2001 vereinbar sein, wie es auch im Art. 2 der Richtlinie bestimmt wird.

Da die Nachrichten und Meldungen über sicherheitsrelevante Vorfälle erfahrungsgemäß immer personenbezogene Daten enthalten können, werden datenschutzrechtliche Ermächtigungen sowohl für die Verarbeitung in den CERTs und CSIRTs als auch für die Übermittlung durch Betreiber kritischer Infrastrukturen (privat oder öffentlich) an CERTs oder CSIRTs sowie für die Übermittlung von CERTs oder CSIRTS zu anderen Stellen als auch untereinander benötigt.

3 Erwägungsgrund 49 der DSGVO

In der Datenschutz-Grundverordnung der EU (DSGVO, Regulation 2016/679) wird erstmals zur Problematik der Verarbeitung personenbezogener Daten im Rahmen von CERTs/CSIRTs-Netzwerken Bezug genommen, allerdings nur in den Erwägungsgründen und nicht mit einer eigenen gesetzlichen Bestimmung.

Erwägungsgrund 49 der DSGVO bestimmt, dass die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (CERTs/CSIRTs), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellt, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit

Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of Service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren (Erwägungsgrund 49 DSGVO).

Damit umfasst sind also Behörden (public authorities), Computer-Notdienste CERTs/CSIRTs, Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie Anbieter von Sicherheitstechnologien. Betreiber von anderen kritischen Infrastrukturen wie z.B. Energieversorger können dieses Privileg nicht in Anspruch nehmen, obwohl gerade die NIS-Richtlinie auch auf solche abzielt.

Der Erwägungsgrund 49 der DSGVO stellt keine explizite Ermächtigung aus, sondern verweist auf ein berechtigtes Interesse des Verantwortlichen der Datenverarbeitung, welches in Verbindung mit dem Art. 6 Abs. 1 lit f die Verarbeitung und Übermittlung von personenbezogenen Daten in diesen Fällen als rechtmäßig anerkennt. Demnach ist eine Verarbeitung rechtmäßig, wenn die nachstehende Bedingung erfüllt ist:

> *„f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."*

Eine gewisse Widersprüchlichkeit entsteht durch die im Anschluss daran stehende Bestimmung:

„Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung."(Art. 6 Abs. 1 DSGVO).

Die Absicht hinter dieser Bestimmung ist, dass behördliche Tätigkeit gesetzlich normiert sein soll. Dies wird auch im Erwägungsgrund 47 explizit festgehalten.

Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen (Erwägungsgrund 47 DSGVO).

Die Widersprüchlichkeit ergibt sich daraus, dass im Erwägungsgrund 49 der DSGVO Behörden (public authorities) ausdrücklich angeführt sind, die ein berechtigtes Interesse des Verantwortlichen in Anspruch nehmen können, wenn dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist (siehe oben). Dem widerspricht dann der Unterabsatz 1 in Art. 6 Abs. 1 der Datenschutz-Grundverordnung wo Behörden (public authorities) explizit von dem berechtigten Interesse ausgenommen werden.

Der EuGH vertritt in ständiger Rechtsprechung die Ansicht, dass die Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht.[1]

In den Rechtsakten der Europäischen Union haben Erwägungsgründe zwar einen stärkeren Rechtscharakter als etwa die „Erläuternden Bemerkungen" zu österreichischen Gesetzen, da Art. 296 des Vertrags über die Arbeitsweise der Europäischen Union besagt, dass Rechtsakte mit einer Begründung zu versehen sind, wodurch die Erwägungsgründe Teil einer Verordnung sind und sehr wichtig für deren Interpretation. Falls allerdings Widersprüche zwischen Erwägungsgrund und Artikel entstehen, so hat der Artikeltext unmittelbar Vorrang.[2]

Wenn also ein CERT oder ein CSIRT oder eine darauf aufbauende Stelle zur Cyber-Lagebilderstellung im öffentlichen Bereich innerhalb einer Behörde angesiedelt ist und der Erfüllung der behördlichen Aufgaben dient, so muss der Gesetzgeber für die dafür notwendigen Datenverarbeitungen von personenbezogenen Daten auch die gesetzlichen Ermächtigungen schaffen.

