Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)523 A

HISOLUTIONS

STELLUNGNAHME ZUR EXPERTENANHÖRUNG ZUM NIS2UMSUCG

1. Vorbemerkungen

Es ist von höchster Bedeutung, dass dieses Gesetz schnellstens verabschiedet wird. Die Tatsache, dass die Wirtschaft die Einführung fordert, obwohl es zu Mehraufwänden führen wird, spricht hier eine deutliche Sprache. Es besteht die große Sorge, dass sich eine weitere Verzögerung ergibt.
Ziele und Grundidee sind komplett richtig: Was fachlich gefordert wird, sollten alle machen, egal ob reguliert oder nicht.

2. Allgemeine Kritikpunkte

2.1. Rahmenbedingungen

Losgelöst von einzelnen Paragraphen ist zuallererst die zeitlich und inhaltlich fehlende Koordinierung mit dem KRITIS-Dachgesetz problematisch. Hier läuft der Prozess noch schleppender und unerfreulicher als beim hier betrachteten Gesetz. Der erste Entwurf wurde veröffentlicht, ohne jemals mit der Wirtschaft gesprochen zu haben, die Qualität merkte man dann zum Beispiel daran, dass das Wort „Cyber“ im ersten Entwurf des KRITIS-Dachgesetzes nicht einmal vorkam (auch wenn Cybersecurity nicht im Fokus des Gesetzes steht, ist eine vollständige Ausblendung weltfremd und kontraproduktiv).

Noch schlimmer wird es, wenn dann parallel eine dritte Abteilung aus dem BMI „Eckpunkte für eine nationale Wirtschaftsschutz-Strategie“ veröffentlicht. Auch dies offensichtlich nicht abgestimmt und zwar nach meiner Kenntnis weder mit der Wirtschaft noch mit den anderen Abteilungen des BMI.

Aus politischer, verwaltungstechnischer und juristischer Sicht mag dies sinnvoll oder zumindest nachvollziehbar wirken, aus Sicht der betroffenen Unternehmen ist dies mehr als ärgerlich, denn für diese gehören die Themen unauflösbar zusammen.

Es ist Common Sense, dass ein All-Gefahren-Ansatz gewählt werden muss – Deutschland wählt hingegen einen zersplitterten Weg.

Es rächt sich hier in meinen Augen, dass es – brutal gesagt – nichts gibt, was wirklich den Namen Strategie verdient: Egal ob Digitalisierungsstrategie, Nationale Sicherheitsstrategie, Nationale Cyber-Sicherheitsstrategie, Wirtschaftsschutzstrategie: Vision/Mission, SMARTE Ziele (spezifisch, messbar, attraktiv, realistisch, terminiert), abgeleitete konkrete Maßnahmen mit Verantwortlichkeiten und dies alles integriert, übergreifend und in dem Aspekte und Maßnahmen von innerer und äußerer Sicherheit, Finanz- und Industriepolitik, Bildung und Forschung orchestriert: überall Fehlanzeige. Stattdessen Willensbekundungen, Absichtserklärungen und Übersichtspapiere, die nicht ineinandergreifen.

Ein Beispiel für dieses nicht-kohärente Handeln: Wir unterhalten uns meist über die Gefahr des „Gold-Platings“, des Überziehens der europäischen Anforderungen bei der Umsetzung in deutsches Recht, hier haben wir auch einmal die gegenteilige Variante: In Artikel 24 Abs. 1 Satz 2 der originalen NIS-2-Richtlinie heißt es: „Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.“

Dies findet sich in der deutschen Umsetzung nirgends wieder, stattdessen kann das Organisationskonto nicht genutzt werden und wird im Gesetz nicht adressiert, die Haushaltsmittel für die eID werden gestrichen und es droht, dass nicht nur in 2025 keine Weiterentwicklung

stattfindet, sondern ab 2026 sogar die Nutzung der laufenden Verfahren gestoppt werden muss, da die Mittel fehlen.

Das ist das Gegenteil eines strategisch sinnvollen, kohärenten und ganzheitlichen Herangehens.

2.2. Geburtsfehler in Brüssel

Zentrale Fehler sind aus meiner Sicht bereits im Vorfeld, also während des europäischen Gesetzgebungsprozesses geschehen. Dies bezieht in meinen Augen Politik, Wirtschaft und Verbände ein.

Viele hatten offensichtlich – ggf. ermüdet durch den zähen Prozess rund um das IT-Sicherheitsgesetz 2 – den seitens der französischen Regierung aufgebauten Zeitdruck unterschätzt, die dies in ihrer Ratspräsidentschaft umsetzen wollten, welche wiederum durch die parallel stattfindende Präsidentenwahl de facto noch weiter verkürzt war. Vielleicht waren wir uns alle auch zu selbstgewiss, dass wie bei NIS1 die deutschen Muster durch die vorlaufende deutsche Gesetzgebung auch wieder zur Blaupause der EU-Regelungen werden würden.

Es gab dann irgendwann einen Weckruf seitens des BMI auch mit Bitte um Unterstützung durch die Wirtschaft(sverbände) in Brüssel, was u. a. dazu führte, dass das Wirtschaftsforum der SPD und der Wirtschaftsrat der CDU wortgleiche Warnbriefe z. B. an die MdEPs versendeten. Dies führte aber nur noch sehr eingeschränkt zu Erfolgen. Die Erfolge lagen dann unglücklicherweise eher in der Rücksichtnahme auf Aspekte des Föderalismus, als etwa auf Aspekten der deutschen Unternehmensstruktur, Stichwort „Mittelstand als Rückgrat der Wirtschaft“.

Die zentralen Kardinalsfehler sind aus meiner Sicht:

- keine Umsetzungsfristen für die in den Anwendungsbereich fallenden Einrichtungen
- Scope zu breit
- Meldefrist von 24 Stunden nicht angemessen

Um nicht falsch verstanden zu werden: Die inhaltlichen Anforderungen von NIS2 sind, wie schon in den Vorbemerkungen unterstrichen, komplett richtig und eigentlich etwas, was für alle Unternehmen, ob von NIS2 betroffen oder nicht, Gültigkeit haben sollte. Realistisch betrachtet sind diese aber von einem großen Teil der Unternehmen noch nicht annähernd vollständig umgesetzt. Jetzt müssen 30.000 Unternehmen dies zeitgleich umsetzen und vermutlich großteils auf Berater zurückgreifen. Diese Berater gibt es aber ebenfalls nicht in der benötigten Anzahl, denn der Stellenmarkt ist leergefegt. Und ob die sprichwörtliche Molkerei mit 51 Mitarbeitern im Allgäu wirklich für Wohl und Wehe unserer Gesellschaft wichtig ist, lasse ich offen.

Am Ende wird vermutlich Folgendes passieren: Es werden Regeln geschaffen, die nur teilweise oder gar nicht umgesetzt werden und die Ausrede, dass der Markt gar nicht die Ressourcen hergab, werden alle ziehen können, die kleine Molkerei sowie der große Energieversorger. Zumindest den Letztgenannten hätte man dieses Schlupfloch entziehen müssen (und hier auch eventuelle Fristen, in denen nicht geprüft wird, verkürzen können).

Auch angesichts der Zeitenwende wäre die Fokussierung auf die wirklich relevanten Elemente effektiver gewesen. Nun erhöhen wir den Deich überall gleichzeitig um wenige Zentimeter, anstatt an den neuralgischen Punkten, die wir ja kennen, schnell massive Verbesserungen zu erreichen.

Eine risikoorientierte Erweiterung auf etwa 10.000 Unternehmen wäre aus der Gesamtbetrachtung zielführender gewesen. Und die Verwendung der eben nur begrenzt vorhandenen Ressourcen dadurch punktgenauer. Nun können wir nur hoffen, dass es der Markt regelt: in dem Sinne, dass die wirklich relevanten Unternehmen bereit sind, höhere Tagessätze zu bezahlen und so die Mittelständler „ausstechen".

Eine Konjunkturhilfe für Sicherheitsberatungsunternehmen wie meines, die diese Branche nicht gebraucht hätte.

Stattdessen wurde in Deutschland dafür mit der dreijährigen Frist der Nicht-Prüfung ein Kunstgriff gewählt. Dies ist einerseits nachvollziehbar und für deutsche Verhältnisse geradezu elegant; man hätte bei den wirklich neuralgischen Punkten lieber auf diese Schonfrist verzichtet, ihnen dafür aber auch einen weniger überforderten Ressourcenpool geboten.

3. Konkrete Kritikpunkte am Gesetzesentwurf

3.1. Nicht akzeptable Reduktionen auf staatlicher Seite

Von Referentenentwurf zu Referentenentwurf zu finaler Fassung wurde die Liste der von den Vorschriften ausgenommenen Institutionen auf staatlicher Seite immer länger und die Liste von umzusetzenden Punkten immer kürzer.

Als erstes fielen auf Empfehlung des IT-Planungsrates die Kommunen und Gemeinden heraus. In den letzten Jahren hat sich gezeigt: „The weakest link" ist auf der öffentlichen Seite und zwar genau die kommunale Ebene, wie Anhalt-Bitterfeld, Schwerin, Südwestfalen-IT etc. gezeigt haben. Und genau diese werden ausgenommen.
Wichtig ist an diesem Punkt: Ein Großteil der Kommunen und Gemeinden WOLLTE reguliert werden, es ist am Ende eine Frage, wer es zahlen muss. Jetzt ist es geklärt: Die nun nicht zu vermeidenden Schäden zahlen wir alle.

Es gibt nur eine Variante, die teurer ist, als jetzt einen Plan zu entwickeln und umzusetzen, um genau diese Schwächsten, aber für die Gesellschaft und Wirtschaft massiv wichtigen Elemente zu schützen: nichts tun.

Und genau dieser Weg wird beschritten.

Man muss konzedieren, dass es tatsächlich unmöglich wäre, die Erfüllung aller Regelungen fristgerecht zu erreichen. Aber daran hat sich bei der Wirtschaft ja auch niemand gestört. Und wenn man Kommunen und Gemeinden nicht per NIS2-Umsetzung schützen kann, so wäre es das Mindeste gewesen, einen einheitlichen und konkreten Handlungsplan aufzusetzen, wie dieses Ziel bis wann in einheitlicher Qualität erreicht werden kann. Nun verbleibt dies bei den Bundesländern mit absehbar sehr unterschiedlichen Ansätzen, die, auch durch Größe und Finanzkraft der Bundesländer geprägt, unterschiedliche Qualität haben werden.

Das zu erwartende Ergebnis haben wir exemplarisch im letzten Jahr beim Thema iKfz (digitalisierte KfZ-Anmeldung) erlebt. Ein bundesweit standardisierbares Verfahren wurde in rund 500 Varianten eingeführt, die jeweils getrennt geschützt werden mussten, was angesichts mangelnder Auditoren unmöglich war und dazu führte, dass das Verfahren in weiten Teilen Deutschlands zwischenzeitlich wieder gestoppt werden musste.

Ich maße mir definitiv keine rechtswissenschaftliche Kompetenz an und dies erst recht nicht auf dem Gebiet des Verfassungsrechts, aber für mich hat dies durchaus auch etwas mit der angestrebten „Gleichwertigkeit der Lebensverhältnisse“ zu tun, wenn es Gegenden gibt, wo die gesamten kommunalen Serviceleistungen über Monate aufgrund mangelnder Vorsorge durch Cyberangriffe nicht zur Verfügung stehen und sich dies mittelfristig auch mit der Wirtschaftskraft der Regionen korrelieren lässt.

Der gleiche Effekt ist auch bei den jeweiligen Umsetzungen auf Länderebene zu erwarten. Unterschiedliche Umsetzungen, mal als Gesetz, mal als Verordnung, mal als Runderlass. Wer prüft die Passgenauigkeit und qualitative Vergleichbarkeit? Vom bürokratischen Aufwand für überregional tätige Unternehmen ganz zu schweigen.

Mit dieser Entscheidung war klar, dass das Gesetz auf staatlicher Seite schon einmal nicht zu einem wirklichen Cybersicherheitsstärkungsgesetz werden konnte.

Aber es kam noch schlimmer, mit der letzten Version haben wir nun definitiv ein Cybersicherheitsschwächungsgesetz. Als letztes fielen die nachgelagerten Bundesbehörden mehr oder weniger heraus. Nachgelagerte Bundesbehörden müssen nicht mehr IT-Grundschutz umsetzen, was heute mit dem UP Bund noch Pflicht ist (§44).
De facto stellt dieser Punkt im Endeffekt sogar die „Netze des Bundes“ infrage, da alle nachgelagerten Behörden eigentlich nicht mehr die Sicherheitsanforderungen für ein einheitliches Sicherheitsniveau erfüllen.

Ein kurzer Einschub zum Thema IT-Grundschutz: Wichtig ist mir der Hinweis, dass Kritik am IT-Grundschutz ob des zu großen Umfangs, fehlender Flexibilität und damit zu hohen Umsetzungsaufwänden nur in geringem Maße treffend ist. Zum einen gilt auch hier ein risikoorientierter Ansatz, der es eben nicht darauf anlegt, dass alle Inhalte erfüllt werden müssen, zum anderen gibt es auch hier immer die Möglichkeit, sinnvolle Alternativwege zu beschreiten. Das BSI ist hier in einem unverschuldeten Dilemma: Entweder werden Hilfen/Umsetzungsleitfäden etc. als nicht konkret genug empfunden, und wenn sie dann konkret genug sind, wird zu großer Umfang und zu wenig Flexibilität moniert.

Darüber hinaus arbeitet das BSI derzeit intensiv an einer massiven Straffung der Inhalte.

§29 ist ein Horrorkabinett für alle sicherheitsaffin denkenden Personen:

- Ausnahme von der Pflicht aus §30 zu Risikomanagementmaßnahmen (außer Bundeskanzleramt und Ministerien)
- keine Billigungs-, Überwachungs- und Schulungspflicht für Amtsleitungen, wie in §38 für Geschäftsleitungen verpflichtend eingeführt (Warum sind Schulungen für Vorstände zwingend erforderlich, für Amtsleiter aber entbehrlich?)
- Ausnahme von Aufsichts- und Durchsetzungsmaßnahmen durch das BSI aus §61 (was auch die Frage nach einem „Bundes-CISO“ noch spannender macht, dazu später mehr)
- Dass Ausnahmen von Bußgeldvorschriften für Amtsleitungen gemacht werden, ist unvermeidbar, verstärkt aber in der Wirtschaft den Eindruck, dass in allen Belangen unterschiedliches Maß angelegt wird.

Aber auch das ist noch nicht alles. Weiterhin ausgenommen sind:

- IT-Dienstleister, die Dienste für Landes- und Kommunalverwaltungen erbringen,
- „Institutionen der sozialen Sicherung“, Bundesbank, Auswärtiges Amt, Bundeswehr, BND, BfV.
- Der Sektor Forschung wird gemäß der Begriffsdefinition „Forschungseinrichtung“ auf angewandte Forschung mit kommerziellem Zweck begrenzt. Warum keine Grundlagenforschung, also genau der Bereich, wo wir in Deutschland aktuell noch wirklich gut aufgestellt sind? Gleiches gilt für durch den Bund finanzierte Forschungseinrichtungen, welche in der Rechtsform einer Stiftung des öffentlichen Rechts nach Landesrecht aufgebaut sind. Ich verstehe, dass dem Bund hier teilweise die Hände gebunden sind. Das Dumme ist nur: Dem Angreifer sind sie nicht gebunden.

3.2. Rolle und Möglichkeiten des BSI

Grundsätzlich ist die Aufwertung des BSI positiv zu bewerten, auch das Streben nach einer Zentralstellen-Funktion ist wünschenswert. In aller Deutlichkeit: Man wird lange nach einem Experten außerhalb von Behörden suchen müssen, der dem Aspekt des Föderalismus bei der Cybersicherheit in der in Deutschland betriebenen Umsetzung etwas Positives abgewinnen kann (gleiches gilt übrigens für die Themen Digitalisierung und Bildung).

Inhaltsleer ist leider auch §48, der das Amt des Koordinators für Informationssicherheit definiert (was inklusive der inoffiziellen Aussagen, dass dieses beim BSI angesiedelt sein soll, absolut begrüßenswert ist).

Aber welche Rechte und Pflichte sind damit verbunden? Aktuell klingt es nach einem zahnlosen Tiger und reiner Symbolpolitik.

Verstärkt wird es noch dadurch, dass in §29 ja explizit die Aufsichts- und Durchsetzungsmaßnahmen aus §61 ausgehebelt werden. Damit ist eigentlich klar, dass die Rolle eines „Bundes-CISOs“ eher Feigenblatt als „Game Changer“ sein wird. Auch hier hätte ein Austausch mit der Wirtschaft geholfen: All diese Fehler hat die Wirtschaft vor vielen Jahren ebenfalls begangen und lernen müssen, dass es so nicht gut funktioniert.

Erforderlich ist hier aus fachlicher Sicht eine klare Weisungsbefugnis, denn das, was zuvor als Expertenmeinung zur aktuellen Ausprägung des Föderalismus in Bezug auf Kernfunktionen der Cybersicherheit postuliert wurde, gilt in gleichem Maße für das Prinzip der Ressortunabhängigkeit.

Wir brauchen keinen Koordinator, der weiß, dass jeder „sein eigenes Ding macht“, sondern jemanden, der diesem Treiben ein Ende bereitet.

Wenn man die „Best Practices“ aus der Privatwirtschaft auf die Rolle eines Bundes-CISOs überträgt, ergibt sich folgende Beschreibung:

Der Bundes-CISO

- koordiniert das Informationssicherheitsmanagement des Bundes,
- entwickelt und pflegt Programme zur Gewährleistung der Informationssicherheit des Bundes im Benehmen mit den Behörden,
- beaufsichtigt die Umsetzung,
- hat ein direktes Vortragsrecht vor dem Innen- und Haushaltsausschuss des Deutschen Bundestages.

Zusätzlich wäre die verpflichtende Einbindung in alle Gesetzesvorhaben etc., die die Cybersicherheit tangieren, sinnvoll.

Viel dramatischer als diese Ausführungen zum Bundes-CISO ist aber die Tatsache, dass dem BSI neue Aufgaben übertragen wurden, dies aber nicht annähernd in der Haushaltsplanung berücksichtigt wurde.

Statt des erforderlichen Aufwuchses stehen 37 Millionen Euro weniger in der Planung und dementsprechend natürlich auch keinerlei neue Stellen.

Wie will man also die 30.000 Unternehmen prüfen, ob deren Registrierung korrekt ist?
Wie prüfen, ob sich Unternehmen nicht registriert haben (hierzu später noch mehr)?
Wer soll den Unternehmen bei Fragen zur Seite stehen?

Und vor allem: Wer soll die einkommenden Meldungen auswerten und Informationen zur Verfügung stellen?

Zur Verdeutlichung: Die Erstmeldung hat gemäß EU-Template 19 Felder, die 72h-Meldung 35 Felder (davon 19 neu), die Abschlussmeldung (44 Felder, davon 9 neu), egal welche Unternehmensgröße betroffen ist. Diese Informationen müssen aber ausgewertet und verarbeitet werden, damit der damit verbundene Bürokratieaufbau einen Sinn ergibt.

Wir bauen hier auf der Unternehmensseite eine nicht zu unterschätzende Bürokratie auf, die dann auf staatlicher Seite auf ein Vakuum stößt.

Die Verarbeitung der Meldungen zu verwertbaren Informationen an die Unternehmen ist aber nur der eine Hebel zur wirklichen Steigerung der Sicherheit.

Der zweite Hebel ist die in §15 definierte Möglichkeit zur Detektion von Angriffsmethoden und von Sicherheitsrisiken. Leider wird hier nur der halbe Schritt gegangen, in dem dies auf die von NIS2UmsuCG betroffenen Institutionen beschränkt wird. Zielführender wäre hier ein Verzicht auf die Beschränkung auf kritische Infrastrukturen, (besonders) wichtige Unternehmen und Verwaltung.

Gerade beim Bekanntwerden einer neuen Schwachstelle beginnt regelmäßig ein „Rat race“ zwischen Angreifern und Verteidigern, um potenziell Betroffene zu identifizieren. Es wäre in diesem Rennen ein wirklicher „Game Changer“, wenn hier das BSI flächendeckend unterstützen könnte.

Dies hat ja auch nichts mit dem Ausnutzen von Schwachstellen zu tun. Claudia Plattner beschrieb das plastisch auf der IT-Sicherheitsmesse it-sa in diesem Monat mit einem „Rundgang, um zu schauen, ob Türen offenstehen“ und eben nicht dem Durchschreiten oder gar Aufbrechen der Tür. Alle Regeln zur Kontrolle dieser Aktivitäten sind ja korrekt und angemessen im Gesetz hinterlegt. Wenn diese gelten, spricht nichts gegen eine Ausdehnung des Betrachtungsbereiches.

3.3. Der Registrierungs- und Meldeprozess sowie Meldepflichten

Betroffenheitsklärung: Bringschuld des Staates, nicht der Unternehmen

Es ist vollkommen unverständlich, warum man es den Unternehmen überlässt, ihre Betroffenheit festzustellen und diese zu melden.
Ein Gesetz, bei dem der Staat sich außer Lage sieht, selbst zu definieren, wer betroffen ist und die Betroffenen zu informieren, hat aus meiner Sicht schon einen massiven Geburtsfehler.
Ebenso ist unklar, warum dies Ländern wie Kroatien und Lettland möglich ist, den deutschen Behörden aber nicht.
Und nein, es ist in vielen Fällen nicht so einfach, die eigene Betroffenheit festzulegen, die Tücke steckt da im Detail.

Auch hier ist der zu erwartende Effekt schon jetzt klar und wird offen diskutiert: Diverse Anwälte und Justiziare empfehlen bereits jetzt, sich im Zweifelsfall lieber nicht zu registrieren, weil man dann sagen kann, dass man es anders bewertet hat und nicht zugeben muss, „sehenden Auges“ gegen Regeln verstoßen zu haben.

Die Komplexität der Regeln bietet genügend Potenzial für derartige Ausflüchte.

Denkbar wäre ein Zwischenweg, wie ihn Italien wählt: Die Unternehmen melden sich in Kurzform, die Behörde prüft die Betroffenheit, nach Bestätigung durch die Behörde startet die Frist, in der die Unternehmen die vollständige Registrierung durchführen müssen.

Das Information Sharing-Portal ist sinnvoll. Wenn es umfassend integriert ist.

Der Ansatz des Information Sharing-Portals ist positiv, sollte aber integriert Cyber- und physische Gefahren abbilden und tagesaktuell sein. Dies führt dann zur Forderung eines gemeinsamen Meldewesens mit dem KRITIS-Dachgesetz.
Und auch wenn dies in erster Linie diesen Gesetzentwurf betrifft, also nicht integraler Bestandteil dieser Anhörung ist, so kann man die Punkte auch nicht völlig voneinander trennen: Dem BSI fehlen die Ressourcen, um eine wirklich funktionale Melde- und Informationsplattform bieten zu können.
Die Aufgaben des BBK (das hiermit explizit nicht kritisiert werden soll!) sind lt. Eigendarstellung:

- Selbstschutz
- Warnung der Bevölkerung
- Schutzbau
- Aufenthaltsregelung
- Katastrophenschutz nach Maßgabe des § 11 ZSKG
- Maßnahmen zum Schutz der Gesundheit
- Maßnahmen zum Schutz von Kulturgut

Was davon ist auch nur annähernd mit der dort angedachten Meldestellenfunktionalität vergleichbar oder auch nur ein guter Startpunkt dafür?
Sprich, wir wollen hier etwas aufbauen, wofür nicht nur Personal, sondern jegliche Vorerfahrung fehlt und was nicht wirklich zur eigenen Grundausrichtung passt. Und dies in einer Situation, in der die integrierte Betrachtung losgelöst von der behördlichen Zuständigkeit absolut zwingend erforderlich ist.

Die Bündelung der Verantwortlichkeit (kombiniert mit der Finanzierung der entsprechend erforderlichen Stellen) erhöht massiv die Qualität und reduziert die Aufwände für Unternehmen (und durch Synergieeffekte auch für die Verwaltung). Eine Win-Win-Situation, die wir einfach an uns vorbeiziehen lassen.

Dies alleine würde aber auch noch nicht für ein wirklich nutzenoptimiertes Informationsportal sorgen.

Eine gute Informationsbasis ist keine Tool-, sondern eine Mindset-Frage.

Aus eigener Anschauung: Mein Unternehmen ist geheimschutzbetreut, in der Allianz für Cybersecurity für zusätzlichen Austausch vertraulicher Informationen „freigeschaltet", dennoch fällt mir kein einziger Fall ein, in dem wir von staatlicher Seite Informationen erhalten haben, die wir nicht schon kannten – meist reicht das Lesen von heise.de aus, also nicht einmal besonderer, nur Experten bekannten / zugänglichen Informationsquellen.

Die Plattform allein löst nicht das Problem, wir brauchen einen Paradigmenwechsel:

Aktuell wird das Risiko bewertet, wenn eine Information einen Unberechtigten erreicht. Nicht bewertet wird aber das oft signifikant höhere Risiko, wenn eine Information die Berechtigten NICHT erreicht. Hier braucht es Regeln und einen Mindset-Wechsel hin zu einem „Mehr und schneller".

Ärgerlich auch, dass derzeit beim Portal nicht die Möglichkeiten des Organisationskontos genutzt werden können (konkret Modul 6 des Organisationskontos), dies würde massive Ersparungen für Staat und Wirtschaft bedeuten. Ein schönes Beispiel, wo langsame Digitalisierung der Verwaltung und Budgetrestriktionen in kürzester Zeit zu Mehraufwänden führen, respektive reale Einsparungen verhindern. Nichtsdestotrotz sollte die zeitnahe Umsetzung und Nutzung des Organisationskontos explizit weiterverfolgt und eingefordert werden. Es ist nicht vermittelbar, warum Unternehmen jetzt einen weiteren „Account" für ihre Interaktion mit staatlichen Stellen haben sollen, wenn das Organisationskonto im Onlinezugangsgesetz eigentlich als zentrale Schnittstelle von Staat und Wirtschaft angelegt ist. Sinnvoll wäre zumindest in der Zwischenzeit für Konzerne auch die Schaffung eines „Oberkontos", das für mehrere meldungspflichtige Tochterunternehmen gilt, um hier den Pflegeaufwand zu minimieren.

Zu kurze und missverständliche Fristen

Aus meiner beruflichen Praxis sind die 24 Stunden bis zur ersten Meldung für viele, gerade kleinere Unternehmen („kleinere" ist hier nicht im Sinne der KMU-Regelungen zu verstehen) zu kurz. Verschärft wird dies durch die uneindeutige Formulierung in § 32 Abs. 1 Nr. 1 BSIG-E:

> 1. „unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall,…"

Da Unternehmen zunächst prüfen müssen, ob ein Sicherheitsvorfall die Erheblichkeitsschwelle überschreitet, muss zwingend klargestellt werden, dass die 24-stündige Frist zur Abgabe einer Erstmeldung erst NACH Abschluss der Prüfung, ob ein Cybersicherheitsvorfall erheblich ist, beginnt und wann diese Prüfung spätestens beginnt.

Es sollte klarer kommuniziert werden, dass man die Anfangsbewertung eines Vorfalls "zeitnah" durchzuführen hat, jedoch nur innerhalb der Arbeitszeit. Damit würde ein am Samstag festgestellter Vorfall eventuell (und spätestens) am Montagmorgen bewertet, frühestens also am Dienstag zum Ablauf der 24 Stunden führen, sofern die Bewertung einen erheblichen Sicherheitsvorfall feststellt.

Die aktuelle Formulierung könnte indes dahingehend interpretiert werden, dass die 24-Stunden-Frist ab dem Zeitpunkt beginnt, an dem die betroffene Einrichtung von einem Sicherheitsvorfall erfährt. Dies würde de facto zur Pflicht einer 24*7-Verfügbarkeit verschiedener Mitarbeitergruppen führen, was zumindest für kleinere Unternehmen schwer tragbar ist.

