STORMSHIELD

MEINUNGEN

EU-RICHTLINIE NIS2: WAS ÄNDERT SICH?

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Die NIS-Richtlinie wurde im Juli 2016 von den EU-Institutionen verabschiedet und soll ein bestimmtes Sicherheitsniveau für Netzwerke und Informationssysteme kritischer und sensibler Infrastrukturen in den Mitgliedsländern der Europäischen Union gewährleisten. Sechs Jahre später wird die Überarbeitung dieser Richtlinie beschleunigt, wobei die ersten Vereinbarungen zwischen der Kommission, dem Parlament und dem Europäischen Rat im Mai und Juni 2022 getroffen werden sollen. Die neue NIS2-Richtlinie ist noch nicht verabschiedet und wirft bereits viele Fragen zu ihren Auswirkungen und ihrem Geltungsbereich auf. Hier einige Erklärungen.

EINE ERWEITERUNG DER BETEILIGTEN AKTEURE

Die Zunahme von Cyberangriffen in den letzten Jahren zwingt die EU-Mitgliedstaaten, ihr Sicherheitsniveau zu erhöhen, um Bürger, Gebietskörperschaften und Unternehmen zu schützen. Um dieser Herausforderung zu begegnen, wird die NIS-Richtlinie in einer Version 2.0 reformiert, harmonisiert und gestärkt. Laut **Thierry Breton**, EU-Kommissar für Binnenhandel, soll diese Reform *„mehr Sicherheit auf dem Gebiet der für die Gesellschaft und die Wirtschaft kritischen Dienstleistungen bieten"*. Und es ermöglichen, *„die Regeln zu modernisieren"*.

Die erste Stufe der Harmonisierung wird sich in einer genaueren Definition der betroffenen Sektoren niederschlagen. Und so kommt eine erste Frage auf: **Fällt mein Unternehmen unter die NIS2-Richtlinie? Im Amtsblatt der Europäischen Union ist vermerkt, dass es insgesamt 18 betroffene Sektoren gibt, die in kritische Sektoren und Sektoren mit hoher Kritikalität unterteilt werden.** Es gibt 11 Sektoren mit hoher Kritikalität: Energie (Strom, Fernwärme und -kälte, Erdöl, Gas, Wasserstoff), Verkehr (Luft-, Schienen-, Wasser-, Straßentransport), Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Unter die kritischen Sektoren fallen 9: Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, verarbeitendes Gewerbe/Herstellung von Waren (Herstellung von Medizinprodukten, von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, von elektrischen Ausrüstungen, von Maschinen, von Kraftwagen und Kraftwagenteilen und sonstiger Fahrzeugbau), Anbieter digitaler Dienste und Forschung. Für eine noch genauere Beschreibung wird in der europäischen Richtlinie eine Liste von Einrichtungen aufgeführt, die Tätigkeitsfeldern entspricht. Zudem ist bei der NIS2-Richtlinie die Größe der Einrichtung zu berücksichtigen, da die Anzahl der Mitarbeiter (mindestens 50) oder der Umsatz (oder Bilanz, mindestens 10 Millionen Euro) ebenfalls als Auswahlkriterium gelten.

Diese Liste ist nicht erschöpfend und bestimmte Details sind im Rahmen der nationalen Umsetzungen noch zu definieren, beispielsweise zur einzelnen Einbeziehung oder zum einzelnen Ausschluss von Einrichtungen (nach einer nationalen Risikoanalyse oder einer nationalen Verteidigungs- oder Sicherheitsklausel. Für Frankreich erklärte **Guillaume Poupard,** ehemaliger Generaldirektor der ANSSI, im Juni 2022, dass die NIS2-Richtlinie ihren Aktionsradius erheblich erweitern werde, was *„eine zehnfache Zunahme der Anzahl der als Betreiber von Grundversorgungsdiensten (OSE) eingestuften Akteure"* bedeuten würde. Bisher gibt es keine offiziellen Zahlen über die Anzahl der betroffenen Unternehmen, aber erste offizielle Mitteilungen der ANSSI gehen davon aus, dass bis zu mehreren tausend französische Organisationen von der NIS2-Richtlinie betroffen sind. **Und für eine bessere Anpassung der Verordnung an die Besonderheiten jedes Sektors arbeitet die ANSSI mit den Berufs- und Branchenverbänden (Gewerkschaften usw.) zusammen.** Anfang 2023 wurden bereits erste Konsultationen durchgeführt.

Mit dem Sektor der öffentlichen Verwaltung werden also auch die lokalen und regionalen Gebietskörperschaften in diese Reform einbezogen. Laut einem Interview mit **Yves Verhoeven**, dem stellvertretenden Direktor für Strategie bei ANSSI, für die Zeitung La *Tribune*: „*Das überarbeitete NIS bietet die Möglichkeit, die lokalen und regionalen Gebietskörperschaften zu regulieren und ihnen Regeln für die Cybersicherheit aufzuerlegen*". Wie zuvor erklärt, hat jeder Mitgliedstaat es in der Hand, den Geltungsbereich der neuen Richtlinie auf seine Kommunalverwaltungen auszuweiten oder nicht.

In der ersten Version vergessen, werden nun auch die Akteure der Lieferkette (Subunternehmer und Dienstleister), die Zugang zu einer kritischen Infrastruktur haben, der NIS2-Richtlinie unterworfen. Denn Schwachstellen in der Infrastruktur eines Anbieters konnten die Sicherheit der OSE für die er arbeitet, in Frage stellen. Der Cyberangriff, der im Juli 2021 das Unternehmen Kaseya traf, ist ein trauriges und berühmtes Beispiel für solche *Supply-Chain-Attacken.* Sobald NIS 2 angewendet wird, wird die Realität vor Ort ganz anders aussehen. Beispielsweise werden im Energiesektor nicht mehr nur Stromerzeuger, -transporteure und -verteiler zu Sicherheitsmaßnahmen verpflichtet. Alle Zulieferer für kritische Infrastrukturen werden ebenfalls einbezogen .Dienstleistungsunternehmen und andere NSE werden insbesondere verpflichtet sein, jeden Sicherheitsvorfall innerhalb von 72 Stunden zu melden, um die Ausbreitung des Angriffs einzudämmen.

So ist zu erwarten, dass kleine und mittlere Unternehmen schnell ein CISO-Profil einstellen werden, um den Sicherheitsanforderungen gerecht zu werden und weiterhin bei Großunternehmen tätig zu sein. Dies führt zu einer zusätzlichen Anspannung auf einem Arbeitsmarkt, der bereits an seinem Wendepunkt zu stehen scheint ...

NIS2, AUF DEM WEG ZUM ENDE DER OSE

Definitionspunkt, bevor wir über deren Ende sprechen: **Was ist ein OSE?** Gedacht als eine Erweiterung des Status von OIV der in Frankreich durch das Militärprogrammgesetz von 2013 eingeführt wurde, ist ein OSE ein Betreiber von Grundversorgungsdiensten, dessen Ausfall des IT-Systems oder seiner Infrastruktur erhebliche Auswirkungen auf das Funktionieren der französischen Wirtschaft oder Gesellschaft hätte.

Doch mit der Einbeziehung von Subunternehmern und Dienstleistern, die für eine kritische Infrastruktur und vor allem eine semantische Bewegung verantwortlich sind, **signalisiert die NIS2-Richtlinie das Ende der OSE. Von nun an wird der Umfang dieser regulierten Betreiber in zwei Typologien von Akteuren unterteilt: wesentliche Einheiten (EE) und wichtige Einheiten (EI), die nach der Kritikalität der damit verbundenen Sektoren unterschieden werden.** Die NIS2-Richtlinie bezieht hier eine Proportionalität zwischen den Einrichtungen auf Ebene der Sicherheitsmaßnahmen, der Regulierung sowie auch der Sanktionen ein. Dies ist logisch, denn so haben wesentliche Einheiten bei einem

Ausfall des Dienstes logischerweise größere Auswirkungen als wichtige Einheiten. Das Ende der Betreiber von Grundversorgungsdiensten (und der Anbieter digitaler Dienste) sowie die Annahme der Typologien wesentlicher und wichtiger Unternehmen zielen darauf ab, alle Verpflichtungen gegenüber diesen Akteuren zu harmonisieren.

Dieser Wunsch nach Harmonisierung wirft auch Fragen auf, denn es sind tatsächlich die Unternehmen und Betreiber, die sich ... selbst als EE oder EI bezeichnen müssen. Dabei orientieren sie sich an einer der zuvor festgelegten Branchen und der Größe ihrer Einheit (ETI und Großunternehmen, mittlere Unternehmen sowie Klein- und Kleinstunternehmen). Eine grundlegende Regel erklärt, dass die wesentlichen Einheiten insbesondere die großen Einheiten der 11 Sektoren mit hoher Kritikalität sind. Ergänzend dazu kann jedes Mitgliedsland nach eigenem Ermessen bestimmte Betreiber nach Mechanismen zur leichten Anpassung als wesentlich oder wichtig bezeichnen.

