STAND DER TECHNIK VON NIS-MASSNAHMEN – AUSLEGUNGSHILFEN ZWISCHEN IT, OT UND IOT

Alexander Novotny

Member des Privacy Sustainable Computing Lab, Wirtschaftsuniversität Wien, Institut für Wirtschaftsinformatik und Gesellschaft
Welthandelsplatz 1, 1020 Wien, AT
alexander.novotny@wu.ac.at; https://www.privacylab.at

Schlagworte: ***Informationssystemsicherheit, NIS-Richtlinie, Stand der Technik, Internet of Things***

Abstract: *Die Netz- und Informationssystemsicherheitsrichtlinie (NIS-RL) verpflichtet Betreiber bestimmter Dienste (z.B. Cloud-Computing, Online-Marktplätze, Banken, Energieversorgung, etc.) geeignete und verhältnismäßige Sicherheitsmaßnahmen unter Berücksichtigung des Stands der Technik zu ergreifen. Sicherheitsmaßnahmen können sich jedoch für klassische Informationstechnologie (IT), Operations Technology (OT) und im Internet of Things (IoT) unterscheiden. Dieser Beitrag ordnet bestehende und im NIS-Recht neu geschaffene Auslegungs-Mechanismen für den Stand der Technik in den Kontext von Sektoren, der Konvergenz von IT und OT sowie des Internet of Things ein.*

1. Einleitung

Der Cyberangriff auf das ukrainische Stromnetz 2015 hat gezeigt, wie verwundbar kritische Infrastrukturen durch ihre Abhängigkeit von Netz- und Informationssystemen sind. Insgesamt waren 225.000 Kunden in der Westukraine von dem mehrere Stunden dauernden Blackout betroffen.[1] 2016 hat die Europäische Union die Netz- und Informationssystemsicherheitsrichtlinie (NIS-RL) 2016/1148[2] verabschiedet, um ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union und das Funktionieren des wirtschaftlichen und gesellschaftlichen Lebens sowie des Binnenmarkts sicherzustellen[3]. In Österreich wurde die NIS-RL durch das Netz- und Informationssystemsicherheitsgesetz (NISG) sowie Änderungen im Telekommunikationsgesetz 2003 umgesetzt, welche mit Ablauf des 28. Dezember 2018 in Kraft getreten sind.[4] Anbieter digitaler Dienste (AdD), Betreiber wesentlicher Dienste (BwD) und Einrichtungen der öffentlichen Verwaltung (EdöV)[5] müssen NIS-Sicherheitsvorkehrungen am Stand der Technik umsetzen.[6]

NIS-Verpflichtete, welche kritische Netz- und Informationssysteme betreiben, müssen den unbestimmten Begriff des Stands der Technik zunächst grundsätzlich selbst bestimmen[7]. Diese wissen vielfach nicht welche konkreten Maßnahmen sie treffen müssen, um den rechtlichen Erfordernissen zu entsprechen. Die unter Unternehmen wahrgenommene Rechtsunsicherheit ist hoch. Im Gegenzug werden aber auch Unklarheiten über

---

1 Vgl. Electricity Information Sharing and Analysis Center (E-ISAC), SANS Industrial Control Systems, Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (aufgerufen am 22. November 2018), 18. März 2016, S. iv.

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 Erwägungsgrund 1 leg. cit.

4 Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) erlassen und das Telekommunikationsgesetz 2003 geändert wird, BGBl. I Nr. 111/2018.

5 §§ 17 Abs. 1., 21 Abs. 1, 22 Abs. 1 leg. cit.

