DIE NIS-RICHTLINIE UND DER RECHTLICHE RAHMEN VON CERTS

Christof Tschohl / Walter Hötzendorfer / Gerald Quirchmayr / Edith Huber / Otto Hellwig

Wissenschaftlicher Leiter, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
christof.tschohl@researchinstitute.at; http://www.researchinstitute.at

Senior Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
walter.hoetzendorfer@researchinstitute.at; http://www.researchinstitute.at

Universitätsprofessor, Universität Wien, Fakultät für Informatik
Währinger Straße 29, 1090 Wien, AT
Gerald.Quirchmayr@univie.ac.at

Senior Researcher, Donau Universität Krems
Dr. Karl Dorrek Str. 30, 3500 Krems an der Donau, AT
edith.huber@donau-uni.ac.at; http://www.donau-uni.ac.at

Senior Researcher, SBA-Research
Favoritenstraße 16, 1040 Wien, AT
ohellwig@sba-research.org; http://www.sba-research.org

Schlagworte: ***CERT, CSIRT, NIS-Richtlinie, Cybersicherheit, IT-Sicherheit***

Abstract: *CERTs entstanden als Einrichtungen der Praxis und somit existierte zunächst kein rechtlicher Rahmen für CERTs bzw. war und ist dieser in vielerlei Hinsicht unbestimmt. Mit der NIS-Richtlinie und dem geplanten Cybersicherheitsgesetz in Österreich wird der Rechtsrahmen für CERTs nun konkretisiert. Basierend auf Ergebnissen der KIRAS-Projekte CERT-Kommunikationsmodell und CERT-Kommunikationsmodell II beschreibt der Beitrag die aktuellen rechtlichen und faktischen Rahmenbedingungen für CERTs, geht auf die neuen Vorgaben der NIS-Richtlinie ein und zeigt Bedarf auf, gesetzliche Bestimmungen für CERTs zu schaffen.*

1. Einleitung

Mit dem Ansteigen der allgemeinen Bedrohung durch Angriffe auf IKT-Systeme und kritische Infrastrukturen wächst auch die Bedeutung von CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams).[1] Diese können als nationale CERTs für ein ganzes Land, für eine Branche, für bestimmte kritische Infrastrukturen oder für ein einzelnes Unternehmen zuständig sein. CERTs entstanden als Einrichtungen der Praxis zur Unterstützung bei IT-Sicherheitsvorfällen und somit existierte zunächst kein rechtlicher Rahmen für CERTs bzw. war und ist dieser in vielerlei Hinsicht unbestimmt.

[1] Die Begriffe CERT und CSIRT werden nachfolgend synonym verwendet. CERT ist eine eingetragene Marke der Carnegie Mellon University, siehe dazu http://www.cert.org/incident-management/csirt-development/cert-authorized.cfm? (alle Internetadressen abgerufen am 25. Januar 2017). In Übereinstimmung mit den Empfehlungen der Carnegie Mellon University, wonach CSIRT der generische Begriff ist, verwendet auch die NIS-Richtlinie den Begriff CSIRT. Ein CSIRT kann bei der Carnegie Mellon University beantragen, den Begriff CERT im Namen führen zu dürfen, wenn es deren diesbezügliche Guidelines einhält, und wird dann in eine entsprechende öffentliche Liste aufgenommen.

Am 8. August 2016 trat die Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL)[2] in Kraft. In Österreich wird derzeit an einem Gesetz zu deren Umsetzung gearbeitet, im Folgenden vorläufig als Cybersicherheitsgesetz bezeichnet. Gemäß Art. 25 Abs. 1 NIS-RL sind diese nationalen Umsetzungsrechtsakte bis 9. Mai 2018 zu erlassen und ab 10. Mai 2018 anzuwenden. Die NIS-Richtlinie verpflichtet die Mitgliedstaaten zur Einrichtung von CSIRTs und sieht bestimmte Vorgaben und Aufgaben für diese vor. Damit nimmt der Rechtsrahmen für CERTs konkretere Formen an.

