RECHTSFOLGEN DER EVOLUTION VON SCADA HIN ZUM IOT

Thomas Hrdinka

Ziviltechniker, ZTH Consulting Engineering, Dissertant, Universität Wien, Arbeitsgruppe Rechtsinformatik
Ocwirkgasse 22, 1210 Wien, AT
thrdinka@zth.at; http://www.zth.at

Schlagworte: ***NIS-RL, NISG, Cybersecurity, Privacy, Hacking, Haftung, Risiko, Stand der Technik***

Abstract: *Das IoT ist eine Weiterentwicklung der üblicherweise isolierten SCADA Systeme hin zu flexiblen und millionenfach vernetzten Komponenten, deren potenzielle Einsatzgebiete jene der NIS-RL weitaus übertreffen. Betreiber «Wesentlicher Dienste» haben geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen, wo hingegen bei IoT nicht nur diese sondern auch Haushalte, öffentlicher Dienst, KMUs, uvm. betroffen wären. Es stellt sich hier zusätzlich die Frage der Privacy, wobei gem. DSGVO ebenfalls der Stand der Technik für die Gewährleistung der Sicherheit einzuhalten ist.*

1. Ausgangssituation

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-RL[1]) ist seit mehr als zwei Jahren in Kraft, wobei die Umsetzungsfrist für die MS bis 9. Mai 2018 lief. Sie reguliert die grundlegenden Erfordernisse der europäischen Netzwerksicherheit, wobei die Meldepflicht von Cyberangriffen auf «wesentliche Dienste»[2] eine besondere Stellung einnimmt. Erst dadurch sollen Sicherheitsvorfälle und ihre Dimensionen erkennbar werden, was Voraussetzung dafür ist, um diese im Vorfeld erfolgreich abzuwehren zu können. Unter einem Sicherheitsvorfall sind alle Ereignisse zu verstehen, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben. Die potentiellen Sektoren für Betreiber eines wesentlichen Dienstes werden in Art. 5 Abs. 1 NIS-RL aufgelistet. Mit fast 8-monatiger Verspätung setzte der österreichische Gesetzgeber mit dem NISG[3] diese RL um, wobei alle in der RL genannten Sektoren in § 2 NISG als wesentlich bestimmt werden.

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastrukturen,
- Gesundheitswesen,
- Trinkwasserlieferung und -versorgung,
- Digitale Infrastruktur, sowie Anbieter Digitaler Dienste.

---

1 NIS-RL: RL (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016.

2 Art. 4 Z. 4 NIS-RL : «*Betreiber wesentlicher Dienste*» eine öffentliche oder private Einrichtung einer in Anhang II genannten Art, die den Kriterien des Art. 5 Abs. 2 entspricht: «*Eine Einrichtung stellt einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist; die Bereitstellung dieses Dienstes ist abhängig von Netz- und Informationssystemen; und ein Sicherheitsvorfall würde eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken.*»

3 NISG: Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG).

2. Technische Grundlagen

2.1. SCADA[4]

Der Grund warum gerade wesentliche Dienste durch Cyberangriffe bedroht sind, liegt an den Fernwirksystemen: SCADA ist eine breit eingesetzte Technologie zur Überwachung von Produktionsabläufen i.V.m. Sensoren und Aktoren (Steuerungen). Diese Systeme werden in zahlreichen lt. NIS-RL und NISG bestimmten Sektoren für wesentliche Dienste eingesetzt. Deren Verwundbarkeit begründet sich ua. dadurch, dass häufig gleichartige Systeme des selben Herstellers branchenübergreifend, manchmal auch vernetzt eingesetzt werden, und somit zahlreiche neuartige Angriffsvektoren gegenüber Industrien entstehen, die es so vorher nicht gegeben hat. Die Steuerung erfolgt über eigens dafür geschaffene Rechnernetze, und heute vermehrt gesichert über das Internet. Aus der Historie gesehen sind nämlich SCADA Systeme in sich abgeschlossen und somit von anderen Systemen isoliert; die Frage der IT-Sicherheit hat sich daher in der Vergangenheit nicht gestellt. Jedoch aufgrund der zunehmenden Vernetzung von SCADA mit der Organisation und zukünftig auch mit Smart-Homes udgl., werden Hackerattacken zwecks Sabotage oder Terror immer attraktiver. Technisch bekannte Hilfsmittel des «bösen Zoos» wie Viren, Würmer und Trojanische Pferde werden grob fahrlässig bis sogar bereitwillig mit Hilfe von Spielen, Apps, USB-Sticks, E-Mail Anhängen, uvm. in die Organisationsinfrastruktur eingeschleust, deren malignes Wirken dann auf die wesentliche bzw. kritische Infrastruktur[5] und somit auf SCADA überspringen kann.

Ein historisch bedeutendes Beispiel dafür ist das Wirken des Computerwurms Stuxnet[6], welches eine hochspezialisierte Software zum Angriff auf SCADA Systeme darstellte. Der Beginn der Verbreitung startete im Jahre 2007, und erst im Jahre 2010 kam es in den Urananreicherungsanlagen im Iran zu massiven Störungen.

2.2. IoT[7]

Das Internet of Things ist eine Weiterentwicklung der üblicherweise isolierten SCADA Systeme hin zu flexiblen, und millionenfach vernetzten Komponenten mit Sensoren und Aktoren, deren potenzielle Einsatzgebiete jene der NIS-RL weitaus übertreffen. Es werden somit nicht nur wesentliche Dienste mit neuen Risiken der Cybersicherheit konfrontiert, sondern auch Haushalte, öffentlicher Dienst, KMUs, uvm. Bei Einsatz von IoT stellt sich weiters insb. bei Haushalten aber auch bei Unternehmen die Frage der Privacy, wobei hier gem. DSGVO ebenfalls der Stand der Technik für die Gewährleistung der Sicherheit einzuhalten ist.

Der technische Entwicklungsprozess ist bei weitem nicht abgeschlossen, sondern betrifft immer mehr die Privatsphäre der Nutzer. Besonders wird im Symantec Report[8] die Gefahr durch das IoT zugemessen, welches dort leicht sarkastisch als «*Insecurity of Things*» tituliert wird. Bis 2020 sollen demnach geschätzte 21 Milliarden IoT-Geräte weltweit im Netz angebunden sein. Nachdem jedes dieser Geräte eine Firmware, dh. eine Betriebssoftware, besitzt, wo nicht sichergestellt sein kann, ob diese vor Hackerangriffen sicher, aktuell oder überhaupt wartbar ist, wo weiters nicht sichergestellt ist wer und wann solch eine zeitraubende Wartung durchführen soll, stellen diese Geräte «*eine latente Sicherheitslücke für jeden Haushalt und für jedes Unternehmen dar. Auch bieten sich solcherart ungewartete Geräte geradezu für die Schaffung eines Botnetzes*[9] *an, wo zu bestimmten Zeiten weltweit, dezentral Angriffe gegen kritische Infrastrukturen oder ganze Staaten gefahren werden können – eine tickende Zeitbombe eben.*»[10]

---

4 SCADA: Supervisoring Control And Data Akquisition.

5 Legaldefinition «Kritische Infrastruktur» gem. § 74 Abs. 1 Z. 11 StGB (BGBl. 60/1974) u. § 22 Abs. 1 Z. 6 SPG (BGBl. 566/1991 idgF.)

6 Computerwurm: «RootkitTmphider»; Nachfolger «Duqu».

7 IoT: Internet of Things.

8 Symantec: 2016 Internet Security Threat Report, Symantec Corporation, Mountain View, 2016.

9 Von Roboter: Verteiltes, automatisiertes Netzwerk von Schadprogrammen.

10 Hrdinka, Auf Spurensuche in der Cyberwelt - Digitale Beweise mit IT-Forensik, 45. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, NWV Verlag, 2018.

2.3. Schutz

Die Maßnahmen gem. dem Stand der Technik für den Schutz wesentlicher bzw. kritischer Infrastrukturen müssen folglich lauten[11]:

- Recht: die NIS-RL musste von den MS bis spätestens 9. Mai 2018 in nationales Recht umgesetzt werden. Der österreichische Gesetzgeber tat dies verspätet mit dem NISG, welches die geforderten Computer Notfall Teams, Meldepflichten von Sicherheitsvorfällen, Risikoanalysen, Sicherheitskonzepte konkretisiert.
- Organisation: eine Risikoanalyse und Bewertung der Risiken ist ein erster Schritt um Sicherheitskonzepte, Berechtigungspyramiden, technische Sicherheitsmaßnahmen und regelmäßige Audits zu erstellen.
- Technik: regelmäßige Updates und Patches der Softwarehersteller müssen nicht nur in der Organisationsinfrastruktur sondern auch in den SCADA und IoT Systemen erfolgen – eine nicht zu unterschätzende aufwändige und kostenintensive Herausforderung.
- Technische Normen: Die NIS-RL fordert eine einheitliche Anwendung internationaler Sicherheitsnormen, wobei dafür der ENISA[12] eine beratende Funktion zukommt.

2.4. Technische Normen

Gem. § 21 Abs. 1 NISG haben Anbieter digitaler Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen, wobei in lit. e leg. cit. die Einhaltung der internationalen Normen einzuhalten sind. In § 17 Abs. 1 NISG wird bestimmt, dass Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen haben. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein. In den Erläuterungen wird in diesem Zusammenhang auf die europäischer Ebene (z.B. mit Unterstützung der ENISA) und bereits bestehende und etablierte internationale Standards verwiesen, die für diesen Bereich einschlägig sind. Jedoch hat die ENISA bis dato keine neuen Standards ausarbeiten lassen, und verweist in ihrem jüngsten einschlägigen Report[13] auf bekannte IT-Sicherheitsstandards wie insb. der prozessorientierten technischen Norm ISO 27001[14]. Obwohl dieser Standard weitgehend verbreitet ist, so ist er nicht speziell für SCADA Systeme und schon gar nicht für IoT entworfen worden. Somit ist diese Empfehlung der ENISA zu hinterfragen, zumal die beschriebenen Maßnahmen in dieser Normenreihe für viele betroffene Betreiber wesentlicher Infrastrukturen als völlig überschießend gelten können.

2.4.1. NIST 800–82 Rev 2[15]

Eine in diesem Zusammenhang relevante US-Norm ist die NIST Special Publication 80082 Rev 2 «Guide to Industrial Control Systems (ICS) Security», welche eine Sicherheitsleitlinie für Industriekontrollsysteme darstellt, und wo Sicherheitsempfehlungen für SCADA und PLC[16] beschrieben werden. Darüber hinaus sind Verweise auf zahlreiche weitere einschlägige Securitynormen enthalten. Eine entsprechende Europäische Norm in gleicher Qualität sucht man in diesem Bereich vergeblich. Das ist der Grund, warum dieser Standard tlw. auch in Europa verwendet wird.

---

11 Hrdinka, Cyberkriminalität und Hackerattacken – Eine Gefährdung für die Abwasserwirtschaft?, Österreichische Wasserwirtschaftstagung «Die Zukunft der Abwasserwirtschaft in Österreich», ÖWAV, Linz, 2017.

12 ENISA: European Network and Information Security Agency.

13 ENISA, Improving recognition of ICT security standards – Recommendations for the Member States for the conformance to NIS Directive, Version 1.0, February 1, 2018.

14 EN ISO/IEC 27001:2017-06, International Organization for Standardization, Geneva, 2017.

15 NIST, SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, Gaithersburg, 2015.

16 PLC: Programmable Logic Controller.

Die Motivation zur Schaffung dieser technischen Norm war, dass obwohl SCADA mit herkömmlichen IT-Systemen zahlreiche gleiche Merkmale aufweisen, unterscheiden sie sich dadurch, dass die in ICS ausgeführte Logik direkte Auswirkungen auf die physische Welt hat. Einige dieser Merkmale umfassen ein erhebliches Risiko für die Gesundheit und Sicherheit von Menschenleben, schwere Umweltschäden sowie negative Auswirkungen auf die Wirtschaft. ICS haben besonders erhöhte Leistungs- und Zuverlässigkeitsanforderungen und stehen manchmal im Widerspruch zur Sicherheit beim Entwurf und Betrieb von Steuerungssystemen.