4 Teilnahme von Betreibern kritischer Infrastrukturen

Wie schon erwähnt können Betreiber kritischer Infrastrukturen, die keine elektronischen Kommunikationsnetze oder -dienste betreiben, auf Basis des Erwägungsgrundes 49 kein berechtigtes Interesse des Verantwortlichen in Anspruch nehmen. Damit sie Meldungen von Sicherheitsvorfällen, welche personenbezogene Daten enthalten können, gesetzeskonform an CERTs oder CSIRTs übermitteln dürfen, stehen dem Anschein nach drei Möglichkeiten zur Verfügung.

Erstens eine spezifische gesetzliche Regelung in den nationalen Anpassungsgesetzen. Art. 6 Abs. 2 DSGVO sieht vor, dass die Mitgliedstaaten „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Abs. 1 lit c und e beibehalten oder einführen [können], indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen". Dies ermöglicht den Mitgliedstaaten somit trotz Vorliegens einer Unionsverordnung, die in den Grenzen des Anwendungsbereichs des Unionsrechts grundsätzlich auf den öffentlichen und privaten Bereich gleichermaßen anwendbar ist, auf nationaler Ebene bestimmte „spezifischere Bestimmungen" zu erlassen. Obwohl diese Klausel zunächst nur auf den öffentlichen Sektor gerichtet war, wird sie auch auf den privaten Sektor zu erstrecken sein. In Fällen, in denen den Mitgliedstaaten etwa aus Art. 8 EMRK und der darauf basierenden EGMR-Judikatur aktive Schutzpflichten für den Betroffenen als Grundrechtsträger erwachsen, wird dies sogar geboten sein. Auch aus dem Erwägungsgrund 45 kann abgeleitet werden, dass die Mitgliedstaaten befugt sind, auch spezifischere Vorschriften zum Schutz Privater beizubehalten oder zu erlassen, da unter den dort genannten Voraussetzungen auch Regelungen zu natürlichen Personen (als Verantwortlichen) getroffen werden können. Somit könnten von den Mitgliedstaaten in ihren jeweiligen gesetzlichen Anpassungen an die DSGVO die

1 EuGH, Urt. vom 19.6.2014, Rs. C-345/13, ECLI:EU:C:2014:2013 – Karen Millen Fashions, Rn. 31, s. auch: EuGH, Urt. vom 24.11.2005, Rs. C-136/04, ECLI:EU:C:2005:716 – Deutsches Milchkontor, Rn. 32; EuGH, Urt. Vom 19.11.1998, ECLI:EU:C:1998:554 – Nilsson u.a., Rn. 54.

2 Pollirer/Weiss/Knyrim/Haidinger, DSGVO Datenschutz-Grundverordnung (2017) S. III-IV.

Verarbeitung und Übermittlung von personenbezogenen Daten von Betreibern kritischer Infrastrukturen an CERTs oder CSIRTs durch eine „spezifischere Bestimmungen" als berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit f definiert werden.

Zweitens die Einholung der Einwilligung der betroffenen Personen bei den Datenverarbeitungen von Betreibern kritischer Infrastrukturen für die Übermittlung von personenbezogenen Daten an CERTs oder CSIRTs im Falle von Sicherheitsverletzungen. Dies könnte bei Vertragsabschluss oder im Zuge der Einwilligung für andere Zwecke der Datenverarbeitung geschehen.

Drittens eine weite Auslegung des letzten Satzes des Erwägungsgrundes 47 der DSGVO, der folgendermaßen lautet:

Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar.

Der Begriff „Betrug" könnte in diesem Zusammenhang durchaus weit ausgelegt werden und alle Sicherheitsvorfälle bei kritischen Infrastrukturen, die von einer Person verursacht sein könnten, umfassen. So ist zum Beispiel im Übereinkommen über Computerkriminalität[3] in Art. 8 von „Computerbezogene[m] Betrug" die Rede, worunter folgende Handlungen, wenn vorsätzlich und unbefugt begangen, verstanden werden: die Beschädigung des Vermögens eines anderen durch Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten; sowie das Eingreifen in den Betrieb eines Computersystems in betrügerischer oder unredlicher Absicht. Damit wäre auch ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit f gegeben und die Verarbeitung und Übermittlung von Meldungen an CERTs oder CSIRTs gerechtfertigt.