Im Rahmen des Forschungsprojektes CERT-Kommunikationsmodell (CERT-Komm) wurden Mitarbeiterinnen und Mitarbeiter aller österreichischen CERT-Betreiber (n=20) über die Herausforderungen der rechtlichen und internationalen Entwicklungen qualitativ und quantitativ befragt. Basierend auf Ergebnissen des Forschungsprojekts CERT-Komm und des noch laufenden Nachfolgeprojekts CERT-Komm II beschreibt dieser Beitrag die aktuellen rechtlichen und faktischen Rahmenbedingungen für CERTs, geht auf die neuen Vorgaben der NIS-Richtlinie ein und zeigt auf, inwieweit darüber hinaus Bedarf besteht, gesetzliche Bestimmungen für CERTs – insbesondere im geplanten Cybersicherheitsgesetz – zu schaffen. Zu denken ist dabei insb. an den Umgang mit erlangtem Wissen über Straftaten, sowie Befugnisse betreffend die Verarbeitung und den Austausch personenbezogener Daten etc.[3]

Die Projekte CERT-Komm und CERT-Komm II wurden bzw. werden finanziert im Sicherheitsforschungs-Förderprogramm KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie.

2. CERTs – Geschichte und Grundlagen

Die Entwicklung von CERTs nahm ihren Anfang im Jahr 1988 mit dem Auftreten des Morris-Wurms im akademischen Netzwerk der USA. Damals wurde das CERT/CC[4] geschaffen, dessen Konzept nach wie vor relevant für den Aufbau von CERTs ist. Der Grundgedanke für die Gründung des CERT/CC war, an zentraler Stelle die spezifischen technischen Ressourcen für die Behandlung von IT-Sicherheitsvorfällen zu bündeln, um im Anlassfall rasch reagieren zu können. Die Ankündigung der DARPA über die Gründung von CERT/CC[5] betont, dass dieses Team nicht nur technische Unterstützung bei der Behebung von Zwischenfällen geben, sondern auch die Kommunikation mit den technischen Experten herstellen wird. Im Jahr 1992 wurde mit dem holländischen SURFnet-CERT das erste Europäische CERT gegründet. In dieser Anfangsphase wurden CERTs hauptsächlich im akademischen Bereich, der zu diesem Zeitpunkt die intensivste Internet-Nutzung aufwies, als Teams für die Bekämpfung von Zwischenfällen aufgebaut.

Wichtige weitere Schritte für die Entwicklung der weltweiten CERT-Community waren die Schaffung der Organisation FIRST (Forum of Incident Response and Security Teams[6], derzeit 366 Mitglieder in 78 Ländern[7]) als vertrauensbildende Kommunikationsplattform für CERTs im Jahr 1990 sowie die Einführung einer standardisierten Beschreibungsmethode für die Leistungen und Zuständigkeiten von CERTs in Form des RFC 2350[8] im Jahr 1998. Mittlerweile besitzen eine Vielzahl an Firmen und staatlichen Organisationen «Incident Response Teams», die sehr unterschiedliche Zuständigkeitsbereiche («constituency» lt. RFC 2350) aufweisen. Alle diese Teams haben als Gemeinsamkeit die wesentliche Aufgabe der Behandlung von Cyber-Zwischenfällen,

---

2 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.

3 Vgl. Huber, Sicherheit in Cyber-Netzwerken – Computer Emergency Response Teams und ihre Kommunikation, Springer, Wiesbaden 2015.

4 https://cert.org/about.

5 Carnegie Mellon University, Pressemitteilung vom 13. Dezember 1988, https://www-uxsup.csx.cam.ac.uk/pub/doc/cert/CERT_Press_Release_8812.

6 https://www.first.org.

7 https://www.first.org/members/map.

8 Brownlee/Guttman, Expectations for Computer Security Incident Response, RFC 2350, 1998, https://www.ietf.org/rfc/rfc2350.txt.

die die eigene Zielgruppe betreffen. Bei der dazu nötigen Kommunikation und Zusammenarbeit mit anderen CERTs sowie anderen Playern im Internet spielen auch rechtliche Fragen eine wesentliche Rolle.

