AG KRITIS

KRITIS auf EU-Ebene

Bonn, 25.04.2021

Bewertung der NIS-Richtline in Verbindung mit der RCI-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.

Wie bereits von Kipker et al. (https://intrapol.org/2021/03/12/mmr-3-2021-nis-richtlinie-und-der-entwurf-der-nis-2-richtlinie/) ausführlich erarbeitet, hat die staatenübergreifende Zusammenarbeit im NIS 2 Entwurf einen sehr hohen Stellenwert. Die Computer Security Incident Response Teams (CSIRTs) sollen enger zusammenarbeiten, voneinander auch Unterstützung und Informationen anfordern können und auch in ihrem Hoheitsbereich ein breiteres Spektrum an Aufgaben übernehmen. Mit dem European Cyber Crises Liaison Organisation Network (EU-CyCLONe) entsteht zudem eine weitere Stelle zur Koordination und Bewältigung von IT-bedingten Großschadenslagen, für die auch nationale Krisenreaktionspläne vorbereitet werden müssen. Insgesamt sind die ENISA und die EU-Kommission aktiver und fordern tiefergehende Berichte. Die zweite inkrementelle Veränderung der NIS 2 Direktive liegt in der Definition der Sektoren, die entweder verbreitert (z. B. gehören zum Sektor Energie dann auch Stromhändler, Fernwärme und Wasserstoff) oder komplett neu hinzugefügt werden (z .B. Abwasser und Weltraum). Nachrangig aber dennoch bemerkenswert ist das klare Bekenntnis zu einem Europa-weit koordinierten Schwachstellenmanagement. Dabei soll ENISA eine gemeinsame Schwachstellendatenbank betreiben und die nationalen CSIRTs den Austausch der Schwachstellen-Informationen insbesondere auch mit den Herstellern von Informationstechnologien koordinieren. Es werden auf EU-Ebene dabei keine Anforderungen an Betreiber und Hersteller, sondern an Behörden und Regulierer gestellt.

Die RCE Direktive soll sich aber direkt mit der Resilienz kritischer Dienstleistungen befassen. Nach dem Vorbild der NIS Direktive werden Staaten nun aufgefordert, eine Strategie für das Erreichen einer starken Resilienz aller Kritischen Infrastrukturen auf ihrem Hoheitsgebiet zu erarbeiten. Dazu müssen die Staaten eine Risikoanalyse durchführen und strukturiert nach potenziellen Kritischen Infrastrukturen durchsuchen. Die Liste kritischer Sektoren ist nun mit der NIS 2 Direktive harmonisiert und ggü. der bisherigen ECI Direktive deutlich erweitert. Die EU-Kommission fordert zusätzlich 39 Monate nach Inkrafttreten einen Bericht über Art und

Zahl der identifizierten Infrastrukturen, sowie auch die individuell gewählten Richtwerte, auf denen die Auswahl basiert. Es müssen nationale zuständige Behörden benannt werden, welche nach innen und außen als zentrale Anlaufstelle fungieren und den Kritischen Infrastrukturen aber auch aktiv Unterstützung in Form von Methodologien, Schulungen, Übungen und Austausch innerhalb der Sektoren zukommen lassen.

Ein Kernpunkt sind die Anforderungen (Artikel 10-13), welche sich direkt an die Betreiber Kritischer Infrastrukturen wenden. So werden Risikoanalysen und davon abgeleitete Maßnahmenkataloge eingefordert, welche einer Unterbrechung der Versorgungssicherheit wirksam entgegenwirken. Störungen müssen vom Betreiber unverzüglich gemeldet und von der zentralen Anlaufstelle ggf. mit anderen betroffenen Staaten geteilt werden. Ferner müssen Betreiber bei Hintergrundüberprüfungen von Mitarbeitern unterstützt werden.

Weitere Neuerungen gibt es im Bezug auf Kritische Infrastrukturen von besonderer EU-weiter Bedeutung (Artikel 14-16). Die ehemaligen Verhandlungs- und Mediationsrunden zur Feststellung dieses Status werden nun ersetzt. Wenn mehr als ein Drittel der Mitgliedsstaaten in ihrer Risikoanalyse und Meldung eine bestimmte kritische Infrastruktur als solche identifiziert haben, wird sie von der Kommission als von besonderer EU-weiter Bedeutung benannt. Mit der Critical Entities Resilience Group entsteht nun ein dedizierte Steuerungsgruppe für die grenzüberschreitenden Risiken.

Die nationale Zuständigkeit der lokalen Behörden bleibt für ansässige Betreiber bestehen, jetzt werden aber genauere Anforderungen formuliert, welche von der Behörde erfüllt werden müssen. So wird erwartet, dass Audits und Betriebsbegehungen durchgeführt und Anordnungen ausgesprochen werden, um die Einhaltung der Vorgaben zu erreichen (Artikel 18-3). Dem soll insbesondere auch mit Bußgeldern Nachdruck verliehen werden (Artikel 19).

