AG KRITIS

KRITIS auf EU-Ebene – Teil 2

Bonn, 30.05.2021

Ergänzende Bewertung der NIS 2 Richtlinie in Verbindung mit der RCE Richtlinie unter dem Aspekt der Erhöhung der Versorgungssicherheit und Steigerung der Resilienz kritischer Infrastrukturen

AG KRITIS

Die AG KRITIS ist ein unabhängiger, ehrenamtlicher Zusammenschluss von Expertinnen und Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Die Arbeitsgruppe ist vollständig unabhängig von Staat und Wirtschaft und vertritt keine Interessen von Unternehmen oder Wirtschaftsverbänden.

Inhaltsverzeichnis

Kontext und Historie

> *"Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."*

In Deutschland wird eine Dienstleistung als kritisch betrachtet, wenn ihr Ausfall mindestens 500.000 Menschen betrifft. In anderen (kleineren) Mitgliedsstaaten kann ein sinnvoller Richtwert deutlich davon abweichen. Aus Sicht der EU-Kommission muss die Reichweite der Kritischen Infrastruktur jedoch deutlich größer sein, bzw. mehr als einen Mitgliedsstaat betreffen, damit es in ihren Kompetenzbereich fällt. Bisher gab es dazu zwei einschlägige Direktiven:

Die NIS Direktive (EU 2016/1148) hat die Zielsetzung der Erhöhung der IT-Sicherheit von Netzwerk- und Informationssystemen in der EU und bezieht sich insbesondere auf relevante Sektoren wie Energie, Gesundheit oder Wasserversorgung. Wesentliche Forderungen an jeden Mitgliedsstaat sind:

- Erstellung einer nationalen Cybersicherheitsstrategie
- Benennung einer nationalen zuständigen Behörde
- Einrichtung von Notfallkontakten in der Behörde und den Kritischen Infrastrukturen zur Meldung von Vorfällen und ggf. staatenübergreifende Weitergabe von Warnungen

Zudem gibt es die bereits ältere ECI Direktive (2008/116/EC), welche sich losgelöst von IT-Risiken mit der Identifikation und dem Schutz von Europäischen Kritischen Infrastrukturen (mehr als einen Staat betreffend) beschäftigt. Damals beschränkte man sich aber noch allein auf die Sektoren Energie und Transport. Die Direktive enthält diese wesentlichen Bestandteile:

- Sehr ausführliche Beschreibung wie Staaten bilateral oder multilateral verhandeln können, ob ansässige Unternehmen kritische Dienstleistungen erbringen, und wann die Kommission unter Wahrung der Anonymität der potenziellen Kritischen Infrastruktur mediativ eingebunden werden kann, um die Benennung als Kritische Infrastruktur festzustellen.

- Forderung direkt an den notifizierten Betreiber zur Erstellung eines Betriebssicherheitsplans (Identifikation kritischer Komponenten, Risikoanalyse, Definition geeigneter Maßnahmen).
- Forderung an die Staaten, die Umsetzung der Pläne sicherzustellen und regelmäßig an die Kommission zu berichten.

Aktuelle Entwicklungen

Wegen dieses Zweiklangs von NIS und ECI entstehen daher auch wieder zwei Direktiven, die nur zusammen betrachtet werden können. Während NIS treffend durch NIS 2 leicht aktualisiert wird, wird die ECI durch eine neue RCE Direktive (Resilience of Critical Entities) mit komplett überarbeiteter Struktur und erweitertem Umfang ersetzt.

Zu beiden Entwürfen sind inzwischen Kommentare anderer EU Ausschüsse eingegangen, die im folgenden mit berücksichtigt werden.

Dieser Artikel ergänzt unsere Bewertung vom April 2021 [1].

Ergänzende Bewertung der aktuellen Entwürfe

Strikt defensive Cybersicherheitsstrategie für Staat und Wirtschaft

Der Schutz der zivilen Bevölkerung und der dazu gehörigen Kritischen Infrastrukturen kann nur mit einer strikt defensiven Cybersicherheitsstrategie für Staat und Wirtschaft erreicht werden. Diesen Punkt hatten wir zwar schon mehrfach angebracht, allerdings zwingen uns die aktuellen Kommentierungen der Regulierungsentwürfe nochmals darauf einzugehen.