6 Art. 14, 16 NIS-Richtlinie 2016/1148, ABl. L 2016/194, 20-21.

7 Vgl. Ellmer/Schremser, Der «Stand der Technik» als Kostentreiber? Sind Stand und Regel der Technik Synonyme?, ZVB 2018, S. 278 (S. 279).

die Auslegung von Technikklauseln wie der Stand der Technik-Klausel, über Zusammenhänge zwischen den einzelnen relevanten Rechtsakten einer Materie und ein übertriebenes Begehren nach absoluter Rechtssicherheit als Kostentreiber von technischen Projekten in der Literatur identifiziert.[8]

Hinzukommt, dass Netz- und Informationssysteme in betroffenen NIS-Sektoren häufig auf technischen Lösungen und Komponenten im Bereich des Internets der Dinge (Internet of Things [IoT]) sowie der Automatisierungs- und Prozessleittechnik (Operations Technology [OT]) basieren. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) definiert das IoT als ein «cyberphysisches Ökosystem aus verbundenen Sensoren und Aktuatoren, welche intelligente Entscheidungsfindung ermöglichen»[9]. Beispielsweise werden in den Sektoren Energie sowie Trinkwasserlieferung und -versorgung industrielle Steuerungssysteme (Industrial Control Systems [ICS]) für Öl-, Gas-, Elektrizitäts- und Wasser-Anlagen verwendet. Intelligente Stromnetze (Smart Grids) nützen intelligente Messgeräte (Smart Meters), welche Kommunikationsnetzwerk-basiert die Ausbalancierung von Energiebereitstellung und Energieverbrauch ermöglichen.[10] Im NIS-Teilsektor Straßenverkehr werden intelligente Verkehrssysteme zur Erhöhung der Verkehrssicherheit und Herstellung einer Kommunikationsverbindung zwischen Fahrzeug und Verkehrsinfrastruktur eingesetzt.[11]

Von AdD und BwD bereits heute häufig genützte Normenreihen der Informationssicherheit, wie beispielsweise die ISO/IEC 27000-Reihe und die IT-Grundschutz Standards des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI)[12], sehen für bestimmte Sektoren und Arten von Netz- und Informationssystemen besondere ergänzende Leitlinien und Empfehlungen vor. Ergänzende Normen existieren zum Beispiel für IoT und ICS-Umgebungen[13], das Gesundheitswesen[14], die OT-Sicherheit im Energiesektor[15] und die Sicherheit von Cloud-Diensten[16]. Sie modifizieren, ergänzen und ersetzen teilweise die für Systeme der Informationstechnologie (IT) in der jeweiligen Grundnorm empfohlenen Sicherheitsmaßnahmen.

Dieser Beitrag ordnet bestehende Standards, Normen und Leitlinien sowie im Zuge des NIS-Rechts neu geschaffene Auslegungs-Mechanismen für den Stand der Technik von Sicherheitsmaßnahmen in den Kontext von Sektoren, der OT und des Internet of Things ein.

2. Der unbestimmte Begriff des «Stands der Technik» und seine Präzisierung

Die «Kalkar I – Entscheidung» des deutschen Bundesverfassungsgerichts 1978[17] war wegweisend für die heute vorherrschende dreistufige Definition von Technikklauseln:

---

8 Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 283).

9 Vgl. European Union Agency for Network and Information Security (ENISA), Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017, S. 18.

10 Vgl. Verordnung des Bundesministers für Wirtschaft, Familie und Jugend, mit der die Einführung intelligenter Messgeräte festgelegt wird (Intelligente Messgeräte-Einführungsverordnung – IME-VO), BGBl. II Nr. 138/2012 i.d.F. BGBl. II Nr. 383/2017.

11 Vgl. Art. 2 Abs. 1 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträger, ABl. L 2010/207, 4.

12 Vgl. Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1 – Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Oktober 2017; Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, Oktober 2017; Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Oktober 2017.

13 Ebenda.

14 ISO 27799:2016, Health informatics – Information security management in health using ISO/IEC 27002[2], Juli 2016.

15 ISO/IEC 27019:2017, Information technology – Security techniques – Information security controls for the energy utility industry[1], Oktober 2017.

16 ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, Dezember 2015.

17 BVerfG 2 BvL 8/77 vom 8. August 1978.

- Anerkannte Regeln der Technik
- Stand der Technik
- Stand von Wissenschaft und Technik

Auf niedrigster Stufe stehen die anerkannten Regeln der Technik, welche sich in der österreichischen Rechtsordnung als Legaldefinition beispielsweise in § 4 Z. 27 NÖ BO[18] finden. Anerkannte Regeln der Technik entsprechen einer unter technischen Praktikern und Experten allgemein anerkannten Mehrheitsauffassung an Grundsätzen[19], welche sich in der Praxis bewährt haben[20]. Neben den materiellen Anforderungen an eine technische Lösung stellen die anerkannten Regeln der Technik vor allem auf prozessuale Aspekte der ordnungsgemäßen Aus- und Durchführung einer technischen Kunst ab, wie zum Beispiel der «Baukunst»[21].