Bewertung der aktuellen Entwürfe

Vorstöße zur Verbesserung der Versorgungssicherheit und insbesondere die Aktualisierung teils veralteter Direktiven sind zu begrüßen. Leider vermissen wir auch auf EU-Ebene noch die Umsetzung zentraler Forderungen:

- Wir brauchen eine strikt defensive Cybersicherheitsstrategie. Wir verurteilen den Einsatz und die Bereitstellung offensiver Wirkmittel im Cyberraum. Insbesondere Kritische Infrastrukturen sind anfällig für Angriffe von Cyber-Kriminellen oder von Drittstaaten – egal ob feindlich gesinnt oder „Freunde“. Da eine zweifelsfreie Zuordnung der Herkunft eines Cyberangriffs nach dem Stand der Technik ausgeschlossen ist, muss davon ausgegangen werden, dass sowohl ein Angriff als auch ein Gegenangriff immer auch zivile Infrastruktur treffen kann. Dies ist laut den Zusatzprotokollen der Genfer Konvention von 1977 klar ausgeschlossen, vgl. Art. 52 und 14 ZP II und 54 ZP I. Auch die

deutlich ältere Haager Landkriegsordnung untersagt in Art. 25, 27, und 56 Angriffe auf zivile Infrastruktur im weiteren Sinne.

- Wir brauchen die Unabhängigkeit der National Competent Authorities (NCA) von verdeckten Sicherheitsinteressen - die NCAs müssen in die rechtliche Lage versetzt werden, Sicherheitslücken auch entgegen der Interessen von Sicherheitsbehörden umgehend schließen zu lassen, um das IT-Sicherheitsniveau in der gesamten EU nachhaltig zu erhöhen.
- Wir brauchen ein gesetzlich verpflichtendes Patchmanagement im KRITIS-Umfeld, dies ist für einen sicheren Betrieb alternativlos. Hersteller müssen verpflichtet werden können, auf Weisung einer NCA, notfalls bußgeldbewehrt, Patches für bekannt gewordene Sicherheitslücken in Kernkomponenten kritischer Infrastruktur zu entwickeln. KRITIS-Betreiber müssen Aktualisierungen und Softwareverteilung auf Integrität und Herkunft prüfen. KRITIS-Betreiber müssen auch binnen einer vorgegebenen Frist Empfehlungen und Mindeststandards der NCA umsetzen.
- Wir brauchen im KRITIS-Umfeld Software, welche grundsätzlich quelloffen gestaltet sein sollte. Dort wo dies nicht möglich ist, sollen Quellcode und Build-Chain zumindest in treuhänderischer Verwaltung aufbewahrt werden. Dies sorgt dafür, dass ein Patch zur Behebung einer kritischen Sicherheitslücke auch dann noch erstellt werden kann, wenn der ursprüngliche Hersteller nicht mehr existiert oder eine Fehlerbehebung durch den Hersteller unwahrscheinlich
- Wir brauchen die Gründung nationaler Cyber-Hilfswerke und harmonisierte europäische Koordination von Cyber-Hilfswerken. Diese sind ein wesentlicher Pfeiler in der Bewältigung von Cyber-Großschadenslagen im KRITIS-Umfeld. Zivile Helfer und Spezialisten verschiedenen Fachbereiche können so gebündelt den Auswirkungen von Ausfällen oder Einschränkungen der Kritischen Infrastruktur bzw. ihrer kritischen Versorgungsdienstleistung entgegenwirken.

Es gibt aber auch Lichtblicke, die eine Verbesserung versprechen. Die einzelnen Maßnahmen wirken dabei allerdings oftmals nicht weitreichend genug oder die Implementierung wird sich noch bewähren müssen.

Europäische Kooperation

Bereits die ursprüngliche NIS Direktive von 2016 beinhaltete die Schaffung einer europäischen Koordinationsgruppe und eine Vernetzung der nationalen Computer Security Incident Response Teams (CSIRTs). Diese Kooperation wird mit dem NIS2 Entwurf dahingehend erweitert, dass jeder Mitgliedsstaat auch eine Behörde für die Bewältigung von Großschadenslagen zu benennen hat und einen nationalen Krisenreaktionsplan vorlegen soll.

Zudem wird in Artikel 6 des NIS2 Entwurfs ein Europa-weit koordiniertes Schwachstellenmanagement vorgesehen. Dabei soll ENISA eine gemeinsame Schwachstellendatenbank betreiben und die nationalen CSIRTs den Austausch der Schwachstellen-Informationen koordinieren.

Darüber hinaus adressiert der neu geschaffene Artikel 26 teilweise den von uns geforderten defensiven Informationsaustausch über Cybersicherheitsprobleme. Obwohl ENISA und nationale Behörden bzw. CSIRTs den Informationsaustausch zwischen Betreibern Kritischer Infrastrukturen fördern sollen, ist die konkrete Teilnahme der europäischen und nationalen Behörden leider nicht verbindlich festgeschrieben. Eine Einbindung von Forschungsinstituten bzw. wissenschaftlichen Institutionen wird gar nicht erst erwähnt.

