Bonn, 12.08.2020

AG KRITIS

Evaluation der Cyber-Sicherheitsstrategie für Deutschland 2016

Am 30. Juli 2020 bat das Bundesministerium des Innern, für Bau und Heimat um Mitwirkung der „Gesellschaft und Wirtschaft“ bei der Evaluation der Cyber-Sicherheitsstrategie 2016. Als Frist für Einreichungen beim Ministerium war der 7. August 2020 benannt, eine Fristverlängerung bis zum 14.08.2020 wurde der AG KRITIS allerdings zeitgleich gewährt. Als Basis der Evaluation diente der folgende Fragebogen:

Fragebogen

1. Welche Schwerpunktthemen und Ziele der CSS 2016 haben sich bewährt? Welche Verabredungen, Strukturen und Maßnahmen wirkten sich positiv auf die Zielerreichung aus?

- Da umgesetzte Maßnahmen meist in der Realisierungsphase umbenannt werden - und in der Strategie selbst auch keine Zuordnung vorgenommen wird - ist es äußert schwierig. die vorhandenen Erfolge zu finden oder zu bewerten. In Bezug auf "Die Fähigkeit zur Analyse und Reaktion vor Ort stärken" sind wir uns fast sicher, das hier das Mobile Incident Response Team des BSI gemeint sein muss - die im ITSiG2-Ref2 vorgesehene Vergrößerung begrüßen wir. Wir empfehlen darüber hinaus die hauptamtlichen, festangestellten Kräfte im MIRT durch eine ehrenamtliche Organisation ergänzen, die bei Katastrophen oder Großlagen zusätzlich aktiviert und mobilisiert werden können.

2. Welche Schwerpunktthemen und Ziele der CSS 2016 erachten Sie als erreicht bzw. für überholt und bedürfen nach Ihrem Kenntnisstand zukünftig weniger Beachtung?

- Themen der Verteidigungspolitik gehören nicht in eine Cybersicherheitsstrategie für Deutschland und sind eher im Weißbuch des BMVg zu berücksichtigen.
- Der Fokus auf Defensive und Cyberresilienz sollte gesetzt und klar hervorgehoben werden.

3. Welche Schwerpunktthemen und Ziele sind seit der Fortschreibung der CSS im Jahr 2016 aus Ihrer Sicht hinzugekommen und bedürfen einer zusätzlichen Erwähnung? Welche

Verabredungen, Strukturen und Maßnahmen können Staat, Gesellschaft und Wirtschaft festlegen und vereinbaren um die von Ihnen genannten Ziele zu erreichen?

- Stärkere fachliche Unabhängigkeit des BSI vom BMI.
- Das BSI stellt den Chief Information Security Officer (CISO) des Bundes.
- Der Cyber-Sicherheitsrat muss permanente Vertreter aus der Zivilgesellschaft mit einbeziehen als auch transparenter werden.
- Der Fachkräftemangel in der öffentlichen Verwaltung ist anzugehen. Starre Strukturen und unflexibles Handeln halten IT-Experten davon ab, innerhalb des Öffentlichen Dienstes aktiv zu werden.

4. Welche weiteren Änderungen an der CSS würden Sie begrüßen?

- Es sollte die tatsächliche Strategie bzw. die strategische Ausrichtung dargestellt werden. Derzeit entspricht die Strategie eher einer losen Sammlung von Handlungsfeldern und Maßnahmen ohne übergeordnete und strategische Zielsetzungen.
- Der CSS mangelt es an einer klaren Darstellung der nicht-militärischen Ziele und Betrachtungen. Darüber hinaus gibt es zunehmend Verwirrung über Kompetenzen und Zuständigkeiten zwischen Militär und öffentlicher Verwaltung. Hier benötigt es eine eindeutige Abgrenzung zum Militär.
- Eine Cybersicherheitsarchitektur in Deutschland, welche die Kernziele unterstützt und Komplexität reduziert. Damit einhergehend die dafür zwingend erforderliche stärkere inhaltliche Unabhängigkeit des BSI. Zuständigkeiten und Meldewege müssen transparent von Bund über Länder bis Kommunen für öffentliche und private Stellen konkret und transparent beschrieben werden.
- Hervorhebung von dringend erforderlichen Kernzielen "Defensiv statt Offensiv" und "Erhöhung der Cyberresilienz".
    - Dies soll im Gegensatz zu den Offensive-Strategien von zB USA und Israel stehen.
    - Eine solche progressive Positionierung kann auch als Vorreiterrolle innerhalb der EU dienen.
- Zwingende Harmonisierung der Kernziele mit der ENISA Strategie 2020 „A Trusted and Cyber Secure Europe“ und mit der „Security Union Strategie“ 2020 der Europäischen Kommission.
- Einfügen von Recovery-Strategien als wesentlicher Teil einer CSS. Wenn nicht - wie in den Energiesystemen der Ukraine 2015 - ein manueller Betrieb als Rückfallmöglichkeit sichergestellt werden kann, müssen Maßnahmen zur Orientierung an Resilienzphasen

