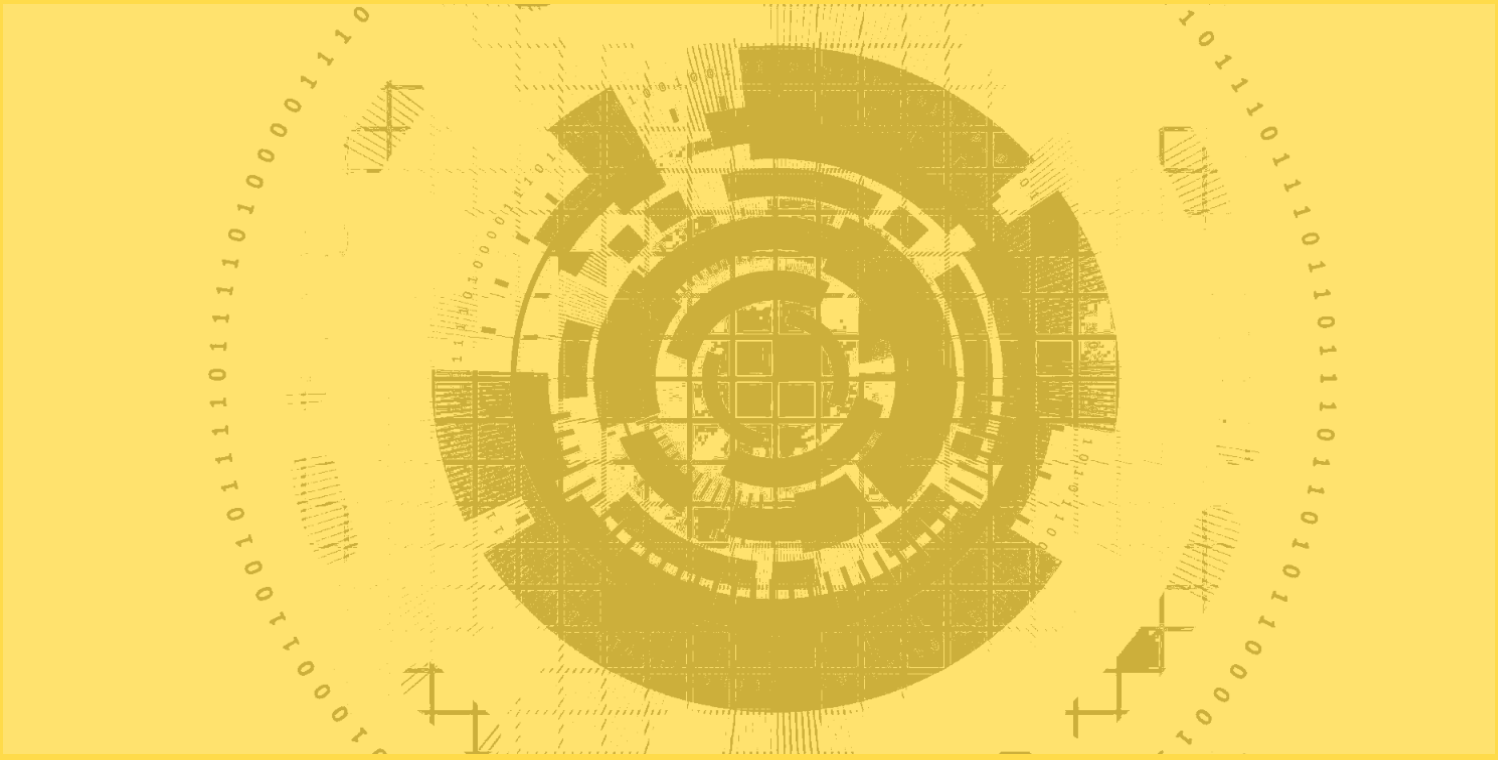
Cyber-Sicherheitsrat Deutschland e.V.

Positionspapier zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz (NIS2UmsuCG)



Einleitung

Die Network and Information Systems 2.0 Directive (NIS2-Richtlinie, NIS2-RL) hat das Ziel, die Cyber-Resilienz innerhalb der Europäischen Union umfassend zu stärken und ein gemeinsames, höheres Cybersicherheitsniveau in den Mitgliedsstaaten zu etablieren. In Deutschland wird diese Richtlinie durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht überführt.