2.4.2. NISTIR 8228 (Draft)[17]

Die besondere Herausforderung bei IoT ist im Gegensatz zu SCADA der Schutz personenbezogener Daten. Aus diesem Grund wird derzeit an einer speziellen Norm für IoT Sicherheit gearbeitet, des NISTIR 8228 «Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks». Dieser Entwurf enthält interessante und verfolgenswerte Ansätze. Eine europäische Norm ist hingegen so wie für SCADA nicht verfügbar. Die Vorschläge zum Umgang mit Sicherheits- und Datenschutzrisiken bei IoT waren bis 24. Oktober 2018 öffentlich. Der Entwurf nennt drei Überlegungen, die sich auf den Datenschutz und die Sicherheit des IoT auswirken können, und enthält Empfehlungen für Organisationen bezüglich ihres IoT-Risikos:

- Gerätesicherheit: Es muss verhindert werden, dass ein Gerät für Angriffe verwendet wird, einschließlich der Teilnahme an DDoS[18] Attacken, dem Abhören des Netzwerkverkehrs oder des Beeinträchtigens anderer Geräte im selben Netzwerksegment. Dieses Ziel gilt für alle IoT-Geräte.
- Datensicherheit: Schutz der Vertraulichkeit, Integrität und/oder der Verfügbarkeit von Daten (incl. personenbezogene Daten), die vom IoT-Gerät erfasst, gespeichert, verarbeitet oder übertragen werden. Dieses Ziel gilt für jedes IoT-Gerät mit Datenverarbeitungen.
- Privatsphärenschutz: Schutz der Privatsphäre von Personen, die durch die Verarbeitung personenbezogener Informationen beeinträchtigt werden über die Risiken betreffend Geräte- und Datensicherheit hinaus. Dieses Ziel gilt für alle IoT-Geräte, die personenbezogene Daten verarbeiten.

3. Rechtsdogmatische Bewertung

3.1. Risiko

Die Forderung nach einer Risikoabschätzung und folglich der Risikominimierung ist sowohl in Art. 32 Abs. 1 DSGVO[19] und Art. 4 Z. 9 NIS-RL bestimmt. Gem. NIS-RL wird das Risiko definiert als «*alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben*», hingegen wird in § 3 Z. 8 NISG eine davon abweichende Legaldefinition verwendet: «*alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben.*» Den Unterschied macht das Fehlen des vernünftigen Aufwandes. Wenn nicht in §§ 21 und 22 Abs. 1 bei den zu treffenden Sicherheitsvorkehrungen eben dieser vernünftige Aufwand beim feststellbaren Risiko i.S.d. NIS-RL erwähnt wäre, so würde ansonsten eine allumfassende Risikoanalyse durchzuführen sein, was einem «Gold-Plating» entspräche.

Diese Verankerung des Verhältnismäßigkeitsgrundsatzes, der sich in Art. 14 Abs 1 NIS-RL findet, ist wesentlich um überschießende Maßnahmen per se zu vermeiden: In dieser Bestimmung wird die Verhältnismäßigkeit

---

17 NIST, Draft NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, National Institute of Standards and Technology, Gaithersburg, 2018.

18 DDoS: Distributed Denial of Service.

19 Datenschutzgrundverordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016; Art. 32 Abs. 1: «*Sicherheit der Verarbeitung: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.*»

nicht nur angesprochen, sondern auch näher definiert. Demnach müssen die Sicherheitsanforderungen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

3.2. Stand der Technik

Im Hinblick auf SCADA und in naher Zukunft absehbar auch IoT Systeme haben Betreiber wesentlicher Dienste geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen. Diese haben geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen, und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein (Vgl. §§ 17 bzw. 19 Abs. 1 NISG).