Systeme militärischer Einrichtungen sind im Cyberraum nicht von Kritischen Infrastrukturen zu unterscheiden. Zum einen ist eine Tarnung als Kritische Infrastruktur sehr leicht, und zum anderen ist es sogar denkbar, dass kompromittierte KRITIS-Systeme durch einen Angreifer als Operationsbasis für weitere Angriffe genutzt werden. Der Einsatz offensiver Wirkmittel gegen diese Systeme würde also den Angriff nicht dauerhaft und wirksam unterbinden, jedoch die Kritische Infrastruktur treffen. Dabei ist es unerheblich, ob diese Infrastruktur in einem gegnerischen Staat, einem neutralen Staat oder einem verbündeten Staat seht. Da zivile Infrastruktur anvisiert und getroffen wird, steht dies im klaren Widerspruch zu den Zusatzprotokollen der Genfer Konvention von 1977.

Die Feststellung des Ausschusses für auswärtige Angelegenheiten des EU Parlaments in seiner Entwurfskommentierungen, dass ziviles und militärisches im Cyberraum eng zusammen liegen

und Werkzeuge sehr wahrscheinlich einer Doppelverwendungsfähigkeit (engl. Dual-Use) unterliegen, unterstreicht eigentlich nur das Bedürfnis einer strikt defensiven Strategie – unabhängig von jeglichen militärischen Organisationen oder Geheimdiensten. Daher fordern wird nochmal nachdrücklich:

- Die Unabhängigkeit der National Competent Authorities (NCA)
- Verpflichtende „responsible disclosure“ von Sicherheitslücken

Rüstungsindustrie ist nicht KRITIS

Der Schutz ziviler Infrastrukturen darf nicht in einer Regulierung mit dem Schutz militärnaher Industrie vermengt werden. Die nationalen Sicherheitsinteressen und die der EU-Staatengemeinschaft müssen in speziell dafür vorgesehenen Regulierungen und Direktiven adressiert werden.

Es ist daher nicht nachvollziehbar, warum in der Direktive für Resilient Critical Entities bei der Identifizierung der Kritischen Infrastrukturen (engl. critical entities) auf Methodologien der Common Security and Defence Policy (CSDP) (vgl. AFET Draft Opinion RCE [3] - Amendment 4) verwiesen werden soll. Auch ist bei Fragen des Zivilschutzes nicht nachvollziehbar, warum eine enge Kooperation mit der NATO und der OSCE (vgl. AFET Draft Opinion RCE [3] - Amendment 5) angestrebt werden soll.

Dieses vermengte Vorgehen ist strukturell nicht zielführend. Unter Hinzunahme der Methoden zur Bedrohungsanalysen aus dem CSDP kann ein Staat zwar Unternehmen, die unter anderem auch in militärischen Lieferketten eingebettet sind, als Kritische Infrastruktur identifizieren. Diese Unternehmen sind aber mit unzureichend ausgestalteten Handlungsvorgaben aus der zivilen Regulierung konfrontiert, welche der Kritikalität der Bedrohung nicht gerecht werden.

Kryptographie vs. Lawful Interception

Die NIS 2 Direktive formuliert in ihren Artikeln keine explizite Anforderung für „Lawful Interception“ von Ende-zu-Ende-verschlüsselter Kommunikation. Im Kontext der Argumentation in der Präambel Absatz (54) und der Cybersecurity Strategie der EU (2020-12-16) Abschnitt 2.2 „Tackling Cybercrime“ ist diese Forderung aber grundsätzlich angelegt (vgl. Kipker). Bestrebungen zur Einschränkung der Nutzung oder Verbreitung kryptographischer Verfahren gab es in den letzten Jahrzehnten immer wieder. Diese haben sich allesamt als nutzlos bzw. sogar nachteilig herausgestellt, wie es die ENISA bereits 2016 im Bericht „On the free use of cryptographic tools for (self) protection of EU citizens“ [8] dargelegt hat. Daher sollte der letzte Satz aus Absatz (54) der Präambel des NIS 2 Entwurfs gestrichen werden.