(siehe Risk, Systems and Decisions 2019, Fig. 1.2): Plan - Absorb - Recovery – Adapt – festgeschrieben werden.

- Die Auswirkungen der Bestrebungen auf die Wirtschaft, Verschlüsselung durch Befugnisse zu schwächen, sind nicht ausreichend berücksichtigt. Jede Schwächung der Verschlüsselung als auch das Zurückhalten von Sicherheitslücke gefährdet Unternehmen wie auch den Staat selbst.
- Das Problem der Ransomware wächst weiter. Die Akteure müssen als Organisierte Kriminalität bekämpft werden, Ihre Aktionen müssen in der Finanzwelt beobachtet und unterbunden werden. Eine Vermischung mit militärischen Themen ist nicht zielführend.

5. Welche Anregungen haben Sie für den anstehenden Fortschreibungsprozess?

- Wir schließen uns den veröffentlichten Empfehlungen und der Antworten der Stiftung neue Verantwortung (SNV) auf diese Frage vollumfänglich an. (https://www.stiftung-nv.de/de/publikation/evaluation-der-cyber-sicherheitsstrategie-fuer-deutschland-2016)
- Wir möchten insbesondere betonen, dass zur Fortschreibung der Strategie eine Reihe von interdisziplinären, inklusiven Workshops mit Teilnehmern aus Politik, Wissenschaft, der Zivilgesellschaft und der Industrie unumgänglich sind, um verlorenes Vertrauen zurückzugewinnen und die volle Strahlkraft einer neuen Strategie zu entfalten. Die Cyberresilienz Deutschlands kann nur durch Integration aller Beteiligten gesteigert werden.
- Die Transparenz des Prozesses muss gegenüber der Öffentlichkeit sichergestellt werden.

Kommentare und Anmerkungen zu einzelnen Abschnitten

Handlungsfeld 1 - Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

„Digitale Kompetenz bei allen Anwendern fördern“ (S.14)

- Wesentlich für die Entwicklung von Kompetenzen bei Anwendern, aber auch Betreibern und Entwicklern von KRITIS, ist die Integration von Cybersicherheit in die Ausbildung. Die CSS muss insbesondere hier einen Schwerpunkt setzen, um Konzepte und Mindeststandards für Cybersicherheit in verschiedene Ausbildungswege einführen.

„Voraussetzungen für sichere elektronische Kommunikation und sichere Webangebote schaffen“ (S. 15)

- Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung widersprechen sich. Ermittlungsinteresse der Sicherheitsbehörden ist nachvollziehbar, muss aber in jedem Fall maximal grundrechtsschonend und Datensparsam realisiert werden. Das IT-Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme muss stärker als bisher beachtet werden. Wenn der Staat hier Fehler macht und nicht verhältnismäßig agiert, verliert er bei digitalen Fragen das Vertrauen der Bürger gesamtstaatlich. Eine Ressorttrennung gibt es im Kopf der Bürger nicht - das alleinige Vorhandensein der Möglichkeit einer QTKÜ-Software in Behördenhand wirkt sich direkt auf das Vertrauen der Bürger gegenüber allen Digitalprojekten des Bundes aus.

Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft

„Kritische Infrastrukturen sichern“ (S. 22)

- Grundsätzlich ist festzustellen, dass die Tiefe und die konkrete Ausprägung dieses Punktes einer stärkeren Detaillierung bedarf, sodass relevante Maßnahmen und Konzepte zur Steigerung der Cyberresilienz abgeleitet werden können.
- Grundsätzlich sind die strategischen Ziele in diesem Abschnitt gut und richtig, dies ist allerdings kein Alleinstellungsmerkmal der CSS, sondern eher der Arbeit des UP KRITIS und dem UP Bund zu verdanken.