Da die technische Entwicklung schneller als die Gesetzgebung ist, hat es sich in vielen Rechtsbereichen bewährt, den unbestimmten Rechtsbegriff «Stand der Technik» zu verwenden. Der Stand der Technik, auch als best available techniques (beste verfügbare Technik – BVT) bezeichnet, ist nach der in der Kalkar-Entscheidung[20] des Deutschen Bundesverfassungsgerichts entwickelten Drei-Stufen-Theorie von den anerkannten Regeln der Technik und dem Stand von Wissenschaft und Technik zu unterscheiden. Wenn die Rechtsordnung mit dem Maßstab der allgemein anerkannten Regeln stets einer weiter strebenden technischen Entwicklung hinterher hinkt, wird das lt. Rz. 97 vermieden, wenn «*der rechtliche Maßstab für das Erlaubte oder Gebotene hierdurch an die Front der technischen Entwicklung verlagert wird, da die allgemeine Anerkennung und die praktische Bewährung allein für den Stand der Technik nicht ausschlaggebend sind. Bei der Formel vom Stand der Technik gestaltet sich die Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte allerdings schwieriger. Sie müssen in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist*».

Die einzige Legaldefinition in der österreichischen Rechtsordnung zum «Stand der Technik» findet sich in § 2 Abs. 8 Z. 1 AWG[21] i.V.m. § 71a Abs. 1 GewO[22]: «*Der Stand der Technik (beste verfügbare Techniken – BVT) der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist*». Bei der Festlegung des Standes der Technik ist weiters unter Beachtung der sich aus einer bestimmten Maßnahme ergebenden Kosten und ihres Nutzens und des Grundsatzes der Vorsorge und der Vorbeugung im Allgemeinen wie auch im Einzelfall im AWG bestimmte Kriterien zu berücksichtigen, was auch in diesem Fall den Verhältnismäßigkeitsgrundsatz normiert.

Selbstverständlich können die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterschiedlich sein, sodass es nicht möglich ist, den Stand der Technik abschließend zu beschreiben. Dementsprechend fehlt es auch dem NISG an einer abschließenden Begriffsdefinition. Aus Gründen der Rechtssicherheit würde es jedoch in hohem Maß sinnvoll erscheinen, gewisse Grundlagen festzulegen. Angelehnt an die Gesetzesbegründung zum deutschen BSIG[23] bzw. an die Vorgaben des IT-Sicherheitsstandards ISO 2700114 sollte das NISG zumindest folgende oder ähnliche Konkretisierung[24] enthalten: «*Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren,*

---

[20] Beschluss BVerfG 2 BvL 8/77 vom 8. August 1978.

[21] Abfallwirtschaftsgesetz BGBl I 102/2002.

[22] § 79 Abs. 1 Gewerbeordnung BGBl. 194/1994 idgF: «*Die Behörde hat Auflagen dann nicht vorzuschreiben, wenn sie unverhältnismäßig sind, vor allem wenn der mit der Erfüllung der Auflagen verbundene Aufwand außer Verhältnis zu dem mit den Auflagen angestrebten Erfolg steht.*»

[23] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik BGBl I S 2821.

[24] Bundeskammer der Ziviltechniker, 16/SN-78/ME XXVI. GP – Stellungnahme zu Entwurf, 29. Oktober 2018.

Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Standes der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.»

Diese Einstufung und Abgrenzung schlägt sich in dieser Definition in der Formulierung «Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen» nieder. Vgl. dazu Bartels[25]: «*demzufolge wird dann die zentrale Frage zu stellen sein, unter welchen Voraussetzungen vom objektiv zu bestimmenden Stand der Technik, der das beste und effektivste Schutzniveau meint, welches auf dem Markt erhältlich ist, nach unten aus subjektiven Gründen (technische subjektive Unmöglichkeit und wirtschaftliche Zumutbarkeit) abgewichen werden kann.*»

Im Bereich IoT würde eine ISO 27001 Sicherheitsprüfung als größtenteils verfehlt erscheinen, und geeignete technische Normen sucht man bis dato vergeblich. Best Practices oder der derzeit sich in Begutachtung befindliche US-Standard NISTIR 8228 für IoT können hier jedoch brauchbare Alternativen bieten. Die Folgen der Missachtung von Mindestanforderungen sollen im Folgenden rechtsdogmatisch aufbereitet werden.