Article 2 – Definitions (23) – Public Administration

Mit „Public Administration“ meint die NIS 2 Direktive alle öffentlichen Verwaltungen, welche dem NUTS (Nomenclature of Territorial Units for Statistics) Level 1 oder 2 zuzuordnen sind. Aus der Direktive 1059/2003 ergibt sich somit ein Schwellwert von 800.000 Einwohnern und erfasst in Deutschland zum Beispiel die Regierung Oberpfalz oder die Region Düsseldorf. Der Ausschluss von „public security, law enforcement, defense and national security“ ist aus unserer Sicht aber im Sinne einer strikten defensiven Cybersicherheitsstrategie gerechtfertigt und nicht als KRITIS einzustufen.

Unsinnige Forderung nach Angriffserkennungssystemen

Konkrete Maßnahmen zur Absicherung ergeben sich immer aus einer Risikoanalyse im Rahmen eines umgesetzten ISMS. Die konkrete Nennung automatisierter Angriffserkennungs- und Angriffsbehandlungssysteme (vgl. „active cyber defense programme … real-time capability to discover, detect, analyse and mitigate threats“ – AFET Draft Opinion NIS [2]) im Text der Direktive räumt dieser Maßnahme eine unreflektierte Priorität ein. Die dafür aufgewendeten Ressourcen fehlen dann aber wahrscheinlich für andere Maßnahmen, welche nach einer Risikoanalyse als wichtiger und zielführender erachtet würden. Technische Maßnahmen haben in einer Vorgabe wie der NIS 2 Direktive nichts verloren.

Meldefristen für Vorfälle

Es wird von mehreren Seiten vorgeschlagen, die initiale Meldefrist für signifikante Vorfälle von 24 auf 72 Stunden zu erhöhen (ITRE Draft Opinion NIS [4] - Amendment 61 und IMCO Draft Opinion NIS [6] – Amendment 56). Als ein Grund wird eine Angleichung an die GDPR genannt. Allerdings sind die zu meldenden Vorfälle gemäß GDPR und NIS-2 von völlig unterschiedlicher Natur. Artikel 20 4 (a) des NIS 2 Entwurfs beschreibt nur die initiale Meldung von Sicherheitsvorfällen, wenn ein signifikanter Schaden bereits eingetreten ist oder unmittelbar bevorsteht. Der Sinn einer initialen Meldung ohne weitere Details besteht aber gerade in der rechtzeitigen Warnung anderer Kritischer Infrastrukturen, so dass weitere gleichgelagerte Vorfälle verhindert oder abgemildert werden können. Die Stärkung des CSIRT-Netzwerkes und die Einführung des EU CyCLONe (Cyber Crises Liaison Organisation Network) unterstreichen genau dieses Bestreben. Angesichts der Schnelligkeit, in der Angreifer Schwachstellen auf breiter Front ausnutzen können, würde eine Frist von 72 Stunden den Zweck verfehlen.

Als weiterer Grund wird angeführt, dass eine Meldepflicht von der Bewältigung eines Vorfalls ablenkt. Der Aufwand einer bewusst inhaltsarmen Benachrichtigung an eine fest benannte nationale Stelle sollte jedoch sehr überschaubar sein. Zudem ermöglicht nur eine schnelle Meldung auch Unterstützung und Koordination in Großschadenslagen. Wie das Beispiel der Colonial Pipeline aus der jüngsten Vergangenheit zeigt, ist eine Bewältigung signifikanter Vorfälle ohne externe Unterstützung evtl. nicht möglich.

Entweder KRITIS oder nicht, aber kein KRITIS-light

Die Einführung von „important entities“ zusätzlich zu den „essential entities“ ähnelt der im deutschen IT-SiG 2.0 eingeführten Kategorie der „Unternehmen im besonderen öffentlichen Interesse“. Der Sinn und Nutzen dieser Differenzierung ist – wie im IT-SiG 2.0 – fragwürdig. Ohne nachvollziehbare Kriterien, warum ein Sektor bzw. eine Organisation als „essential“ oder als „important“ eingestuft wird, erscheint die Zuordnung willkürlich. Insbesondere ist nicht nachvollziehbar, warum der Sektor Ernährung in Deutschland als KRITIS behandelt wird, im NIS 2 Entwurf aber nur als „important entity“ eingestuft wird. Entweder Infrastrukturen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens und ihr Ausfall führt zu erheblichen Versorgungsengpässen oder zu Gefährdungen für die öffentliche Sicherheit, oder sie sind eben nicht Kritische Infrastruktur (KRITIS).