Der Cyber-Sicherheitsrat Deutschland e.V. unterstützt das Ziel, unterschiedliche Sicherheitsstandards in den EU-Mitgliedsstaaten zu harmonisieren und insgesamt ein höheres Schutzniveau für die kritische Infrastruktur zu erreichen. Cyber-Resilienz in der Wirtschaft und der Gesellschaft insgesamt müssen erhöht werden. Im Sinne der Beteiligung von Verbänden und Zivilgesellschaft am Gesetzgebungsprozess haben wir unsere Forderungen an den Gesetzgeber in einem Positionspapier zusammengefasst. Dies sehen wir als konstruktiven Beitrag zur wirksamen Implementierung der NIS2-Richtlinie und langfristigen Unterstützung der gesetzgeberisch angestrebten Ziele.

V.i.S.d.P.: Hans-Wilhelm Dünn, Präsident, Cyber-Sicherheitsrat Deutschland e.V.

Autoren: Jan Arfwedson, Prof. Dr. Andre Döring, Hans-Wilhelm Dünn, Hannes Harthun, Dr. Alexander Löw

Cyber-Sicherheitsrat Deutschland e.V.
Spichernstraße 2
10777 Berlin

Tel.: (+49) 30 6796 365 26
info@cybersicherheitsrat.de
www.cybersicherheitsrat.de

Facebook | Twitter | LinkedIn | Xing | Instagram

1 Koordinierung bestehender und geplanter Regulierungen

Historisch gesehen hat sich die Regulierung der Cybersicherheit in einem stückwerkartigen Stil entwickelt. Angesichts bestehender und anstehender Regulierungsvorgaben wie dem KRITIS-Dachgesetz (als Umsetzung der CER-Richtlinie), formulierten Vorhaben in der Cybersicherheitsstrategie der Bundesregierung und dem Inkrafttreten der DORA-Verordnung sollten mögliche Dopplungen vermieden werden.
Das NIS2-Umsetzungsgesetz zielt auf den Cyberraum, das KRITIS-Dachgesetz nimmt physische Gefahren in den Fokus, jedoch handelt es sich in beiden Fällen um ähnliche Gefährdungslagen. Hierfür sollen unterschiedliche Meldesysteme für Vorfälle eingerichtet werden. Aus Sicht des CSRD e.V. sollte es ein einheitliches Meldesystem und einheitliche Ansprechpartner auf Bundesebene geben.
Sich wiederholende Anforderungen, beispielsweise durch mehrfache, teilweise bereits bestehende fachspezifische Meldepflichten, sollten vermieden werden. Eine fragmentierte Herangehensweise könnte andernfalls zu Überlappungen und Inkonsistenzen führen, beispielsweise wären Unternehmen verpflichtet, denselben Vorfall unter verschiedenen Gesetzen mehrfach melden müssen, was zu Ineffizienzen führt.

Es fällt allgemein auf, dass jede zusätzliche Regulierung der Cybersicherheit im Detail neue Anforderungen mit sich bringt, die im Wesentlichen auf den Vorgaben des Annex A der ISO/IEC 27001 basieren. Aus diesem Grund erscheint es sinnvoll, die ISO/IEC 27001:2022 als Grundlage für die Anforderungen an die Cybersicherheit kritischer Infrastrukturen zu etablieren. Branchenspezifische Anforderungen könnten dann als Umsetzungsempfehlungen im Sinne einer ISO/IEC 27002 präzisiert werden. Auf dieser Grundlage lässt sich eine einheitliche Vorgehensweise unter Verwendung bestehender weltweit anerkannter Standards erreichen.
Die gleichwertige Schutznorm BSI-Grundschutz bezieht sich noch auf die Norm ISO27001:2013, weist jedoch detaillierte Controls zur Umsetzung auf (Technische Richtlinien) und ist vollständig in deutscher Sprache verfasst. Vor der Akkreditierung ist zu prüfen, welche der beiden Normen sinnvoller angestrebt werden soll. Durch die steigende Diversifizierung von Schutznormen nach Branchen ergeben sich für KMU immer höhere Umsetzungshürden. Diese sich idealerweise zu harmonisieren und querschnittlich auszulegen, bzw. wie bei ISO/IEC 27001 und BSI-Grundschutz gegenseitig anzuerkennen. Eine Regelung hierzu fehlt.

2 Einbeziehung öffentlicher Verwaltung

Staatliche Institutionen sind nicht nur wegen ihrer kritischen Daten, sondern auch wegen ihrer Rolle als Vertreter der öffentlichen Ordnung besonders gefährdet für politische motivierte Cyberangriffe, wie mehrere Beispiele in der Vergangenheit gezeigt haben. Da es vorrangiges Ziel des Gesetzgebungsprozesses ist, die kritische Infrastruktur zu schützen, sollte die öffentliche Verwaltung als wesentlicher Betreiber der kritischen Infrastruktur

auf allen staatlichen Ebenen in den Anwendungsbereich einbezogen werden, auch als Signal an Betroffene der NIS2-Gesetzgebung in Wirtschaft und Gesellschaft.