Zwischenmeldungen auf ein angemessenes Maß beschränken

Auch nach dieser Erstmeldung wird es nicht gerade besser und vor allem nicht bürokratiearm. Reichte beim IT-Sicherheitsgesetz 2 eine Meldung pro Vorfall, so reden wir jetzt von bis zu fünf Meldungen.
Noch einmal: Für einen Großkonzern mag dies alles machbar sein, wir reden hier aber von der Ausdehnung auf mittlere Unternehmen. Für Unternehmen mit 50 bis 249 Mitarbeitenden wäre es daher wünschenswert, sie zumindest von den Zwischenmeldungen zu befreien. Hier ist einfach auch nicht mit einem Erkenntnisgewinn zu rechnen, der anderen Unternehmen zeitnah zur Verfügung gestellt werden könnte (mal ganz losgelöst von der Frage, wie denn eine zeitnahe Information seitens des BSI gewährleistet werden soll). Aufwand und Mehrwert stehen hier in einem Missverhältnis. Eine andere Möglichkeit wäre, zumindest den Umfang auf ein angemessenes Maß reduzieren oder auf ausgewählte Fälle zu beschränken. Hier könnte die Unternehmensgröße oder die Vorfallsart eine Rolle spielen.

3.4. Der blinde Fleck: Vertrauenswürdigkeitsüberprüfung von Mitarbeitenden

2023 berichtete u. a. der SPIEGEL über die sog. „Vulkan Files“, in der auch für die breite Öffentlichkeit ein Fakt sichtbar wurde, vor dem Fachleute schon lange warnen: Wir müssen neben IT und Physik mehr auf die Menschen schauen. An diversen Stellen u. a. bei Amazon Webservices und Siemens waren in Westeuropa Administratoren beschäftigt, die mit dem russischen Militärnachrichtendienst GRU und dem Auslandsnachrichtendienst SWR in Verbindung gebracht werden konnten.

Spitz formuliert: Selbst sichere IT und sicherer physischer Schutz sind nur Pseudo-Sicherheit, wenn die Personen, die berechtigt Zugang zu IT-Systemen und Infrastrukturen erhalten, nicht auf ihre Vertrauenswürdigkeit überprüft werden können.
Dieser Aspekt wurde sowohl bei NIS2 als auch beim KRITIS-Dachgesetz komplett außenvorgelassen.

Es muss dringend eine Lösung gefunden werden, die es Unternehmen ermöglicht, für einen engen Personenkreis an neuralgischen Punkten Sicherheitsüberprüfungen durchführen zu lassen, die auf dem Prinzip der Freiwilligkeit und entsprechend den Prinzipien und Verfahrensweisen der Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz basieren und von den Unternehmen bezahlt werden.

3.5. Sonstige Kritikpunkte und Verbesserungsvorschläge

Klärung der Situation in der „Karenzzeit“

Wie in den Einführungsbemerkungen erwähnt, ist die Gewährung einer dreijährigen Frist, in der auf Überprüfungen durch das BSI verzichtet wird, eine zumindest auf den ersten Blick elegante Lösung für den Umgang mit der in Brüssel schlicht versäumten Definition einer Umsetzungsfrist.

Bei genauerem Betrachten entstehen aber Fragen, die der Gesetzgeber unbedingt im Vorfeld klären sollte:
Was passiert, wenn in diesen 3 Jahren Sicherheitsvorfälle auftreten und das betroffene Unternehmen noch keine vollständige Umsetzung erreicht hat, zu dem es ja nach Gesetz von Tag 1 an verpflichtet ist?
Werden Cyberversicherungen dann noch zahlen? Werden Richter Schadensersatzzahlungen verfügen mit dem Hinweis auf Nicht-Erfüllung des Gesetzes?

Hier sollte eine Klarstellung im Gesetz erfolgen. Denkbar wäre, dass im ersten Schritt neben der Definition der Verantwortlichkeiten und der Etablierung der Meldestruktur zwingend ein konkreter Umsetzungsplan existieren muss, der den terminierten Weg zur kompletten Erfüllung aufzeigt. Im zweiten Schritt muss nachgewiesen werden, dass man sich entsprechend des Plans im Umsetzungsprojekt befindet, um vor negativen Konsequenzen durch nicht komplette Erfüllung freigestellt zu werden.