EINE NEUE VERBINDLICHE DIMENSION DER RICHTLINIE

Thierry Breton zufolge bietet diese Reform der Richtlinie den Unternehmen mehr Sicherheit, „*indem sie ein System von Verpflichtungen und Sanktionen einführt*". **Die NIS2-Richtlinie** ist laut dem EU-Kommissar ein echter „*großer Fortschritt*" und **erweitert daher ihre Durchsetzungsbefugnisse**. Welchen Pflichten unterliegen jedoch die wesentlichen und wichtigen Einheiten? Zunächst einmal ermöglicht die Verpflichtung, einen Schaden innerhalb von 72 Stunden zu melden, eine schnellstmögliche Reaktion und die Eindämmung der Cyberbedrohung. In der Richtlinie wird zwar eine erste Meldung des Vorfalls innerhalb von 24 Stunden angegeben, in Bezug auf insbesondere die Frist zur Umsetzung der Sicherheitsmaßnahmen gibt es im Rahmen der nationalen Umsetzung jedoch noch Spielraum. Zum Zeitpunkt des Verfassens dieses Artikels (und seiner Aktualisierung) wurden die Fristen zur Umsetzung der Richtlinie für die betroffenen Einheiten noch nicht angegeben. Parallel dazu müssen sich Unternehmen, Auftragnehmer und Behörden Sicherheitsprüfungen unterziehen, um Empfehlungen zu erhalten und so drastische Sicherheitsstandards zu erfüllen. Risikoanalyse und Sicherheit für Informationssysteme, Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebs, Sicherheit der Lieferkette, Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Informationssystemen, Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, grundlegende Verfahren (wie Cyberhygiene und Schulungen), Sicherheit des Personals oder die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung sind allesamt in der NIS2-Richtlinie vorgesehene Sicherheitsmaßnahmen.

Für nicht kooperierende oder sich fehlverhaltende Unternehmen hat die NIS2-Richtlinie auch die Sanktionen ausgearbeitet. Im Falle eines Sicherheitsvorfalls und der Weigerung, mit den Behörden zusammenzuarbeiten, stattet NIS 2 die Staaten mit einem Anordnungsrecht aus. Die Unternehmen müssen sich also den Forderungen des Staates unterwerfen und können mit Geldstrafen zwischen 1,4 % und 2 % des Umsatzes belegt werden. Wie bei dem früheren OSE-Status kann der Geschäftsführer haftbar gemacht werden.

Doch **obwohl diese Reform die Sicherheit erhöhen soll, wirft sie auch Haushaltsfragen auf.** Bei den Tausenden von betroffenen Unternehmen müssen sich die Exekutivausschüsse auf ihre Budgets für Investitionen in Cybersicherheitsprodukte konzentrieren. Und ihnen mehr Flexibilität zugestehen. Und wie sieht es mit den Gemeinden, Departements und Regionen aus? Diese Einrichtungen sind weniger flexibel als ihre privaten Pendants und müssen mit den Möglichkeiten, die sich ihnen bieten (wie dem Plan France Relance), mit begrenzten Budgets und fehlenden Humanressourcen zurechtkommen. Ein Rückstand in Bezug auf Instrumente und Kompetenzen, der insbesondere für kleine und mittlere Gemeinden bereits heute schwer aufzuholen ist und sich nach der Umsetzung der NIS2-Richtlinie sogar noch verschärfen könnte.

NIS 2, wann ist es soweit? Die Antwort ist nicht so einfach. **Das Europäische Parlament hat zwar die neue NIS2-Richtlinie am Donnerstag, den 10. November 2022, offiziell verabschiedet, die nationale Umsetzung wird jedoch bis zum 17. Oktober 2024 abgeschlossen werden.** Im zweiten Halbjahr 2023 sind Konsultationsphasen in Bezug auf die Verfassung weiterer regulatorischer Texte (Erlasse, Verordnungen) vorgesehen. Die Umsetzung auf nationaler Ebene dürfte daher nicht vor Ende 2023, Anfang 2024 erfolgen. Genug Zeit für alle betroffenen Stellen, sich auf eine große Veränderung angesichts der Cyberbedrohung vorzubereiten?