3.3. Haftung

Obwohl mit der Meldung gem. NIS-RL keine höhere Haftung der zur Meldung von Vorfällen verpflichteten Partei begründet wird, werden im NISG keinerlei Haftungsbestimmungen aber auch umgekehrt Haftungsbeschränkungen normiert. Die subjektive Vorwerfbarkeit gegenüber den Entwicklern und Betreibern wesentlicher Dienste kann jedenfalls gem. § 1299 ABGB[26] mit der Sachverständigenhaftung begründet werden, denn wer sich als Experte oder Spezialist ausgibt, kann sich nicht mit mangelnder Erfahrung oder Unkenntnis entschuldigen. Im Einzelfall wird letztlich die Judikatur über die Haftung zu entscheiden haben.

Gem. ErwGr. 50 der NIS-RL sind zwar Hersteller von Hardware und Softwareentwickler keine Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste, jedoch verstärken ihre Produkte die Sicherheit von Netz- und Informationssystemen. Daher spielen sie eine wichtige Rolle dabei, die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste in die Lage zu versetzen, ihre Netz- und Informationssysteme sichern zu können. Derartige Hardware- und Softwareprodukte unterliegen lt. ErwGr. 50 bereits geltenden Produkthaftungsvorschriften. Ob Software allerdings der verschuldensunabhängigen Produkthaftung unterliegt ist gemeinhin umstritten[27] und wird mehrheitlich verneint, denn Produkte im Sinne des § 4 PHG[28] sind bewegliche körperliche Sachen, seien sie auch Teil einer anderen Sache, und Energie. Wenn hingegen Software «embedded» ist, also bspw. die Firmware einer PLC eines SCADA Systems oder insb. IoT-Geräte Teil einer beweglichen körperlichen Sache ist, dann wird die Produkteigenschaft mehrheitlich bejaht. Es kommt daher darauf an, ob die Software selbst als Sache angesehen werden kann[29], oder Teil einer beweglichen Sache ist. Vgl. dazu auch Völkel zu virtuellen Währungen: «*Wenn die Einheiten virtueller Währungen erst einmal erzeugt sind, so handelt es sich um Sachen i.S.d. § 285 ABGB*»; dh. virtuelle Währungen (Software) könnten sehr wohl als bewegliche Sache klassifiziert werden, wenn der Erzeugungsprozess begründet werden kann. Interessant ist in diesem Zusammenhang, dass die NIS-RL im ErwGr. 50 im Falle Software eine Produkthaftung beispielhaft erwähnt, was zukünftig in richtungsweisende Judikatur einfließen könnte.

---

[25] Bartels, TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin, 13. August 2016. Stellungnahme zum «Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik» des BSI.

[26] Allgemeines Bürgerliches Gesetzbuch JGS 946/1811 idgF.

[27] Koziol/Apathy/Koch, Gefährdungs-, Produkt- und Eingriffshaftung, in: Österreichisches Haftpflichtrecht, Band III, Jan Sramek Verlag, Wien 2014, ISBN 978-3-7097-0022-8, S. 136 ff.

[28] Produkthaftungsgesetz BGBl 99/1988 idgF.

[29] Völkel, Privatrechtliche Einordnung der Erzeugung virtueller Währungen, Ecolex Juli 2017, Manz, S. 639–641.

3.4. Strafrecht

Der Widerrechtliche Zugriff auf ein Computersystem[30] wird im § 118a StGB[31] geregelt, sowie im Verwaltungsstrafrecht gem. §§ 62 u. 63 DSG[32], wenn personenbezogene Daten betroffen sind. Unterscheiden sich beide Bestimmungen im Wortlaut «Zugriff auf ein Computersystem» im StGB vs. «Zugang zu einer Datenverarbeitung» im DSG, so sind unter Computersystem gem. § 74 Z. 8 StGB sowohl die einzelne als auch verbundene Vorrichtung, die der automationsunterstützten Datenverarbeitung dient zu verstehen. Auch wenn gem. § 118a StGB mehr Tatbestandsmerkmale erfüllt sein müssen als nach § 62 DSG, stehen diese Bestimmungen zueinander in Konkurrenz, weil beide die widerrechtliche Verschaffung eines Zugangs zu einer Datenverarbeitung unter Strafe stellen. Nachdem der Gesetzgeber diese Bestimmung des § 52 DSG-2000 wortgleich im § 62 DSG, welches seit 25. Mai 2018 in Kraft ist, übernommen hat, wäre eine Reparatur ehestmöglich geboten, da eine Subsidiaritätsregelung im Hinblick auf die einschlägigen Bestimmungen des Strafgesetzbuches fehlt, insb. in Bezug auf § 118a. Aufgrund des Doppelbestrafungsverbots ne bis in idem des Art. 4 Abs. 1 des 7. ZP zur EMRK würde eine Strafverfolgung eines Verdächtigen, welcher bereits mit einer Verwaltungsstrafe gem. §§ 62 oder 63 DSG im selben Fall pönalisiert wurde, wohl nicht möglich sein. Ein wesentlicher Unterschied zum Datenschutz ist, dass die Strafbarkeit nach § 118a StGB nur dann gegeben ist, wenn der Täter beabsichtigt, die Daten seines Opfers auszuspionieren. Lt. Reindl-Krauskopf[33] wird diese Absicht neben der Datenverwendungs- und Gewinn- bzw. Schädigungsabsicht verlangt[34]. Er muss außerdem eine spezifische Sicherheitsvorkehrung überwinden; ist diese nicht vorhanden oder entspricht nicht dem Stand der Technik, so könnte der Täter straffrei bleiben. Diese Umstände sind i.Z.m. IoT umso prekärer, als gerade beim Hacken von IoT Geräten das Strafrecht mit dem Datenschutz im Falle der Verarbeitung personenbezogener Daten kollidiert.

Eine weitere in gewissen Fällen problematische, jedoch im Gegenzug zur vorherigen so gewollte Bestimmung ist, dass der § 118a ein Ermächtigungsdelikt darstellt. Werden Unternehmen gehackt, so wird fallweise von einer Anzeige abgesehen, wenn der potenzielle Schaden durch Bekanntwerden des Angriffs höher eingestuft wird, als der tatsächlich eingetretene. Weiters können bei einem Hackerangriff auch die Ermächtigungsdelikte § 119 StGB, der Verletzung des Telekommunikationsgeheimnisses, bzw. § 119a StGB, dem missbräuchlichen Abfangen von Daten erfüllt sein, wenn eine spezielle Einrichtung oder Software am Zielsystem installiert wird, um Geheimnisse wie Passwörter zu erspähen. Da die Täter nur auf Ermächtigung des Opfers verfolgt werden können, ist eine Strafverfolgung dann ausgeschlossen, wenn die Opfer keine Kenntnis über das Hacken ihrer Systeme oder das Abfangen ihrer Daten haben, was i.d.R. der Fall sein wird. In diesem Zusammenhang kommt das NISG ins Spiel, wo Betreiber wesentlicher Dienste zur Meldung von Sicherheitsvorfällen verpflichtet werden. Die operative Unterstützung und der Informationsaustausch würde eine Verbesserung der gegenwärtigen oben beschriebenen unbefriedigenden Situation darstellen, jedoch wäre der Anwendungsbereich ausschließlich bei den im NISG benannten wesentlichen Betreibern gegeben. Andere Branchen die zukünftig IoT Systeme nutzen werden wohl auf sich alleine gestellt bleiben.

Technisch gesehen erfordert das Hacken eines Computersystems i.d.R. auch dessen Veränderung, da Sicherheitsmechanismen zu überwinden sind, und somit das Computersystem zumindest zeitweise manipuliert werden muss, um eindringen zu können. Die Folge solcherart Angriffe sind nicht unerhebliche Aufwände der Opfer, welche diese beschädigten Sicherheitsmechanismen wieder in Stand bringen müssen bzw. die Passwörter neu vergeben müssen, und daher das System in der Funktionsweise gestört wird. Folglich sind häufig

---

30 Vgl. §§ 118a, 119a, 126a u. 126c StGB, BGBl 60/1974 idgF.

31 Strafgesetzbuch BGBl 60/1974 idgF.

32 Datenschutzgesetz BGBl I 165/1999 idgF.

33 Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 ff.