5 CSIRTs bei Sicherheitsbehörden

Die Einrichtung von CERTs oder CSIRTs innerhalb von Sicherheitsbehörden hat andere rechtliche Voraussetzungen. Hierbei kommt aus Datenschutzsicht die Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates zum Tragen. Sie regelt den Datenschutz von Datenverarbeitungen von zuständigen Behörden. Diese zuständigen Behörden können nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden einschließen, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke dieser Richtlinie übertragen wurde (Erwägungsgrund 11 Richtlinie 2016/680).

3 Übereinkommen über Computerkriminalität, BGBl. III Nr. 140/2012.

Der Zweck der Datenverarbeitungen, die durch diese Richtlinie geregelt werden, beinhaltet sowohl die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung als auch den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit (Art. 1 Abs. 1 Richtlinie 2016/680). Wenn solche Stellen oder Einrichtungen jedoch personenbezogene Daten zu anderen Zwecken als jenen dieser Richtlinie verarbeiten, gilt die DSGVO.

Zum Beispiel obliegt den österreichischen Sicherheitsbehörden laut Sicherheitspolizeigesetz (§ 22 Abs. 1 Z 6 SPG) der besondere Schutz von Einrichtungen, Anlagen, Systemen oder Teilen davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben (kritische Infrastrukturen). Eine Einrichtung von CERTs oder CSIRTs innerhalb der österreichischen Sicherheitsbehörden unterliegt somit eindeutig der Richtlinie 2016/680 und nicht der DSGVO, da sowohl die Sicherheitsbehörden als zuständige Behörden als auch die Zwecke dieser Datenverarbeitung in den Anwendungsbereich der Richtlinie fallen.

Um die Rechtmäßigkeit einer solchen Datenverarbeitung zu gewährleisten, muss eine gesetzliche Regelung vorliegen. Im Art. 8 der Richtlinie wird bestimmt, dass die Mitgliedstaaten vorzusehen haben, dass die Verarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Art. 1 Abs. 1 genannten Zwecken wahrgenommenen wird, und auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt (Art. 8 Abs. 1Richtlinie 2016/680).

Zusätzlich sollen im Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs der Richtlinie regelt, zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben werden (Art. 8 Abs. 2 Richtlinie 2016/680).

Eine Bestimmung, die eine Rechtmäßigkeit der Datenverarbeitung durch ein berechtigtes Interesse des Verantwortlichen konstituiert, analog zur DSGVO, ist hier nicht vorgesehen. Um die Rechtmäßigkeit von Datenverarbeitungen von CERTs oder CSIRTs innerhalb der Sicherheitsbehörden sicherzustellen, ist damit auf jeden Fall eine dementsprechende gesetzliche Regelung notwendig.

Dies könnte analog auch für den Betrieb von CERTs oder CSIRTs innerhalb der militärischen Landesverteidigung gelten (in Österreich im Bundesministerium für Landesverteidigung und Sport (BMLVS)).

Zusammenfassung

Die Kenntnis eines aktuellen und umfassenden Lagebildes im Bereich der kritischen Infrastrukturen und deren Informations- und Kommunikationsdiensten und -netzen ist für die gesamtstaatliche Sicherheit von großer Bedeutung. Dabei sind CERTs/CSIRTs als Sammel- und Verteilpunkt von sicherheitsrelevanten Meldungen und Informationen notwendiger Bestandteil.

Die NIS-Richtlinie 2016/1148 sieht die Schaffung eines Netzwerks von Computer-Notfallteams (CERTs/CSIRTs) und die Pflicht der Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und CSIRTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen, vor. In den hierbei verwendeten Datenverarbeitungen und -übermittlungen können personenbezogene Daten enthalten sein.

Nur die neue Datenschutz-Grundverordnung (DSGVO) nimmt im Erwägungsgrund 49 Bezug auf die Verarbeitung und Übermittlung von personenbezogenen Daten innerhalb und zwischen CERTs/CSIRTs, Betreibern von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien.

Für Betreiber anderer kritischer Infrastrukturen und Behörden sind noch eigene gesetzliche Bestimmungen notwendig, damit sie datenschutzkonform an CERTs/CSIRTs-Netzwerken teilhaben können.

Danksagung

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

Literatur

[1] Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie)

[2] 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 – DSGVO)

[3] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

[4] Hans-Jürgen Pollirer; Ernst M. Weiss; Rainer Knyrim; Viktoria Haidinger: DSGVO – Datenschutz-Grundverordnung, MANZ Verlag Wien 2017

[5] Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), Fassung vom 24.04.2017