- Die Erhöhung der Cyberresilienz kritischer Infrastrukturen ist vorzunehmen, um Versorgungsausfälle und -engpässe als auch deren Auswirkungen möglichst kurz und gering zu halten.
- Die Personalausstattung der für KRITIS (insgesamt, aber auch einzelne Sektoren) relevanten Abteilungen und Referate im BSI und KRITIS-relevante Abteilungen im Bundesamt für Katastrophenhilfe und Bevölkerungsschutz, sowie die relevanten Abteilungen und Referate in der Bundesnetzagentur sind zu stärken.
- Der Staat muss kooperativ mit KRITIS-Betreibern mehr verpflichtende Präventionsmaßnahmen festlegen als auch Meldewege und Reaktionspflichten im Schadens- oder Krisenfall für KRITIS-Betreiber konkretisieren.
- Incentivierung der Erhöhung von Redundanzen und Puffern in kritischen Infrastrukturen statt fortwährender Steigerungen der Wirtschaftlichkeit des Betriebs selbiger.
- "Unternehmen von hoher gesellschaftlicher Relevanz" sind weder KRITIS noch KRITIS-nahe.
- Untersuchung, ob über-sektorale KRITIS-Betreiber kaskadierte und übergeordnete Versorgungsausfälle bewirken können, wie z.B. durch einen kommunalen Betreiber, der Energie, Wasser und Transport-Dienstleistungen aus einer Hand bereitstellt.
- Evaluierung der KRITIS Schwellenwerte als auch deren Wirkung und individuelle Anpassung je Sektor.
- Schutz von KRITIS braucht ein unabhängiges BSI. amit KRITIS effektiv geschützt werden können, braucht es eine Meldepflicht für Sicherheitslücken. Das zugehörige Meldewesen benötigt eine hohe Vertrauensstellung damit u.A. alle IT-Störfälle, Prüfberichte und Mängellisten gemeldet werden können, ohne das Gefahr oder Verdacht besteht, dass Inhalte dieser Meldungen in die Hände von Sicherheitsbehörden gelangen können.

„Unternehmen in Deutschland schützen“ (S. 22)

- Der Umfang der "Sensiblisierungs- und Unterstützungsmaßnahmen" (insb. bezogen auf KRITIS) hat zwar zugenommen, die Zielsetzung und konkrete Unterstützungsmaßnahmen für Unternehmen abseits der Allianz für Cybersicherheit und BSI für Bürger muss jedoch überdacht werden. Dies erfordert zusätzliches Personal in einem unabhängigen BSI.
- Unterstützungsdienstleistungen zur "Erreichung des notwendigen Sicherheitsniveaus" scheitern zum einen an der konkreten Definition des gewünschten Sicherheitsniveaus und zum anderen an den verfügbaren Maßnahmen seitens des Bundes.
- Die Unterstützungsdienstleistungen beschränken sich weitestgehend auf generische Hilfestellungen. Konkrete Lösungen für KRITIS-Betreiber - abseits von Informationsmaterial - sind noch ausstehend.

- Der Schutz der privatwirtschaftlichen Unternehmen und KRITIS-Betreiber bedeutet auch die klare Ablehnung eines "Vulnerability Equity Process" als auch das proaktive und sofortige Melden von Schwachstellen an Unternehmen, sobald diese bekannt werden. Den KRITIS-Betreibern sollte schnellstmöglich eine Behebung von Schwachstellen ermöglicht werden, ohne das politische Gremien die Behebung verzögern.

„Die deutsche IT-Wirtschaft stärken“ (S. 23)

- Der Verteidungssektor und die Rüstungsindustrie sind nicht oder nur marginal indirekt für das Allgemeinwohl zuträglich. Sie sind daher im Rahmen einer "strikt defensiven Cybersicherheitsstrategie" nicht zu berücksichtigen.
- Open Source für KRITIS fördern, um mehr Transparenz und Verbesserung bei der Anpassungsfähigkeit und Reaktionsfähigkeit zu erreichen. Zur Ermöglichung von Anpassung an Quellcode in Krisenfällen muss zudem die vollständige Entwicklungskette verfügbar und getestet sein - was bei zukünftigen strategischen Entscheidungen zu berücksichtigen ist.

„Mit den Providern zusammenarbeiten“ (S. 24)

- Jeglicher Zugriff durch den Staat über Telekommunikationsdienstleister auf Kritische Infrastrukturen darf nicht erfolgen. Auch eine Ausleitung bzw. Manipulation von Telekommunikations-Daten an bzw. durch Sicherheitsbehörden darf nicht erfolgen.
- Ein Aufbau von Sensorik-Netzwerken zur Anomalieerkennung kann aufgrund der Sensibilität der Informationen in einem solchen Netzwerk nur eine Aufgabe sein, die von einem unabhängigen BSI übernommen werden kann.

„Eine Plattform für vertrauensvollen Informationsaustausch schaffen“ (S. 25)

- Verbesserung der Fehlerkultur, um den Austausch über Herausforderungen zu fördern. Dies erfordert eine vertrauenswürdige Stelle - wie ein unabhängiges BSI - welches keine Zuarbeit zu offensiven Technologien und Maßnahmen leistet.

Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

„Das Nationale Cyber-Abwehrzentrum weiterentwickeln“ (S. 28)

- Aktuelle Maßnahmen im ITSiG2-Ref2 zeigen, dass Meldungen über Vorfälle neuerdings an das BKA gehen sollen - dies ist eine Schwächung des NCAZ. Richtig wäre, wenn Meldungen über Cybervorfälle aller Art an das NCAZ gehen würden - wo das BKA auch vertreten ist und im Rahmen seiner begrenzten Zuständigkeit an der Vorfallsbearbeitung mitwirken kann.
- Auch im NCAZ muss weiterhin konsequent eine rein defensive Cybersicherheitsstrategie verfolgt werden.

„Die Fähigkeit zur Analyse und Reaktion vor Ort stärken“ (S. 29)

- Die hohe Anzahl an möglichen Stellen, die im Krisenfall potentiell verantwortlich sein können, behindert die Bearbeitung von - meist unübersichtlichen - Vorfällen vor Ort erheblich. Strukturen, Verantwortlichkeiten und Kommunikationsprozesse müssen klar und deutlich aufgestellt und abgegrenzt werden. Klare Kompetenztrennung und lokale Ansprechpartner sind wesentlich für eine Stärkung der Reaktionsfähigkeit "vor Ort".
- Regionale Stellen und lokal verfügbare Kräfte müssen deutlich ausgebaut werden. Die großen, zentral strukturierten Stellen des Bundes (MIRT, QRF, MCT, MAD, BND, IRT) können diese Ressourcen vor Ort nicht ausreichend für den Cyber-Notfall vorhalten. Eine wesentliche Stärkung stellt die Schaffung einer auf freiwilligen Reaktionskräften basierenden Organisation dar, um die Verfügbarkeit im breiten Raum zu gewährleisten. Die AG KRITIS hat hierzu eine erste Fassung für das sog. Cyber-Hilfswerk entwickelt. (https://ag.kritis.info/chw-konzept/)
- Die Kommunikation zwischen staatlichen und nicht-staatlichen, regionalen Stellen muss weiter ausgebaut werden, um lokale Reaktionen überregional effizient abstimmen zu können.

„Strafverfolgung im Cyber-Raum intensivieren“ (S. 30)

- Eine strikte Trennung von Stellen die Cybervorfälle behandeln und Sicherheitsmeldungen kommunizieren und Stellen mit operativen Aufgaben in der Strafverfolgung, i.e. welche ggf. die Nutzung von digitaler Überwachung und Eingriffen erlaubt, ist notwendig um die Effektivität der mit Cybersicherheit beauftragten Stellen nicht zu verlieren. Sicherheitslücken dürfen nicht von Sicherheitsbehörden zurückgehalten werden, sondern

müssen - z.B. an ein unabhängiges BSI - gemeldet werden, so das diese unverzüglich an Hersteller weitergereicht und abgestellt werden können.

„Cyber-Spionage und Cyber-Sabotage effektiv bekämpfen“ (S. 31)

- Die CSS bietet vorwiegend eine technische und fachliche Analyse sowie Bewertung der gegen Bundesbehörden und sonstige Ziele gerichteten Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund (Beobachtung/Analyse). Die Angriffsziele "Spionage" und "Sabotage" sollten keinen eigenen Punkt in einer CSS benötigen, sondern Teil der primären Ziele der Strategie sein.