Eine Stufe höher steht der Begriff des Stands der Technik, bei dem es nicht auf eine allgemeine Anerkennung ankommt, welche sich bei neuen technisches Verfahren typischerweise nur langsam etabliert.[22] Die Funktionstüchtigkeit des fortschrittlichen technischen Verfahrens muss erprobt und erwiesen sein.[23] Eine bloße Durchsetzung des Verfahrens in der Praxis ist ausreichend, welche nicht notwendigerweise bereits auf einer allgemeinen Anerkennung durch technische Experten basiert.[24] Im Europarecht existiert zusätzlich der Begriff der «besten verfügbaren Technik» (BVT) bzw. «best available technology» (BAT), welche der österreichische Gesetzgeber regelmäßig mit dem «Stand der Technik» per Legaldefinition, zum Beispiel in § 71a Abs. 1 GewO[25] und § 2 Abs. 8 Z. 1 AWG[26], gleichsetzt.[27]

Die höchste Anforderung stellt der Stand von Wissenschaft und Technik, der nicht mehr auf das realisierbare und umsetzbare begrenzt ist. Er beschreibt fortschrittlichste technische Verfahren auf Basis der neuesten Erkenntnisse, welche wissenschaftlich fundiert sind.[28] Für Rechtsanwender ist der aktuelle Stand von Wissenschaft und Technik am schwierigsten zu ermitteln, da er sich am dynamischsten ändert sowie der aktuelle Stand der Forschung und noch laufende wissenschaftliche Kontroversen mit zu berücksichtigen sind.[29]

Der «Stand der Technik» ist demnach ein unbestimmter Rechtsbegriff, der jedoch auf unterschiedliche Weise nachfolgend mit Bedeutung gefüllt werden kann. Er ist kein Satz fix festgelegter Anforderungen zu einem Zeitpunkt, sondern eine Bandbreite möglicher technischer Umsetzungsvarianten zwischen den anerkannten Regeln der Technik als Untergrenze und dem Stand der Wissenschaft und Technik als Obergrenze.[30]

Aufgrund der dynamischen Entwicklung der Technologie im Bereich der Netz- und Informationssystemsicherheit hat der Unionsgesetzgeber in Art. 16 Abs 1. NIS-RL[31] auf eine Legaldefinition und Verweise verzichtet. Lediglich der Begriff der «Sicherheit der Systeme und Anlagen»[32] wurde mittels Durchführungsverordnung insoweit konkretisiert, als er das systematische Management von Netz- und Informationssystemen, die physi-

[18] NÖ Bauordnung 2014, LGBl. Nr. 1/2015.
[19] Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 281).
[20] Vgl. Seibel, Abgrenzung der «anerkannten Regeln der Technik» vom «Stand der Technik», NJW 2013, S. 3000 (S. 3001).
[21] Rechberger, Der Sachverständige und die «allgemein anerkannten Regeln der Technik», bauaktuell 2015, S. 15 (S. 17).
[22] Vgl. Seibel, NJW 2013, S. 3000 (S. 3003).
[23] Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 279).
[24] Vgl. Seibel, NJW 2013, S. 3000 (S. 3003).
[25] Gewerbeordnung 1994, BGBl. Nr. 194/1994 i.d.F. BGBl. I Nr. 125/2013.
[26] Abfallwirtschaftsgesetz 2002, BGBl. I Nr. 102/2002 i.d.F. BGBl. I Nr. 70/2017.
[27] Vgl. Piska/Erlacher, Beste verfügbare Techniken – eine neue Größe im Anlagenrecht? ZTR 2014, S. 67 (S. 74).
[28] Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 283).
[29] Vgl. Seibel, NJW 2013, S. 3000 (S. 3003).
[30] Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 284).
[31] NIS-Richtlinie 2016/1148, ABl. L 2016/194, 1.
[32] Art. 16 Abs 1. lit. a leg. cit.