Definition IT-Sicherheitsbeauftragte

In §45 und §46 werden die Rollen von IT-Sicherheitsbeauftragen definiert. Dies ist positiv, es bleibt aber zu unkonkret. Sinnvoll wäre die konkrete Benennung von Aufgaben und vor allem Rechten. Das verwendete Wort „beteiligen“ ist de facto wertlos.
So droht die Machtlosigkeit der Rolle, vor allem ob der Unklarheit der organisatorischen Aufhängung. Das BSI empfiehlt für IT-Sicherheitsbeauftragte z. B., dass diese nicht dem IT-Verantwortlichen unterstellt werden, da dies einen Zielkonflikt beinhaltet. Eine solche Regelung inkl. der klaren Benennung der Rechte wäre wünschenswert.

Unscharfe Begrifflichkeiten

- *Management von Anlagen*
  Bereits jetzt führt die „Eindeutschung“ des englischen Begriffs „Asset Management“ zu „Management von Anlagen“ zu Verwirrung, da ja parallel von „Kritischen Anlagen“ gesprochen wird und sich so Unklarheiten ob des Betrachtungsgegenstandes ergeben. Der verwendete deutsche Begriff ist ungebräuchlich, der englische Begriff „Asset Management“ daher zu präferieren.
- *Managed Service Provider*
  Eine weitere begriffliche Unschärfe führt zur Verunsicherung gerade im Maschinenbau. Die Definition der „Managed Service Provider“ (MSP) ist problematisch. Monitoring Services und Remote Access sind Standarddienstleistungen eines Großteils der Hersteller. Nach der aktuellen Begriffsbestimmung müsste ein Großteil des deutschen Maschinenbaus als besonders wichtige Einrichtungen eingestuft werden.
  Das gleiche Problem tritt auf, wenn eine Tochtergesellschaft eines Konzerns den anderen Konzerntöchtern IT-Dienstleistungen anbietet (und zwar ausschließlich). Nach aktueller Lesart wären sie damit MSP im Sinne des Gesetzes. Dies erscheint nicht sinnvoll, es sollte eine Klarstellung geben, dass von Ausfällen betroffene Kunden außerhalb der Konzernsphäre liegen.

Geschäftsführungsverantwortlichkeit

Die Formulierung des §38 im 3. Referentenentwurf war passender als die aktuelle. Aktuell wird gefordert, dass die Geschäftsführung die Maßnahmen umsetzt. In der Praxis (und früher auch passender formuliert) lässt die Geschäftsführung Maßnahmen umsetzen, lässt die Umsetzung überwachen und verantwortet diese.

Angesichts des bereits bestehenden Haftungsregimes ist es zielführend, dass das NIS2UmsuCG als Auffangregelung gilt, sofern keine entsprechende Managerhaftung vorgesehen ist.

Untersagung kritischer Komponenten (ehemalig §9b)

Losgelöst vom Inhalt wäre hier im Vorfeld eine Evaluation des bisherigen Procederes notwendig gewesen. Das bisherige und nun unverändert übernommene Verfahren war schon für einen Sektor sehr zeitfressend und aufwändig, bei vermuteter Verzehnfachung wird dies noch schlimmer und impraktikabel.

Konformitätserklärung §53

Dazu gibt es kein Pendant in NIS2. Der Mehrwert hier erschließt sich mir spätestens nach Verabschiedung des Cyber Resillience Acts nicht und es besteht die Gefahr nationaler Alleingänge, die bei der Industrie auf keinerlei Interesse stoßen.

4. Zur Person

Timo Kob ist Gründer und Eigentümer der HiSolutions AG, einem Beratungshaus für Cybersecurity mit derzeit rund 400 Mitarbeitern.

HiSolutions hält nicht nur die Rahmenverträge des BSI für

- die Erstellung von Sicherheitskonzepten der unmittelbaren Bundesverwaltung und
- die Durchführung von vom BSI angeordneten KRITIS-Tiefenprüfungen in den Unternehmen,

sondern auch des Landes Berlin für

- die Erstellung von Sicherheitskonzepten des Landes und der Bezirke

und kennt u. a. aus diesen Projekten den Sicherheitsstatus sowohl auf privatwirtschaftlicher Seite als auch aus Bund, Ländern und Kommunen.

Er selbst ist vom BSI akkreditierter IT-Grundschutzauditor und leitet darüber hinaus eines von zwei „CertLabs“ des BSI, in denen die Prüfung und Abnahme aller Grundschutzzertifizierungen durchgeführt werden.

Er ist Professor für Cybersecurity und Wirtschaftsschutz an der FH Campus Wien.

Er leitet die Bundesfachkommission Cybersecurity des Wirtschaftsrates der CDU, sitzt im Hauptvorstand sowie im Vorstand des Arbeitskreises Sicherheitspolitik des Bitkom und ist als Vertreter des VDMA im Vorstand des Arbeitskreises Cybersecurity des BDI.

Aus diesen Rollen heraus hat er an den jeweiligen Stellungnahmen der Verbände zum NIS2UmsuCG mitgearbeitet, deren Ergebnisse auch mit in diese Stellungnahme eingeflossen sind.