3 Nutzung der Meldungen für Forschung und Information

Daten sind ein wertvolles Gut, im Kontext von Cybersicherheitsvorfällen können sie wichtige Erkenntnisse für den Umgang mit Bedrohungen liefern. Das Sammeln und Analysieren von Daten über Cyberangriffe können Trends aufzeigen und vor zukünftigen Bedrohungen warnen. Die eingegangenen Meldungen sollten daher für das angekündigte tagesaktuelle Lagebild (BSI Information Sharing Portal) genutzt werden und darüber hinaus in anonymisierter Weise der Cybersicherheitsforschung zur Verfügung gestellt werden.

4 Klarheit über den ‚Stand der Technik'

Technologie entwickelt sich ständig weiter. Unternehmen brauchen klare Richtlinien, was als sicher gilt. Insbesondere vor dem Hintergrund weitreichender Investitionsentscheidungen, die das Gesetz mit sich bringen wird, muss deutlich sein, woran sich Betroffene orientieren können. Der Begriff vom „aktuellen Stand der Technik" sollte deutlich definiert werden, wobei auf bestehende Standardisierungsverfahren und Normsetzungsprozesse wie bspw. DIN zurückgegriffen werden sollte. Mindestens sind Schutzbereiche zu priorisieren und deren Schutzziele klar zu definieren, um Fehlinterpretationen zu verhindern und ein europäisches Schutzniveau zu erreichen.

5 Aktive Benachrichtigung Betroffener

Das Wissen über eine Bedrohung ist der erste Schritt, um sie zu bekämpfen und auch in der Prävention beginnt der Prozess mit dem Wissen um seine Notwendigkeit. Dass betroffene Unternehmen selbst prüfen müssen, ob sie von der NIS2-Richtlinie betroffen sind und sich aktiv beim Bundesamt für Sicherheit in der Informationstechnik (BSI) melden bzw. registrieren müssen, führt unserer Einschätzung nach dazu, dass einige betroffene Organisationen und Unternehmen sich bewusst oder unbewusst den Regelungen entziehen und außerhalb der Regulierung agieren. Dies war und ist bereits bei der bestehenden Kritis-Regulierung festzustellen.
Sinnvoller wäre es, betroffene Organisationen und Unternehmen - bspw. wie in Österreich - per Bescheid darüber zu informieren, dass sie betroffen sind.
In Anbetracht der zahlreichen insbesondere mittleren Unternehmen die zukünftig unter die Regulatorik fallen werden, braucht es zudem praxisorientierte Umsetzungs- und Orientierungshilfen zu den gesetzlichen Vorgaben.

6 Fristen für Nachweispflichten nicht aufweichen

Compliance-Management ist ein fortlaufender Prozess, der regelmäßige Überprüfungen und Anpassungen erfordert. Die Frist für erstmalige Nachweise auf nun spätestens vier Jahre nach Inkrafttreten auszuweiten, ist in Anbetracht der aktuellen und zurückliegend stark zunehmenden Bedrohungslage unangemessen und sollte auf maximal 24 Monate nach dem Inkrafttreten festgelegt werden. Auch danach sollte ein zweijähriger Rhythmus etabliert werden, um mit verschiedenen Kontrollinstrumenten die Behebung der Mängel mitzuverfolgen.

7 Klarheit bei der Kategorisierung kritischer Anlagen

Es muss verlässliche Kriterien geben, die langfristig festlegen, was als kritische Infrastruktur gilt. Paragraf 28 des Gesetzentwurfs sieht vor, dass eine Anlage, die zu einem bestimmten Stichtag die in der Verordnung festgelegten Schwellwerte unterschreitet, dann keine kritische Anlage mehr ist. Wie die bisherige Kritis-Regulierung zeigt, führt dies unter Umständen zu einem stetigen Wechsel, sodass eine Anlage in einem bestimmten Zeitraum kritisch ist, dann wieder nicht – und andersherum. Darüber hinaus hat die Erfahrung gezeigt, dass die Betreiber in einem solchen Fall die ergriffenen technischen und organisatorischen Maßnahmen sowie die dazugehörige Sicherheitsorganisation herunterfahren, da sie die Notwendigkeit nicht mehr sehen und womöglich Kosten einsparen wollen.
Dementsprechend sollte eine Anlage, die als kritische Anlage definiert ist, auch bei einer Unterschreitung der festgelegten Schwellwerte von bis zu 20% nach wie vor eine kritische Anlage bleiben.

8 Sanktionen und Bußgelder mit klaren Ahndungsfristen

Die vorgesehenen Sanktionen und Bußgelder in Paragraf 60 sind sinnvoll und notwendig. Allerdings hat die Vergangenheit gezeigt, dass die im bestehenden IT-Sicherheitsgesetz vorhandenen Regelungen zwar existieren, jedoch in der Praxis scheinbar nicht angewendet werden. Das heißt, in Zukunft müssten etwaige Ordnungswidrigkeiten oder Zuwiderhandlungen zeitnah und unkompliziert, entsprechend der in Paragraf 60 geregelten Vorgaben, sanktioniert werden. Wünschenswert wäre daher die Berücksichtigung von etwaigen Fristen innerhalb welcher das BSI tätig werden sollte. Eine Aufweichung der Managementhaftung lehnen wir ab. Behörden sollen regelmäßig bei Verstößen bußgeldfähig werden.

9 Objektivität und Unabhängigkeit der Prüfstellen

Für Unternehmen und Verbraucher ist es entscheidend, dass sie den vergebenen Bewertungen und Zertifikaten vertrauen können. In Bezug auf Nachweisverfahren nach Paragraf 8 Absatz 3 BSIG und vermutlich im Bezug auf die zukünftige Nachweiserbringung im Kontext der NIS2-Umsetzung verhält es sich so, dass der Betreiber die Prüfstelle wählt und beauftragt. Die Kommunikation erfolgt seitens des BSI ausschließlich mit dem Betreiber; nicht mit der Prüfstelle direkt, was den Prozess verkompliziert und wenig effizient erscheinen lässt.
Ein grundlegendes Problem, welches aus dieser Konstellation entsteht, ist, dass Prüfstellen zunehmend als verlängerter Arm des BSI den Betreiber kontrollieren sollen, bspw. ob dieser denn plausible Erklärungen für die Nicht- oder teilweise Abstellung von bestimmten Mängeln aus dem letzten Nachweisverfahren hat. Die prüfende Stelle soll dabei plausibilisieren, ob die Begründung des Betreibers nachvollziehbar ist. Im Falle dessen, dass die Erklärung nicht plausibel ist und die prüfende Stelle dies dem BSI gegenüber mittels der Mängelliste und der Nachweisdokumente aus dem Nachweisverfahren kommuniziert, könnte dies zu entsprechenden Bußgeldern führen.
Hierdurch ist die prüfende Stelle, die wirtschaftlich abhängig vom Betreiber ist, unter Umständen nicht unabhängig und objektiv. Daher wäre es hier generell ein sinnvolles Vorgehen, dass die prüfenden Stellen direkt von Seiten des BSI beauftragt werden und im Losverfahren entsprechende Verfahren zugeteilt bekommen.

10 Anwendung des Reifegradmodells

Ein standardisiertes Bewertungssystem könnte Unternehmen dabei helfen, ihre eigenen Schwachstellen zu erkennen und sich mit anderen zu vergleichen. Die Effektivität der Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) sollte anhand eines Reifegradmodells gemessen und überprüft werden. Eine wesentliche Voraussetzung hierfür ist die Verwendung eines einheitlichen Reifegradmodells. Die ISO/IEC 15504-5 (SPICE-Modell) bietet sich hier als eine geeignete Option an.
Es sollte vermieden werden, eigene Standards zu definieren, die oft an dieses Modell angelehnt sind. Die Messung des Reifegrades und die zentrale Berichterstattung über die Reifegrade ermöglichen den Aufsichtsbehörden die Überwachung der Weiterentwicklung des ISMS in den Unternehmen, die von der NIS2-Umsetzung betroffen sind, anhand einer einzigen Kennzahl. Es könnten Mindestwerte für den Reifegrad festgelegt werden, wie es bereits bei TISAX der Fall ist, wo der Mindestwert für SPICE bei 3 liegt. Dadurch könnte ein einheitliches europäisches Sicherheitsmindestniveau erreicht werden.
In diesem Zusammenhang sollte die Rolle der ISMS-Auditoren gestärkt werden, da es hier wirtschaftliche Abhängigkeiten gibt. Diese Auditoren sollten in der Lage sein, unabhängig zu handeln (siehe 9).