34 Reindl-Krauskopf, Computerstrafrecht im Überblick 11 ff; Reindl, E-Commerce und Strafrecht 147 ff; Thiele SbgK § 118a; Salimi, Zahnloses Cyberstrafrecht, ÖJZ 2012, 998 ff.

mehrere Tatbestände des StGB §§ 118a und 126a bis c bei einem Hackerangriff gleichzeitig erfüllt. Daher könnte ein Hackerangriff auf ein SCADA- oder IoT-System mit den bestehenden Rechtsinstrumenten von den zuständigen Behörden von sich aus verfolgt werden, wenn mindestens einer der Offizialdelikte §§ 126a, 126b, 126c StGB i.V.m. den Ermächtigungsdelikten §§ 118a, 119, 119a leg. cit. erfüllt wird.

4. Ausblick

IoT Systeme sind eine Weiterentwicklung von SCADA und erfordern zusätzlich spezifische Sicherheitsvorkehrungen und Risikoanalysen in Richtung personenbezogenen Datenschutz. Zumal es bei SCADA zumindest eine entsprechende US-Sicherheitsnorm existiert, trotz fehlenden europäischen Pendants, wird bei IoT derzeit vollkommenes Neuland betreten. Der Stand der Technik gründet daher in diesem Bereich hauptsächlich auf Sachverständigenwissen, aber immerhin wird in den USA an einer entsprechenden Sicherheitsnorm für IoT-Systeme gearbeitet. Bezüglich der Haftung von Betreibern und Herstellern von IoT Systemen fehlt es an spezifischen Vorschriften, und es wird wohl die Sachverständigenhaftung gem. ABGB als Rechtsnorm anzuwenden sein. Obwohl die NIS-RL i.d.Z. von einer Produkthaftung spricht, ist diese für Software, außer bei «embedded systems» weitgehend umstritten. Jedenfalls kann bei IoT (embedded System) von einer Produkthaftung ausgegangen werden. Strafrechtlich haben diese Umstände sehr wohl Bedeutung, denn beschädigt der Täter keine Daten am Computersystem des Opfers, unterdrückt nicht den Zugang zu diesen oder stört auch nicht die Funktionsfähigkeit, da er keine spezifische Sicherheitseinrichtung überwinden muss, so bleibt diese Tätigkeit ohne strafrechtlichen Schutz. Aus diesen Gründen wäre es geboten die gut gemeinte NIS-RL, umgesetzt durch das NISG als auch andere relevante Materialien nachzubessern.

5. Literatur

Bartels, TeleTrusT – Bundesverband IT-Sicherheit e.V., Berlin, 13. August 2016, Stellungnahme zum «Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik» des BSI.

Bundeskammer der Ziviltechniker, 16/SN-78/ME XXVI. GP – Stellungnahme zu Entwurf, 29. Oktober 2018.

BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77.

EN ISO/IEC 27001:2017-06, International Organization for Standardization, Geneva, 2017.

ENISA, Improving recognition of ICT security standards – Recommendations for the Member States for the conformance to NIS Directive, Version 1.0, February 1, 2018.

Hrdinka, Auf Spurensuche in der Cyberwelt – Digitale Beweise mit IT-Forensik, 45. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, NWV Verlag, 2018.

Hrdinka, Cyberkriminalität und Hackerattacken – Eine Gefährdung für die Abwasserwirtschaft?, Österreichische Wasserwirtschaftstagung «Die Zukunft der Abwasserwirtschaft in Österreich», ÖWAV, Linz, 2017.

Koziol/Apathy/Koch, Gefährdungs-, Produkt- und Eingriffshaftung, in: Österreichisches Haftpflichtrecht, Band III, Jan Sramek Verlag, Wien 2014, ISBN 978-3-7097-0022-8, S. 136 ff.

NIST, Draft NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, National Institute of Standards and Technology, Gaithersburg, 2018.

NIST, SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, Gaithersburg, 2015.

Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 ff.

Reindl-Krauskopf, Computerstrafrecht im Überblick 11 ff; Reindl, E-Commerce und Strafrecht 147 ff; Thiele SbgK § 118a; Salimi, Zahnloses Cyberstrafrecht, ÖJZ 2012, 998 ff.

Symantec: 2016 Internet Security Threat Report, Symantec Corporation, Mountain View, 2016.

Völkel, Privatrechtliche Einordnung der Erzeugung virtueller Währungen, Ecolex Juli 2017, Manz, S. 639–641.