Internationale Gremien und Organisationen (G8[9], ITU[10], OECD[11]) weisen seit vielen Jahren darauf hin, dass alle Staaten weltweit zumindest ein nationales CERT aufbauen sollten, damit ein international erreichbarer Kontaktpunkt im Falle von schwerwiegenden IT-Sicherheitsvorfällen existiert. In den letzten Jahren wurden die Zuständigkeiten der nationalen CERTs immer stärker auf die nationalen kritischen Infrastrukturen ausgedehnt bzw. in den USA überhaupt ein für kritische Infrastrukturen zuständiges ICS-CERT[12] geschaffen. Das ist eine Reaktion darauf, dass auch kritische Infrastrukturen immer mehr mit IT-Sicherheits-Zwischenfällen rechnen müssen, nicht zuletzt mit Angriffen durch staatliche Akteure anderer Staaten.[13] Dies hat auch zur Folge, dass Staaten nationale Cybersicherheitsstrategien entwickeln, in die CERTs zunehmend einbezogen werden. Diese Entwicklungen haben zu einer starken Sensibilisierung bei der Kommunikation von CERTs geführt. Wie das Beispiel der nationalen CERTs von Russland und der Ukraine zeigt, reicht eine Mitgliedschaft bei FIRST nicht aus, um im Krisenfall miteinander zu kommunizieren.[14]. Mit der Thematik der Rolle von CERTs bei Konflikten zwischen Staaten befasst sich ein Bericht der UNO[15] aus dem Jahr 2015 sowie die OSZE mit ihrer Entscheidung 1202 aus dem Jahr 2016 über vertrauensbildende Maßnahmen[16].

Bei der Gründung der ersten CERTs gab es noch keinerlei staatliche Vorgaben, ob und wie CERTs zu gestalten sind. Dies hat sich mittlerweile geändert. In den USA sind bundesstaatliche Behörden verpflichtet, Vorkehrungen für die Behandlungen von IT-Sicherheitsvorfällen zu treffen und diese Vorfälle auch dem US-CERT zu melden.[17]In Europa ist die ENISA (European Union Agency for Network and Information Security[18]) mit sehr umfangreichen Programmen und Arbeitsschwerpunkten eine treibende Kraft für den Aufbau und die Zusammenarbeit von CERTs in den Mitgliedstaaten. Sie organisiert auch die Europäischen Cyber-Übungen «Cyber-Europe»[19], bei denen CERTs eine wesentliche Rolle spielen. Es gibt in Europa zwar ein EU-CERT, dieses ist allerdings für die EU-Institutionen zuständig und nicht Koordinator für die nationalen CERTs.

Da das Internet keine Grenzen kennt, müssen bei der Behebung eines IT-Sicherheitsvorfalls CERTs mit anderen CERTs bzw. anderen Playern kommunizieren. Dabei spielen auf persönlichem Vertrauen beruhende Kontakte zwischen einzelnen CERT-Mitarbeitern eine sehr wesentliche Rolle.[20]

---

9 G8, G8 Principles for Protecting Critical Information Infrastructures, 2003, http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf.

10 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.

11 https://www.oecd.org/sti/ieconomy/ciip.htm.

12 https://ics-cert.us-cert.gov.

13 UN Group of Governmental Experts, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, http://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/174.

14 Vgl. Rõigas, The Ukraine Crisis as a Test for Proposed Cyber Norms. In: Geers (Hrsg.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2015, S. 135–145, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf, S. 144.

15 UN Group of Governmental Experts, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/172, http://www.cfr.org/internet-policy/un-group-governmental-experts-developments-field-information-telecommunications-context-international-security/p36949.

16 OSZE, Beschluss Nr. 1202 über vertrauensbildende Maßnahmen der OSZE zur Verminderung der Konfliktrisiken, die sich aus dem Einsatz von Informations- und Kommunikationstechnologien ergeben, 2016, https://www.osce.org/pc/227281.

17 Siehe NIST SP800-61 Rev2, https://www.nist.gov/news-events/news/2012/08/updated-nist-guide-how-dealing-computer-security-incidents, sowie Federal Information Security Management Act of 2002 (FISMA), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

18 https://www.enisa.europa.eu.

19 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

20 Kruidhof, Evolution of National and Corporate CERTs – Trust, the Key Factor: In: Hathaway (Hrsg.), Best Practices in Computer Network Defense: Incident Detection and Response, IOS Press, Amsterdam 2014, S. 81–96.

3. Die Rahmenbedingungen und Herausforderungen von CERTs

Ein Ziel des Forschungsprojekts CERT-Komm war es, zu erheben, was nun die Rahmendbedingungen für einen sicheren Cyberspace sein sollen. Dabei konnten folgende Zielgrößen eindeutig erkannt werden, nämlich die messbare Reduktion von erfolgreichen Cyber-Angriffen und Cyber-Terrorismus-Angriffen, die Reduktion von technischen Bedienungsfehlern und verstärkter Schutz für öffentliche IKT. Um dies zu gewährleisten, ist es für CERTs unverzichtbar, sich mit den involvierten Stakeholdern (Akteuren) austauschen. Aber wer sind diese Akteure, mit denen sich ein CERT auseinandersetzen muss?