Wir unterstützen bestimmte Änderungsvorschläge

Manche Änderungsvorschläge geben wichtige und positive Impulse, die wir unterstützen.

[AFET Draft Opinion NIS [2] - Amendment 6 & 8; AFET Draft Opinion RCE [3] - Amendment 2 & 3] Hier werden Krisen, welche den europäischen Markt (engl. internal market) betreffen, konsequent mit der Sicherheit der Bürger (engl. security and safety of citizens) ergänzt. Das rückt aus unserer Sicht den Fokus an die richtige Stelle, da Versorgungssicherheit der Bevölkerung das zentrale Interesse darstellen sollte.

[AFET Draft Opinion NIS [2] - Amendment 15] Hier wird eingebracht, dass die Förderung von Nutzung und Entwicklung von Open Source Einzug in die Nationale Cybersecurity Strategie finden soll.

[AFET Draft Opinion NIS [2] - Amendment 16] Der Änderungsvorschlag zur „mandatory responsible disclosure“ ist ein wesentlicher Beitrag zur Absicherung von Produkten, welche in Kritischen Infrastrukturen eingesetzt werden (vgl. unsere Bewertung der EU-NIS und EU-RCE Richtlinie).

Zusammenfassung

Die neuen Entwürfe sind ein Schritt in die richtige Richtung und beinhalten relevante Klarstellungen, insbesondere was die europäische Zusammenarbeit angeht. Auf der technischen Arbeitsebene und dem konkreten Schutz von Kritischen Infrastrukturen, sowie der Vorbereitung auf Großschadenslagen sehen wir allerdings noch deutliches Potenzial, welches hier noch nicht ausgeschöpft wird. Bei einem so umfangreichen Gesetzgebungsvorhaben halten wir es für notwendig, dass folgende wesentlichen Punkte ihren Weg in die finalen Direktiven finden:

- Strikt defensive Cybersicherheitsstrategie für Staat und Wirtschaft
- Unabhängigkeit der National Competent Authorities (NCA)
- Gesetzlich verpflichtendes Patchmanagement im KRITIS-Umfeld
- Open-Source Einsatz im KRITIS-Umfeld
- Gründung nationaler Cyber-Hilfswerke und harmonisierte europäische Koordination von Cyber-Hilfswerken
- Verpflichtende und defensive Responsible Disclosure von Sicherheitslücken
- Keine Hintertüren für „Lawful Interception“ ermöglichen
- Keine Verpflichtung auf spezifische Schutzmaßnahmen sondern risikobasierte Konzepte
- Meldefristen müssen dem Zweck angemessen bleiben

Abgrenzung

Die AG KRITIS arbeitet vollständig unabhängig von wirtschaftlichen Interessen und vollständig im Ehrenamt. Leider ist es uns daher nicht möglich, jeden Aspekt der NIS-Richtlinie abschließend zu bewerten.

Referenzen

[1] AG KRITIS, KRITIS auf EU-Ebene, https://ag.kritis.info/2021/04/26/bewertung-der-eu-nis-und-eu-rci-richtlinie/

[2] AFET DRAFT OPINION on the proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, https://www.europarl.europa.eu/doceo/document/AFET-PA-691371_EN.pdf

[3] AFET DRAFT OPINION on the proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, https://www.europarl.europa.eu/doceo/document/AFET-PA-692863_EN.pdf

[4] ITRE DRAFT REPORT on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, https://www.europarl.europa.eu/doceo/document/ITRE-PR-692602_EN.pdf

[5] ITRE DRAFT OPINION on the proposal for a directive of the European Parliament and of the Council on the resilience of critical entities, https://www.europarl.europa.eu/doceo/document/ITRE-PA-692663_EN.pdf

[6] IMCO DRAFT OPINION on the proposal for a directive of the European Parliament and of the Council on Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, https://www.europarl.europa.eu/doceo/document/IMCO-PA-691156_EN.pdf

[7] IMCO DRAFT OPINION on the proposal for a directive of the European Parliament and of the Council on the resilience of critical entities, https://www.europarl.europa.eu/doceo/document/IMCO-PA-691165_EN.pdf

[8] ENISA, On the free use of cryptographic tools for (self) protection of EU citizens, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto