Eine Übersicht und Vergleich zur NIS-Richtlinie innerhalb der EU mit dem Fokus auf die Betreiber von Kritischen Infrastrukturen

Philipp Schütz[1]

Keywords: NIS-Richtlinie; Vergleich-NIS-Richtlinie; KRITIS-Schutz; KRITIS-Betreiber

1 Einleitung

Das vorliegende extended Abstract fasst auszugsweise die Erkenntnisse der Veröffentlichung [SC19] zum 16. Deutschen IT-Sicherheitskongress beim Bundesamt für Sicherheit in Informationstechnik vom 21. Bis 23. Mai 2019 in Bonn-Bad Godesberg zusammen. Der vollständige Artikel ist zum Kongresstag im Kongressband erschienen.

Die europäische Gesetzgebung hat mit der NIS-Richtlinie als legislativem Rahmen erstmalig dezidierte Informationssicherheitsanforderungen und -ziele zum Schutz von Kritischen Infrastrukturen und deren übergreifende staatlichen Kollaborationsstrukturen verabschiedet.

2 Erkenntnisinteresse und Ziele

Die zentralen sechs Fragestellungen sind:

1. Ist die NIS-RL in nationales Recht umgesetzt, und wenn ja, über welche nationalen Hoheitsakte (Gesetze, Verordnungen, Dekrete und Cyber-Sicherheitsstrategien)?
2. Existieren ausgeprägte KRITIS-Sektoren, Subsektoren und werden Arten von Betreibern genannt (wie bspw. Stromverteilnetzbetreiber, Wasserversorger)?
3. Über welche Mechanismen findet eine Betreiber-Identifikation statt (etwa analog zu Deutschland über öffentlich zugängliche quantitative und qualitative Schwellwerte, wie in den KRITIS-Verordnungen)?
4. Im Falle von gravierenden Störungen: Welche Meldestrukturen existieren und wie ist das Meldewesen ausgeprägt?

[1] Hochschule Niederrhein University of Applied Sciences , Clavis - Kompetenzzentrum für Informationssicherheit, Webschulstraße 41-43, 41065 Mönchengladbach, Deutschland philipp.schuetz@hs-niederrhein.de

doi:10.18420/inf2019_61

5. Welche Standards, Normen und Rahmenwerke werden den Betreibern zur Härtung des informationstechnischen Sicherheitsniveaus empfohlen (z. B. ISO/IEC 27001, erweitert um sektorspezifische Ergänzungen)?
6. Welcher Verbindlichkeitscharakter entsteht durch entsprechende Betreiber-Sicherheitsnachweise (Vorlage eines Zertifikates, Auditierungen oder andere Nachweise)?

3 Erkenntnisse, Fazit und Ausblick

Von den eingangs formulierten sechs Fragestellungen können zum derzeitigen Stand die ersten vier Fragen hinreichend beantwortet werden. Mit Ausnahme von BE und den partiell zeitlichen Verzügen anderer Staaten, haben neun der zehn Staaten durch entsprechende Hoheitsakte die NIS-RL in nationales Recht überführt. Auch weisen die Ausprägungen der KRITIS-Strukturen mit den assoziierten Organisationen und Kontaktpunkten auf eine überwiegend strukturierte Detailierung hin. Die beiden abschließenden Fragestellungen nach konkretisierten Standards, Normen und Rahmenwerken, sowie den exakten Kontrollen und Nachweispflichten, können, nach jetzigem Stand und aus Sicht des Autors nur für DE und GB ausreichend beantwortet werden. Dies könnte, bezogen auf die acht Staaten, auf mindestens drei der folgenden Gründe zurückzuführen sein. Erstens: Die zuständigen Behörden erarbeiten noch entsprechende Branchenstandards und Vorgaben zu Rahmenwerken. Zweitens: Die Informationen sind nicht öffentlich zugänglich oder derzeit intransparent mit den betrachteten Dokumenten zur Umsetzung der NIS-RL verknüpft. Drittens: Die Vorgehensweise durch die Erhebung und Analyse der Primärquellen (Gesetze, Verordnungen und Strategien zur Cybersicherheit) reicht nicht aus, und so muss der Analyse-Radius möglicherweise um existierende Dokumente der jeweiligen Aufsichtsbehörden pro Sektor erweitert werden. Invariant von den im Beitrag geprüften Dimensionen zur Umsetzung der NIS-RL existieren in einigen Staaten Leitfäden, z. B. zum Umgang mit informationstechnischen Risiken. Daher werden dieser Arbeit weitere Untersuchungsaktivitäten folgen. Insbesondere mit dem Ziel, dass ein qualitativer Vergleich der Rahmenwerke für die Betreiber erfolgt und dadurch eine Synthese zu einem international anwendbaren Modell möglich wird. Dazu sollen zukünftig auch Länder außerhalb der Europäischen Union, wie z. B. die Vereinigten Staaten von Amerika und Japan in die Betrachtung einfließen.

Literaturverzeichnis

[SC19] Schütz, P.: Eine Übersicht und Vergleich zur NIS-Richtlinie innerhalb der EU mit dem Fokus auf die Betreiber von Kritischen Infrastrukturen, In: Tagungsband zum 16. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik 2019, SecuMedia Verlag, Gau-Algersheim 2019, S.297-306