3.1. Stakeholder im CERT-Umfeld

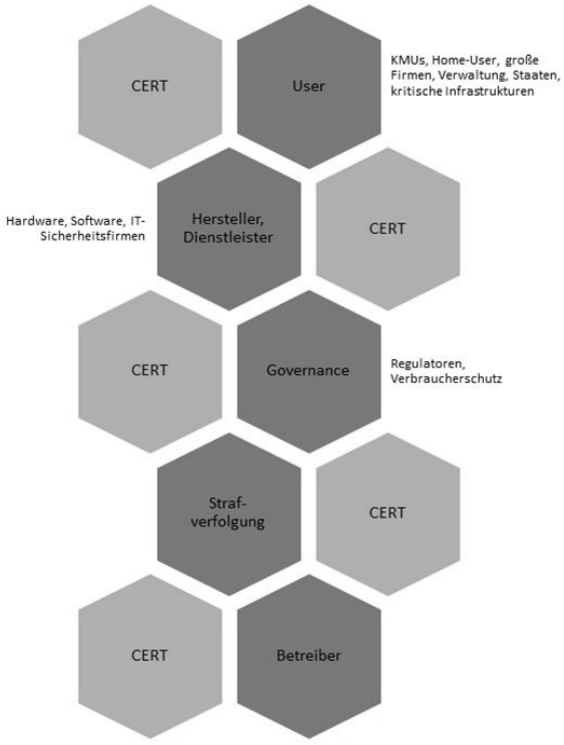

Abbildung 1: Stakeholder im Kontext der Netzwerk- und Informationssicherheit

Wie Abbildung 1 zu entnehmen ist, gibt es eine Vielzahl von Stakeholdern im Kontext der Netzwerk- und Informationssicherheit. Diese Stakeholder haben unterschiedliche Rollen, Ziele und Interessen. Dessen ungeachtet haben CERTs eine klare Rolle, die sich oftmals von den Interessen der anderen Stakeholder unterscheidet. Um die oben genannten Zielgrößen zu erreichen, ist es daher unverzichtbar, zum einen miteinander zu kommunizieren und zum anderen juristisch klare Rahmenbedingungen zu setzen. Eine diesbezügliche Initiative setzte die EU-Kommission in Form der NIS-Richtlinie.[21] Um jedoch die Kommunikation und die Zusammenarbeit unter den verschiedenen CERTs zu stärken, galt es in einem ersten Schritt, jene Faktoren zu erheben, die eine gute Zusammenarbeit ermöglichen.

[21] Vgl. Huber, Sicherheit in Cyber-Netzwerken – Computer Emergency Response Teams und ihre Kommunikation, Springer, Wiesbaden 2015, S. 107 ff.

3.2. Vertrauen als kritischer Faktor

Die Studie hat ergeben, dass die wichtigste Voraussetzung für eine gute Zusammenarbeit das gegenseitige Vertrauen unter den CERTs ist. Dieses Vertrauen wird durch unterschiedliche Variablen beeinflusst, die am Ende dafür verantwortlich sind, ob es zu einer Zusammenarbeit kommt oder nicht. Um die Qualität des Vertrauens zu stärken, müssen allerdings Bedingungen geschaffen werden, die das Vertrauen fördern:

Reputation und Diskretion: Fast alle Befragten gaben an, dass Reputation und Diskretion die wichtigsten Variablen sind, die am Ende entscheiden, ob Kommunikation und Wissensaustausch zustande kommen. Die Angst vor Reputationsverlust mindert die Bereitschaft zum Wissensaustausch. Dies gilt für den möglichen Reputationsverlust sowohl der CERTs selbst als auch der Zielgruppe. Daher ist Diskretion unverzichtbar. Um einen qualifizierten Austausch zu ermöglichen, ist eine Kooperation zwischen CERTs, der Zielgruppe (also den potentiellen Opfern von Angriffen) und der Exekutive notwendig. Eine Pflicht für Akteure, insbesondere CERTs, in diesem Zusammenhang bekannt gewordene Straftaten anzuzeigen (Anzeigepflicht) kann allerdings eine Kooperation der beteiligten Stakeholder verhindern, denn in einem Strafverfahren wird der jeweilige Sicherheitsvorfall offengelegt, und dies widerspricht dem Interesse des Betroffenen an Diskretion. Dieser hat daher einen Anreiz, Informationen nicht an einen Stakeholder weitergeben, der einer Anzeigepflicht unterliegt. Der so gesetzte Fehlanreiz kann langfristig gesehen mehr Schaden anrichten, als eine Anzeigepflicht nutzt.[22]

Integrität und Kompetenz: CERT-Mitarbeiter fordern klar gemeinsame Werte und Normen im Sinne einer Verständlichkeit im Austausch des Wissens. Personen, mit denen Wissen geteilt wird, müssen daher als integer und kompetent eingestuft werden. Rechtlich unklare Situationen führen zu einer starken Vorsicht in der Kommunikation mit anderen Personen. Es bedarf daher einer entsprechenden Harmonisierung der diesbezüglichen gesetzlichen Vorgaben in Europa, um ein gemeinsames Handeln der CERTs zu erleichtern. In diesem Zusammenhang hat die NIS-Richtlinie eine besondere Bedeutung.

Erreichbarkeit und Verlässlichkeit: Weitere wichtige Einflussfaktoren sind die Erreichbarkeit der Kollegen und deren Verlässlichkeit. Attacken, die dem Bereich Cybercrime zuzuordnen sind, erfordern ein schnelles Handeln. Ein wesentlicher Faktor ist daher die Geschwindigkeit, in der der Vertrauensgeber seine Inhalte kommuniziert. Zu lange Reaktionszeiten auf Unterstützungsersuchen verursachen Misstrauen.[23]

Kultureller Hintergrund, Sprachkompetenz und wirtschaftliche Überlegungen der Nationalstaaten: Als Hemmschuh der Kommunikation haben sich in der Vergangenheit mangelnde Sprachkompetenz und der kulturelle Hintergrund erwiesen. Oft verfügen Mitarbeiter insbesondere in ausländischen CERTs nicht über ausreichende Englischkenntnisse, um Cyber-Vorfälle zu diskutieren. Des Weiteren beeinflusst eine gemeinsame historische Vergangenheit das gegenseitige Vertrauen. Die europäische Vergangenheit seit dem EU-Beitritt erweist sich daher als immer noch zu kurz, um über kulturelle Unterschiede hinweg zu sehen. Eine kulturelle Annäherung über die Grenzen hinweg stellt im Zusammenhang mit Cybersicherheit eine besondere Herausforderung dar. Darüber hinaus wird davon ausgegangen, dass wirtschaftliche Interessen der Staaten vorrangig behandelt werden und somit die Vertraulichkeit gegenüber ausländischen CERTs nicht im Vordergrund steht. Dieser Punkt wird in den kommenden Jahren immer brisanter werden. Es stellt sich die Frage, wieviel Sicherheit wert ist. Welche Auswirkungen kann es haben, wenn Gewinnstreben über die Cybersicherheit gestellt wird?

4. CERTs und die NIS-Richtlinie

Kernelemente der NIS-RL sind die Pflicht jedes Mitgliedstaats zur Festlegung einer nationalen NIS-Strategie und zur Benennung von NIS-Behörden und CSIRTs, deren nationale und internationale Kooperation sowie Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste, das sind Dienste bestimmter

[22] Vgl. Huber/Hellwig/Quirchmayr, Wissensaustausch und Vertrauen unter Computer Emergency Response Teams – eine europäische Herausforderung, Datenschutz und Datensicherheit 40/3, 2016, S. 162–166.

[23] Ebenda.

gesellschaftlich bzw. wirtschaftlich bedeutender Wirtschaftssektoren,[24] sowie für Anbieter bestimmter digitaler Dienste[25]. Die Ausdehnung des Anwendungsbereichs auf Anbieter bestimmter digitaler Dienste wird damit begründet, dass zahlreiche Nutzer, darunter auch Betreiber wesentlicher Dienste, von diesen digitalen Diensten zunehmend abhängig sind.[26] Die Sicherheitsanforderungen und Meldepflichten sollen eine Kultur des Risikomanagements fördern und sicherstellen, dass die gravierendsten Sicherheitsvorfälle gemeldet werden.[27]

4.1. Organisatorische Bestimmungen

Anhang I der NIS-Richtlinie enthält die Anforderungen an CSIRTs und ihre Aufgaben. Zu den Anforderungen zählen insbesondere Verfügbarkeit und Betriebskontinuität, was eine ständige Bereitschaft mit einschließt. Die Aufgaben entsprechen den üblichen Kernaufgaben von CERTs, das ist insbesondere das Erkennen von und reagieren auf Sicherheitsvorfälle sowie deren Analyse.

ErwGr. 35 der NIS-RL erwähnt, dass die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung ist, weil die meisten Netz- und Informationssysteme privat betrieben werden und die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste angehalten werden sollten, «sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der Sicherheit von Netz- und Informationssystemen zu bedienen». Darüber hinaus hält ErwGr. 35 fest, dass zur wirksamen Unterstützung des Austauschs von Informationen und bewährten Verfahren unbedingt sichergestellt werden muss, «dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, die an einem solchen Austausch beteiligt sind, keine Benachteiligung aufgrund ihrer Zusammenarbeit erfahren.»

Auf europäischer Ebene wird gemäß Art. 12 NIS-RL ein CSIRTs-Netzwerk eingerichtet, das sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammensetzt. Ihm kommen überwiegend operative Aufgaben zu sowie Aufgaben der Koordination und des Informationsaustauschs betreffend die operative Tätigkeit der einzelnen CSIRTs. Strategische Aufgaben nimmt eine Kooperationsgruppe (Art. 11 NIS-RL) wahr, die sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammensetzt.

4.2. Meldepflichten und freiwillige Meldungen

Ein wichtiger Regelungsgegenstand der NIS-RL ist die Meldung von Sicherheitsvorfällen. Betreiber wesentlicher Dienste müssen Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich der zuständigen Behörde oder dem zuständigen CSIRT melden (Art. 14 Abs. 3 NIS-RL). Ebenso müssen Anbieter digitaler Dienste Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Union erbrachten digitalen Dienstes haben (Art. 16 Abs. 3 NIS-RL). Die Kriterien zur Feststellung, ob ein Sicherheitsvorfall erheblich ist, finden sich in Art. 14 Abs. 4 und Art. 17 Abs. 4 NIS-RL. Entscheidend wird jedoch deren noch ausstehende Konkretisierung durch die Kooperationsgruppe nach Art. 11 NIS-RL (Art. 14 Abs. 7) und durch Durchfüh-

---

[24] Diese Sektoren sind gemäß Anhang II der NIS-RL: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung, Digitale Infrastruktur (IXPs, DNS-Diensteanbieter, TLS-Name-Registries). Betreiber wesentlicher Dienste (vormals Betreiber kritischer Infrastrukturen) sind gemäß Art. 4 Abs. 4 NIS-RL öffentliche oder private Einrichtungen aus diesen Sektoren der Wirtschaft, die einen Dienst bereitstellen, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist, dessen Bereitstellung abhängig von Netz- und Informationssystemen ist, wobei ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken würde (Art. 5 Abs. 2 NIS-RL). Die Mitgliedstaaten haben bis zum 9. November 2018 die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet zu ermitteln (Art. 5 Abs. 1 NIS-RL).

[25] Anbieter digitaler Dienste sind gemäß Art. 4 Abs. 6 NIS-RL juristische Personen, die einen Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst anbieten. Diese Begriffe sind in Anhang III der NIS-RL festgelegt und in Art. 4 Abs. 17 bis 19 NIS-RL definiert.

[26] Vgl. ErwGr. 48 der NIS-RL.

[27] Vgl. ErwGr. 4 der NIS-RL.

rungsrechtsakte (Art. 16 Abs. 8 NIS-RL) sein. Für Anbieter digitaler Dienste besteht eine Ausnahme, wonach die Meldepflicht nur dann gilt, wenn sie Zugang zu den Informationen haben, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten (Art. 16 Abs. 4 letzter Satz NIS-RL).

Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und die keine Anbieter digitaler Dienste sind, können auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen angebotenen Dienste haben (Art. 20 Abs. 1). Ebenso können Betreiber wesentlicher Dienste und Anbieter digitaler Dienste freiwillig Sicherheitsvorfälle melden, die keine Meldepflicht auslösen, weil sie die Erheblichkeitsschwelle nicht überschreiten. Dies ist zwar im Wortlaut der NIS-RL nicht ausdrücklich vorgesehen, ergibt sich aber aus einem Größenschluss und dem Normzweck: Sicherheitsvorfälle bei Betreibern wesentlicher Dienste oder bei Anbietern digitaler Dienste, die noch keine «erheblichen» Auswirkungen auf die Verfügbarkeit dieser Dienste haben, sind für die gesamte Cybersicherheitslage mindestens so bedeutsam wie Vorfälle, die keine wesentlichen Dienste bzw. digitalen Dienste i.S.v. Anhang I und II der NIS-RL betreffen. Außerdem bietet Art. 3 NIS-RL den Mitgliedsstaaten die Möglichkeit, Normen für ein höheres Sicherheitsniveau von Netz- und Informationssystemen zu erlassen. Wenngleich den nationalen Gesetzgeber also aus der NIS-RL keine Pflicht trifft, ein System für freiwillige Meldungen unterhalb der Erheblichkeitsschwelle einzurichten, wäre er dennoch gut beraten, ein solches vorzusehen.

Freiwillige Meldungen sind nach dem in Art. 14 für verpflichtende Meldungen festgelegten Verfahren zu behandeln (Art. 20 Abs. 2 NIS-RL). Somit kann eine freiwillige Meldung auch zu der in Art. 14 Abs. 6 NIS-RL vorgesehenen Unterrichtung der Öffentlichkeit über den Sicherheitsvorfall führen, wenn dies für die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist. Dem hat zwingend eine Anhörung des Meldenden vorauszugehen.

Art. 20 Abs. 2 normiert, dass eine freiwillige Meldung nicht dazu führen darf, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte. Anzumerken ist allerdings, dass freiwillige Meldungen von Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste faktisch Pflichten für den Meldenden auslösen können, die zwar ohne die Meldung auch bestanden hätten, von denen die meldende Einrichtung aber keine Kenntnis hatte und/oder deren Nichteinhaltung ohne die Meldung nicht feststellbar gewesen wäre. Das ist vor allem dann der Fall, wenn ein minderschwerer Vorfall isoliert betrachtet die Erheblichkeitsschwelle nicht erreicht, jedoch in einer Gesamtbetrachtung mit anderen Vorfällen – über die im Einzelfall meldende Einrichtung hinaus – erkennbar ist, dass der einzelne, zunächst unerheblich wirkende Vorfall als Teil einer größeren Sicherheitsbedrohung zu sehen ist. Umgekehrt kann es aber ebenso sein, dass ein minderschwerer Vorfall durch die betroffene Einrichtung vorsichtshalber potenziell als Teil einer erheblichen Bedrohung eingeschätzt werden könnte und sich erst in der Organisationsübergreifenden Gesamtbetrachtung zeigt, dass der Vorfall tatsächlich unerheblich ist.

Für eine wirksame Netzwerk- und Informationssicherheit ist es bedeutsam, dass trotz dieser Umstände, die als Hemmnis für freiwillige Meldungen wirken können, künftig solche Meldungen in der Praxis erfolgen. Um aktuelle Bedrohungen adäquat einschätzen zu können, sind CERTs auf freiwillige Meldungen angewiesen, da – wie soeben erwähnt – eine richtige Einschätzung häufig erst in Zusammenschau mehrerer Einzelereignisse möglich ist und nicht zu erwarten ist, dass in der Praxis häufig Sicherheitsvorfälle auftreten, die eine Pflichtmeldung auslösen. Angesichts der Schwierigkeit einer richtigen Einschätzung der Bedrohungslage ist es für die Vertrauensbildung aus der Sicht betroffener Organisationen enorm wichtig, dass im Bereich der freiwilligen Meldungen zunächst eine Austausch auf einer rein fachlichen (technischen) Ebene stattfinden kann, bevor die zuständigen Behörden informiert werden, die im Rahmen ihrer amtswegigen Handlungspflichten möglicherweise aus reiner Vorsicht unabhängig von einer konkreten technischen Einschätzung Ermittlungsmaßnahmen einleiten, welche innerhalb der betroffenen Organisationen als unangenehmer Eingriff in die Vertrauenssphäre empfunden werden könnten (siehe zum Vertrauensproblem schon oben Kapitel 3.2). In der österreichischen Umsetzung, soweit diese bisher einschätzbar ist, wird daher vorgesehen sein, dass alle Meldungen bei einem

CERT zu erstatten sind und nicht direkt bei einer der NIS-Behörden. Damit soll gewissermaßen eine Art «Puffer» entstehen, die eine möglichst richtige Einschätzung der Bedrohungslage zunächst auf einer rein fachlichen bzw. technischen Ebene hält, bevor ggf. entsprechende Verfahren eingeleitet werden.

5. Regelungsbedarf im Cybersicherheitsgesetz

Der wesentliche Zweck des geplanten Cybersicherheitsgesetzes ist die Umsetzung der NIS-RL in Österreich. Zugleich soll es jedoch auch weitere Zwecke erfüllen. Insbesondere soll es einen Rechtsrahmen für die in Österreich bereits bestehenden CERTs und deren Aktivitäten schaffen. Hervorzuheben ist die dringende Notwendigkeit, eine Rechtsgrundlage für den Austausch personenbezogener Daten zwischen CERTs zu schaffen, der auch derzeit bereits stattfindet oder im Sinne der Aufgabenerfüllung der CERTs stattfinden sollte.

Über die datenschutzrechtliche Notwendigkeit einer klaren Rechtsgrundlage hinaus sollte vor allem Rechtssicherheit geschaffen werden, welche konkreten Maßnahmen CERTs im Rahmen ihrer Aufgabenerfüllung setzen dürfen. Beispielsweise ist nach der aktuellen Rechtslage fraglich, ob ein CERT (z.B. CERT.at) ein IT-System einer fremden Organisation sog. Penetration-Tests unterziehen darf, wenn dafür bei reiner Sachverhaltsbetrachtung ein Angriff auf das IT-System durchzuführen ist, der ohne entsprechende Rechtfertigung als rechtswidrige Cyberattacke zu bewerten wäre.

Zugleich bedarf es gesetzlicher Maßnahmen, die sicherstellen, dass diese und andere Befugnisse von CERTs sich im Rahmen der grundrechtlichen Schranken bewegen und nicht überschritten werden. In diesem Zusammenhang sollte das Gesetz Klarheit darüber schaffen, was von CERTs erwartet wird, also welche Aufgaben und Rollen diese zu erfüllen haben. Da die faktische Macht der CERTs nicht zu unterschätzen ist, sollte – ähnlich wie für die Polizei nach dem Sicherheitspolizeigesetz (SPG) – eine strenge Akzessorietät zwischen Aufgaben und Befugnissen normiert werden. Auch die Rechtsnatur der CERTs und deren Entscheidungen, also ob und wann diese in Vollziehung der Gesetze handeln und allenfalls sogar Hoheitsgewalt ausüben, ist für allfällige Fragen des Rechtsschutzes in der Praxis wesentlich.

Eine klare rechtliche Grundlage ist nicht nur eine rechtliche Notwendigkeit für den Austausch bestimmter Daten, sondern trägt auch zur Rechtssicherheit bei. Je einfacher und schneller die Frage beantwortet werden kann, ob eine bestimmte Datenübermittlung zulässig ist, desto rascher kann die Datenübermittlung erfolgen und desto mehr Datenaustausch zum Zwecke der Aufrechterhaltung der Netzwerk- und Informationssicherheit wird insgesamt stattfinden.

6. Schlussfolgerungen

Eine wirksame Prävention und Bekämpfung von Bedrohungen der Cybersicherheit insbesondere im Zusammenhang mit kritischen Infrastrukturen bedarf einer intensiven Kooperation auf nationaler und internationaler Ebene sowohl in fachlicher Hinsicht als auch in Bezug auf Reaktionen der zuständigen staatlichen Behörden. Diese Kooperation erfordert einen weitgehenden Austausch von Informationen, der betroffene Einrichtungen oft an die Grenzen des Vertrauens bringt. Ein System des Informationsaustausches hat zu berücksichtigen, dass die Probleme der Cybersicherheit nicht ausschließlich polizeilichen oder militärischen Charakter haben sondern eine zivile bzw. wirtschaftliche Dimension bergen, die unter Umständen mit einer reinen Betrachtung nach Aspekten der nationalen Sicherheit nicht immer leicht vereinbar sind. Ein nationaler Rechtsrahmen zur Cybersicherheit sollte daher nicht nur die erforderliche Rechtssicherheit, sondern auch mit vertrauensbildenden Konzepten ein System schaffen, das möglichst große Anreize auch für eine freiwillige umfassende Kooperation bietet. Klare gesetzliche Bestimmungen sollten dabei nicht nur zur Vereinfachung und damit zur Beschleunigung der Reaktion auf konkrete Sicherheitsvorfälle führen sondern auch berücksichtigen, dass CERTs in der zu erwartenden künftigen Entwicklung an Bedeutung massiv gewinnen werden und daher eine faktische Macht erhalten, die es nach rechtsstaatlichen Kriterien auch zu begrenzen gilt. Die Ausgewogenheit des Konzepts zur Kooperation und zum Informationsaustausch wird maßgeblich über den Erfolg mitentscheiden.