sche Sicherheit und die Sicherheit der Umgebung, die Versorgungssicherheit und die Kontrolle des Zugangs zu Netz- und Informationssystemen umfasst.[33]

In Erwägungsgrund 66 der NIS-RL wird erwogen, dass die Entstehung von Normen für Sicherheitsanforderungen «ein vom Markt ausgehender Vorgang»ist und die «Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern» sollten.[34] Der Unionsgesetzgeber hat einen Primat der Definition des Stands der Technik im Wege der Normung vorgegeben. Systematisch ist trotzdem darauf hinzuweisen, dass bei sich widersprechenden rechtlichen und im Wege der Normung entwickelten Sicherheitsanforderungen, das Recht maßgeblich ist.[35] Selbst wenn es zu einer geplanten konkreten Sicherheitsmaßnahme keine Anhaltspunkte im Recht oder in einschlägigen technischen Normen gibt, müssen Rechtsanwender bedenken, dass trotzdem ein Stand der Technik faktisch existiert. Dieser ist dann durch den Rechtsanwender selbst zu ermitteln, beispielsweise unter Zuhilfenahme empirischer Mittel wie Marktanalysen und Studien.

Kann die Einhaltung von einschlägigen Normen der Informationssicherheit nachgewiesen werden, ist dies eine starke Argumentationsgrundlage für eine normkonforme Lösung gegenüber anderen gleichwertigen, aber von der Norm abweichenden Lösungen. Nachweise können prozessual als Prima-facie Beweis dienen[36] und für sie besteht die widerlegbare Vermutung, dass der jeweilige Stand der Technik erfüllt wurde[37].

3. Auslegungshilfen auf Unions-Ebene

Zunächst bieten die Erwägungsgründe der NIS-Richtlinie Anhaltspunkte für die Auslegung von Sicherheitsmaßnahmen am Stand der Technik. In den Erwägungsgründen 49 und 57 wird darauf hingewiesen, dass AdD ein geringeres Risiko als BwD trifft und deshalb von diesen geringere Sicherheitsanforderungen gefordert werden sollten. Diese Wertung könnte so interpretiert werden, dass sich AdD im Kontinuum von möglichen Maßnahmen am Stand der Technik an weniger strengen Maßnahmen, die knapp über den anerkannten Regeln der Technik liegen, orientieren können. Für BwD dürfte dieser Maßstab jedoch nicht ausreichend sein.

Für BwD hat die in Art. 11 NIS-RL verankerte NIS-Kooperationsgruppe ein Referenzdokument für Sicherheitsmaßnahmen[38] herausgegeben. Die NIS-Kooperationsgruppe besteht aus Vertretern der Mitgliedstaaten, der Europäischen Kommission und der ENISA.[39] Das Referenzdokument definiert Grundprinzipien für Sicherheitsmaßnahmen und grenzt vier Domänen von Sicherheitsmaßnahmen ab: Governance und Ökosystem, Schutz, Verteidigung und Resilienz. Innerhalb der vier Domänen werden generische Sicherheitsmaßnahmen genannt (z.B. «Kryptographie» in der Domäne «Schutz»).[40]

In den Erwägungen zur NIS-Richtlinie wurde als Ziel festgeschrieben, dass die ENISA Leitlinien in Bezug auf die Normung von Sicherheitsanforderungen herausgeben solle[41] und die Kommission in Bezug auf Durchführungsrechtsakte zu Sicherheitsanforderungen für AdD den «Stellungnahmen der ENISA weitestgehend Rechnung tragen»[42] soll. Den Leitlinien der ENISA kommt demnach bei der Auslegung des Stands der Tech-

---

33 Vgl. Art. 2 Abs. 1 Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls, ABl. L 2018/26, 48.

34 Vgl. Erwägungsgrund 66, NIS-Richtlinie 2016/1148, ABl. L 2016/194, 10.

35 Vgl. Ellmer/Schremser, ZVB 2018, S. 278 (S. 281).

36 Vgl. Rechberger, Der Sachverständige und die «allgemein anerkannten Regeln der Technik», bauaktuell 2015, S. 15 (S. 15).

37 Vgl. Seibel, NJW 2013, S. 3000 (S. 3001).

38 NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, Februar 2018.

39 Art. 11 Abs. 2 NIS-Richtlinie 2016/1148, ABl. L 2016/194, 17.

40 Vgl. NIS Cooperation Group, Februar 2018, S. 18.

41 Vgl. Erwägungsgrund 66, NIS-Richtlinie 2016/1148, ABl. L 2016/194, 10.

42 Vgl. Erwägungsgrund 69, leg. cit.

nik von Sicherheitsmaßnahmen hohes Gewicht zu. Die ENISA hat seit dem Inkrafttreten der NIS-Richtlinie 2016 zahlreiche Leitlinien in mehreren Bereichen der kritischen Infrastrukturen und digitalen Dienste herausgegeben, welche für die Auslegung des Stands der Technik von NIS-Maßnahmen in der OT und dem IoT Relevanz haben. Diese behandeln die Sicherheit des IoT im Kontext kritischer Informationsinfrastrukturen[43] und in ICS/SCADA Umgebungen[44], von Cloud-Diensten im Kontext des IoT[45], von intelligenten Spitälern und Gesundheitsdienstleistungen[46] sowie Flughäfen (Smart Airports)[47], von Distributed Ledger Technologien (Blockchains) im Finanzsektor[48], der Signalübertragung in der Telekommunikation[49] sowie Empfehlungen für Threat Intelligence Plattformen[50] und die Cybersicherheits-Kultur von Organisationen[51].

4. Auslegungshilfen auf nationaler Ebene in Österreich

Im österreichischen NIS-Gesetz ist für die von BwD und EdöV zu treffenden Sicherheitsvorkehrungen festgelegt, dass diese «den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein» haben.[52] Die von AdD zu treffenden Sicherheitsvorkehrungen hingegen «haben unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, das dem bestehenden mit vernünftigem Aufwand feststellbaren Risiko angemessen ist»[53]. In Gegenüberstellung zum ursprünglichen Ministerialentwurf des NISG müssen Sicherheitsvorkehrungen von BwD und EdöV den Stand der Technik nun genauso wie AdD nur mehr «berücksichtigen»[54] statt ihm zu «entsprechen»[55]. Daraus ist ein abgeschwächter Maßstab erkennbar.

Da für AdD keine Verordnungsermächtigung zur Festlegung geeigneter Sicherheitsvorkehrungen und keine ex ante Nachweispflicht vorgesehen ist[56], werden die zu treffenden Sicherheitsvorkehrungen ex lege insofern konkretisiert, als diese der Sicherheit der Systeme und Anlagen, der Bewältigung von Sicherheitsvorfällen, dem Betriebskontinuitätsmanagement, der Überwachung, Überprüfung und Erprobung sowie der Einhaltung der internationalen Normen Rechnung zu tragen haben[57]. Für BwD können konkrete Sicherheitsanforderungen, die jedenfalls als geeignet erachtet werden, im Verordnungswege durch den Bundeskanzler im Einvernehmen mit dem Innenminister festgelegt werden. Hierbei sollen auch die Ergebnisse der NIS-Kooperationsgruppe und der ENISA, sowie einschlägige internationale Standards der Netz- und Informationssicherheit berücksichtigt werden.[58]

---

43 Vgl. ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017.

44 Vgl. ENISA, Communication network dependencies for ICS/SCADA Systems, Dezember 2016.

45 Vgl. ENISA, Towards secure convergence of Cloud and IoT, September 2018.

46 Vgl. ENISA, Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures, November 2016.

47 Vgl. ENISA, Securing Smart Airports, Dezember 2016.

48 Vgl. ENISA, Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector, Dezember 2016.

49 Vgl. ENISA, Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation, März 2018.

50 Vgl. ENISA, Exploring the opportunities and limitations of current Threat Intelligence Platforms, Public Version 1.0, Dezember 2017.

51 Vgl. ENISA, Cyber Security Culture in organisations, November 2017.

52 §§ 17 Abs. 1., 22 Abs. 1 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), BGBl. I Nr. 111/2018.

53 § 21 Abs. 1. leg. cit.

54 §§ 17 Abs. 1., 22 Abs. 1 leg. cit.

55 §§ 15 Abs. 1., 19 Abs. 1 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), 78/ME XXVI. GP.

56 Vgl. Erläuterungen zu § 21 Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) erlassen und das Telekommunikationsgesetz 2003 geändert wird, 36/34 RV XXVI. GP, S. 21; § 4 Abs. 2 Z. 3 NISG, BGBl. I Nr. 111/2018.

57 § 21 Abs. 1. NISG, BGBl. I Nr. 111/2018.

58 Vgl. Erläuterungen zu § 17 NISG, 36/34 RV XXVI. GP, S. 19.

Das Bundeskanzleramt erarbeitet gemeinsam mit dem österreichischen Government Computer Emergency Response Team (GovCERT) und dem NIS-Büro, welches dem Innenministerium unterstellten Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT) zugeordnet ist, ein NIS Fact Sheet[59]. Das NIS Fact Sheet soll Rechtsanwender bei der Anwendung europäischer oder international anerkannter Normen unterstützen. Es ordnet die relevanten Normkapitel internationaler Informationssicherheitsstandards zu den in Abschnitt 3.2. beschriebenen, durch die NIS-Kooperationsgruppe definierten vier Domänen von Sicherheitsmaßnahmen zu. Erkannt und referenziert werden das österreichische Informationssicherheitshandbuch[60], der BSI IT-Grundschutz[61], die ISO 27001:2017[62], ISA/IEC 62443 3-3[63], die CIS Critical Security Controls (Version 6 / 7)[64] und das NIST Cybersecurity Framework[65].

Domäne	Schutz
Kategorie	Systemadministration
Sicherheitsmaßnahme	Administrative Zugangsrechte
Österreichisches Informationssicherheitshandbuch Version 4.0.1	9.1 Zugriffskontrollpolitik12.5 Protokollierung und Monitoring
BSI IT-Grundschutz	M 2.220, M 2.20, M 2.38, M 4.312
ISO 27001:2013	A.9.2.3 Management of privileged access rights
ISA/IEC 62443 3-3	SR 1.3, 1.4
CIS CSC Version 6.0	3, 5, 8, 11, 13, 14, 18
CIS CSC Version 7.0	5, 4, 8, 11, 13, 14, 18
NIST Cybersecurity Framework	PR.AT-2

Tabelle 1: Beispiel Sicherheitsmaßnahme «Administrative Zugangsrechte».[66]

Durch Nachweis der Einhaltung der im NIS Fact Sheet angeführten Teile bzw. Kapitel einer Norm können NIS-Verpflichtete die Erfüllung einer Sicherheitsmaßnahme nachweisen. Tabelle 1 beschreibt dies anhand des Beispiels der Absicherung administrativer Zugangsrechte zu Netz- und Informationssystemen, welchen aufgrund der ihnen zugeordneten erhöhten System-Privilegien ein hohes Gefährdungspotential innewohnt.

Neben der geplanten sektorübergreifenden Verordnung jedenfalls geeigneter Sicherheitsmaßnahmen steht den BwD durch ihre jeweiligen Sektorenverbände die Möglichkeit offen, eigene Branchensicherheitsstandards mit sektorspezifischen Sicherheitsvorkehrungen vorzuschlagen. Über die Eignung der in einem Branchenstandard erarbeiteten Sicherheitsvorkehrungen hat der Innenminister mittels Bescheid zu entscheiden. Spezifi-

59 Bundeskanzleramt, Авт. I/8 – Cyber Security / GovCERT / NIS-Büro BMI/II/BVT/5-NIS, Nationale Umsetzung der NIS-Richtlinie – NIS Fact Sheet 08/2018, Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices, Version 2.0, 29. Oktober 2018.

60 Zentrum für sichere Informationstechnologie – Austria (A-SIT), Österreichisches Informationssicherheitshandbuch, Version 4.0.1, 19. Jänner 2016.

61 BSI-Standard 200-1, Version 1.0, Oktober 2017; BSI-Standard 200-2, Version 1.0, Oktober 2017; BSI-Standard 200-3, Version 1.0, Oktober 2017.

62 ÖVE/ÖNORM EN ISO/IEC 27001: 2017 07 01, Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen, 1. Juli 2017.

63 IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels[1.0], August 2013.

64 Center for Internet Security (CIS), CIS Controls V7, 19. März 2018; Center for Internet Security (CIS), The CIS Critical Security for Effective Cyber Defense, Version 6.1, 31. August 2016.

65 National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 16. April 2018.

66 Bundeskanzleramt, Abt. I/8 – Cyber Security / GovCERT / NIS-Büro BMI/II/BVT/5-NIS, NIS Fact Sheet 08/2018, Version 2.0, 29. Oktober 2018, S. 9.

sche Sicherheitsvorkehrungen können auch für einzelne Teilsektoren[67] vorgeschlagen werden.[68] Das Konzept wurde aus der Umsetzung der NIS-Richtlinie in Deutschland übernommen. Zum jetzigen Zeitpunkt wurde vom deutschen BSI die Eignung von branchenspezifischen Sicherheitsstandards (B3S) für die Branchen Wasserversorgung, Abwasserbeseitigung, Lebensmittelhandel, Informationstechnik, und Fernwärme bestätigt; B3S für weitere Sektoren befinden sich in Erstellung bzw. Vorabeignungsprüfung.[69] In Österreich sind derzeit sektorspezifische Sicherheitsstandards in verschiedenen Branchenverbänden in Ausarbeitung, unter anderem in den Sektoren Energie und Trinkwasserlieferung und -versorgung.

Mit sektorspezifischen Sicherheitsstandards können Spezifika der Absicherung von OT und IoT-Lösungen in einem bestimmten Anwendungsgebiet angemessen in der Auslegung des Stands der Technik berücksichtigt werden. Beispielsweise sind im OT-Bereich zur Steuerung industrieller Anlagen häufig bestehende Altsysteme im Einsatz, welche Verwundbarkeiten besitzen, die mit wirtschaftlich angemessenen Mitteln nicht behoben werden können (z.B. eine Altsoftware erfordert eine veraltete Betriebssystemversion, für welche der Hersteller keine Updates mehr bereitstellt).[70] Sicherheitsmaßnahmen orientieren sich an der Bereitstellung kompensierender Maßnahmen, welche nicht die Verwundbarkeit selbst schließen, sondern das Risiko deren Ausnützbarkeit auf anderem Wege reduzieren (z.B. netzwerktechnische Isolierung von Systemen, Härtung der umgebenden Infrastruktur, engmaschige Systemüberwachung, etc.). Sektorspezifische Sicherheitsstandards ermöglichen die explizite Berücksichtigung alternativer Sicherungsmaßnahmen, sodass für eine technische Lösung insgesamt dem Stand der Technik entsprechende Sicherheitsvorkehrungen berücksichtigt werden können.

5. Conclusio

Der Stand der Technik von Netz- und Informationssystem-Sicherheitsmaßnahmen ist ein zunächst unbestimmter und dynamischer Begriff zwischen den anerkannten Regeln der Technik als Untergrenze und dem Stand von Wissenschaft und Technik als Obergrenze. Sowohl auf Unionsebene als auch auf nationaler Ebene werden zahlreiche auf bestehenden sowie anerkannten Normen und Standards der Informationssicherheit basierende Auslegungshilfen erarbeitet, welche die Freiheitsgrade in der Auslegung deutlich eingrenzen. Im Unionsrecht verankertem hohem Gewicht kommen dabei den Leitlinien und Empfehlungen der ENISA zu, welche Sicherheitsfragen in OT und IoT, wie beispielsweise zur Sicherheit in intelligenten Spitälern, Flughäfen und ICS/SCADA Umgebungen, ausführlich beleuchtet hat. Auf nationaler Ebene kommt man dem unionsrechtlichem Auftrag etablierte internationale Informationssicherheitsstandards bei der Auslegung besonders zu berücksichtigen durch die Erstellung eines detaillierten Zuordnungsschlüssels zu einzelnen Normabschnitten anerkannter und gebräuchlicher Normen wie der ISO/IEC 27001[71], dem BSI IT-Grundschutz[72] und den CIS Critical Security Controls[73] nach. Die Definition von sektorspezifischen Sicherheitsstandards bietet insbesondere Raum den Stand der Technik von Sicherheitsvorkehrungen für Netz- und Informationssysteme in (Teil-)Sektoren zu präzisieren, wie beispielsweise für intelligente Verkehrssteuerungssysteme, Smart Meter und Systeme im Kernnetz von Flughäfen.

---

67 Vgl. Anhang II, NIS-Richtlinie (EU) 2016/1148, ABl. L 2016/194, 27.

68 Vgl. Erläuterungen zu § 15 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), 78/ME XXVI. GP, S. 17.

69 Vgl. Deutsches Bundesamt für Sicherheit in der Informationstechnik, Übersicht über Branchenspezifische Sicherheitsstandards (B3S), https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/ITSiG/Was_tun/Stand_der_Technik/B3S_BAKs/B3S_BAKs_node.html (aufgerufen am 3. Jänner 2019).

70 Vgl. Herbert, The Importance of Operational Technology (OT) Systems to Maintain a Secure Standard of Living in Today's Modern Society, https://www.fortinet.com/blog/business-and-technology/the-importance-of-operational-technology-ot-systems-for-a-standard-of-living-in-today-s-modern-society.html (aufgerufen am 21. November 2018), Fortinet, 6. Dezember 2017.

71 ÖVE/ÖNORM EN ISO/IEC 27001: 2017, 1. Juli 2017.

72 BSI-Standard 200-1, Version 1.0, Oktober 2017.

73 CIS Controls V7, 19. März 2018; CIS, Version 6.1, 31. August 2016.

6. Literatur

Bundeskanzleramt, Abt. I/8 – Cyber Security / GovCERT / NIS-Büro BMI/II/BVT/5-NIS, Nationale Umsetzung der NIS-Richtlinie – NIS Fact Sheet 08/2018, Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices, Version 2.0, 29. Oktober 2018.

Deutsches Bundesamt für Sicherheit in der Informationstechnik, Übersicht über Branchenspezifische Sicherheitsstandards (B3S), https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S_BAKs/B3S_BAKs_node.html (aufgerufen am 21. November 2018).

Electricity Information Sharing and Analysis Center (E-ISAC), SANS Industrial Control Systems, Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (aufgerufen am 22. November 2018), 18. März 2016.

Ellmer, Heimo/Schremser, Roman, Der «Stand der Technik» als Kostentreiber?, Sind Stand und Regel der Technik Synonyme?, ZVB 2018, S. 278–285.

European Union Agency for Network and Information Security (ENISA), Towards secure convergence of Cloud and IoT, September 2018.

ENISA, Signalling Security in Telecom SS7/Diameter/ 5G – EU level assessment of the current situation, März 2018.

ENISA, Exploring the opportunities and limitations of current Threat Intelligence Platforms, Public Version 1.0, Dezember 2017.

ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017.

ENISA, Cyber Security Culture in organisations, November 2017.

ENISA, Communication network dependencies for ICS/SCADA Systems, Dezember 2016.

ENISA, Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector, Dezember 2016.

ENISA, Securing Smart Airports, Dezember 2016.

ENISA, Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures, November 2016.

Herbert, Ronald Jules Jr., The Importance of Operational Technology (OT) Systems to Maintain a Secure Standard of Living in Today's Modern Society, https://www.fortinet.com/blog/business-and-technology/the-importance-of-operational-technology-ot-systems-for-a-standard-of-living-in-today-s-modern-society.html (aufgerufen am 21. November 2018), Fortinet, 6. Dezember 2017.

NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, Februar 2018.

Piska, Christian/Erlacher, Eva, Beste verfügbare Techniken – eine neue Größe im Anlagenrecht? ZTR 2014, S. 67–76.

Rechberger, Walter H., Der Sachverständige und die «allgemein anerkannten Regeln der Technik», bauaktuell 2015, S. 15–17.

Seibel, Mark, Abgrenzung der «anerkannten Regeln der Technik» vom «Stand der Technik», NJW 2013, S. 3000–3004.