EU-CyCLONe

Artikel 14 der NIS2 Richtlinie erklärt das europäische System EU-CyCLONe - (European Cyber Crises Liaison Organisation Network). Europäische Festlegungen über Incident- und Krisen-Response begrüßen wir, daher ist Artikel 14 ein Schritt in die richtige Richtung. Wir empfehlen allerdings, hier den Mitgliedsstaaten eine weitere Pflicht aufzuerlegen, nämlich neben den staatlichen "crisis management authorities" auch eine zivilgesellschaftliche und ehrenamtliche Organisation zur Unterstützung der crisis management authorities aufzubauen. Dies würde dafür sorgen, das in ganz Europa Organisationen ähnlich unseres CHW-Konzepts entstehen würden.

Staatliche Verantwortung und Aufsicht (von kritischen Infrastrukturen) sicherstellen

Unsere politische Forderung "Staatliche Verantwortung und Aufsicht (von kritischen Infrastrukturen) sicherstellen" sehen wir mit den Artikeln 18 und 19 der RCE Direktive als erfüllt. Wenn diese in der vorliegenden Form verabschiedet werden, wird sich die Gesamtsituation verbessern.

Angemessene Personalausstattung relevanter Behörden

Weiterhin fordern wir eine "angemessene Personalausstattung relevanter Behörden". Sowohl an mehreren Stellen in der NIS2 Richtlinie (Artikel 8 und 9), als auch in Artikel 8 Absatz 4 der RCE Direktive finden sich dort Formulierungen, die von "englisch: adequate ressources" sprechen - wenngleich dies wortgleich unserer Forderung entspricht, wird sich zeigen, ob eine so vage Formulierung das gewünschte Ziel wirklich erreicht. Wir haben es als vorsichtig positiv bewertet, dass die "adequate ressources" im NIS2 Entwurf an vielen verschiedenen Stellen für jeweils konkrete einzelne Elemente der staatlichen Cybersicherheitsstrategie gefordert werden.

Responsible Disclosure

Unsere politische Forderung nach verpflichtender "responsible disclosure" von Sicherheitslücken sehen wir nicht als erfüllt an. Es finden sich zwar im Artikel 6 der NIS2 Richtlinie konkrete Aussagen zum Umgang mit Sicherheitslücken, allerdings stehen diese in einem "coordinated disclosure" Kontext - diese Formulierung schließt die Implementierung eines sogenannten VEP nicht aus. VEP steht für Vulnerabilities Equities Process (siehe z. B. https://en.wikipedia.org/wiki/Vulnerabilities_Equities_Process). Dabei wird jede gemeldete Sicherheitslücke erst von Behörden geprüft und darüber entschieden, ob diese dem Hersteller gemeldet wird oder für die Ausnutzung durch Sicherheitsbehörden zurückgehalten wird. Ein solcher Prozess ist mit dem europäischen Verständnis von Bürgerrechten und IT-Sicherheit im Allgemeinen nicht vereinbar. Daher ist an dieser Stelle wesentlich, dass die NIS2 Richtlinie einen VEP konkret ausschließt.

Gleichzeitig erkennen wir aber an, dass EU-Direktiven keine Aspekte der nationaler Sicherheit der Mitgliedsstaaten regeln können. Und da solche Sicherheitslücken unter Umständen auch die Forschungsgrundlage für offensive Cyberwaffen sein können, fallen gemeldete Sicherheitslücken zumindest aus Sicht der Sicherheitsbehörden unter Umständen in den Bereich der nationalen Sicherheit.

Im Sinne unserer Forderung nach einer strikt defensiven Cybersicherheitsstrategie ist es notwendig, den Umgang mit Sicherheitslücken verbindlich zu regeln. Möglich wäre hier aber ein internationales Abkommen anzustreben, dass den Umgang mit Digitalwaffen vergleichbar zu ABC-Waffen-Abkommen regelt. Es erscheint zumindest zielführender, als diesen Aspekt unter den schwierigen europarechtlichen Rahmenbedingungen in der NIS2 Richtlinie zu regeln.

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

Abgrenzung

Die AG KRITIS arbeitet vollständig unabhängig von wirtschaftlichen Interessen und vollständig im Ehrenamt. Leider ist es uns nicht gelungen, jeden Aspekt der NIS-Richtlinie abschließend zu bewerten. Folgende Punkte wurden von uns noch nicht vertiefend betrachtet oder bewertet und flossen daher nicht in diese Bewertung ein:

- Unternehmen in besonderem öffentlichen Interesse – quasi eine Art KRITIS-light für bestimmte Unternehmen – hier finden sich Regelungen im Annex I und II der NIS-Richtlinie
- Die Zuordnung von Diensten und Dienstleistungen zu den „essential“ oder „important“ services
- Der Umgang mit dem DNS-System
- Ob und wenn ja in welchem Umfang Medizingerätehersteller zukünftig von KRITIS- oder KRITIS-ähnlichen Aufgaben betroffen sein werden.

Wir haben vor, diese noch unbearbeiteten Punkte in zukünftigen Bewertungen zu vertiefen.