„Ein Frühwarnsystem gegen Cyber-Angriffe aus dem Ausland“ (S. 32)

- Die auf diese Weise gesammelten Erkenntnisse müssen unverzüglich und vollständig der zuständigen Stelle, nämlich dem NCAZ im BSI, zur Verfügung gestellt werden. Der BND darf diese Informationen nicht für sich behalten, da eine Zuständigkeit des BND für einen so festgestellten Vorfall nur in wenigen Einzelfällen gegeben ist - in allen anderen Fällen fällt die Zuständigkeit der Vorfallsbearbeitung auch den anderen staatlichen Stellen im NCAZ zu.

„Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)“ (S. 32)

- Die parlamentarische Kontrolle aller Sicherheitsbehörden - insbesondere mit Geheimanteilen - muss intensiviert werden. Die Cybersicherheit kann kein demokratiefreier Raum sein.

„Verteidigungsaspekte der Cyber-Sicherheit stärken“ (S. 33)

- Cybersicherheit kann nicht durch offensive Maßnahmen gestärkt werden. Die wechselseitigen Abhängigkeiten zwischen Systemen und Entwicklungsprozessen, sowie die spezifischen Eigenschaften von Cyber-"Waffen", verbieten jede offensive Operation. Offensive Cybertechnik eignet sich weder zur Abschreckung noch zur Vergeltung und verbietet sich aufgrund der zwangsläufigen Nutzung und Gefährdung ziviler Ziele als mögliche Kollateralschäden. Eine CSS muss deshalb ausschließlich defensiv ausgelegt sein, wenn sie zur Erhöhung der Cybersicherheit beitragen soll.
- Eine wesentliche Beteiligung militärischer Kräfte, wie der Bundeswehr, an einer Cyber-Verteidigung ist insofern schwierig, als dass eine Separierung interner und externer Sicherheit schwer ist. Die Verteidigung kann nur auf den zivilen Anlagen im Inland stattfinden, was eine Beteiligung der Bundeswehr nur im Rahmen der Amtshilfe erlaubt.
- Da die notwendigen Kompetenzen zur defensiven Cybersicherheit nicht zum Kompetenzbereich der Bundeswehr gehören, dafür aber an anderen Stellen bereits

verantwortlich verankert sind, ist es nicht ratsam solche Fähigkeiten über den "Selbstschutz" hinaus in der Bundeswehr aufzubauen.

„CERT-Strukturen in Deutschland stärken“ (S. 34)

- Neben dem BSI CERT-Bund als nationales CERT existieren viele nationale und private CERTs. Eine Vernetzung wurde geplant und teilweise umgesetzt. Es bestehen aber weiterhin Unklarheiten über Kompetenzen und Verantwortlichkeiten.
- Die Verantwortungsbereiche und Kompetenzprofile müssen von den lokalen bis zu den nationalen, europäischen und internationalen Stellen klar definiert und insbesondere auf der lokalen Ebene transparenter kommuniziert werden. Bessere Einbindung kommunaler und Landes IT-Sicherheitsakteure untereinander wie auch klare Meldewege und Zuständigkeiten für operative Fragen im Normalbetrieb aber auch im Falle einer Krise für Kommunen, Städte, Landkreise müssen deutlich verbessert werden.

„Ressourcen einsetzen, Personal gewinnen und entwickeln“ (S. 37)

- In der Strategie steht: "Es wird darum gehen, die Arbeitgeberattraktivität des Öffentlichen Dienstes offensiver darzustellen und die bestehenden dienst- und tarifrechtlichen sowie monetären Rahmenbedingungen zielgerichtet zu nutzen." - Die AG KRITIS stellt dazu fest: Die zielgerichtete Nutzung reicht nicht aus - das Laufbahnrecht und die starren Strukturen des öffentlichen Diensts müssen reformiert werden. Die öffentliche Verwaltung muss in die Lage versetzt werden, vergleichbare Gehälter wie die freie Wirtschaft anbieten zu können. Auch die traditionelle Arbeitsweise ist wenig attraktiv. Es braucht auch eine Reform, um zu moderneren, flexibleren Modellen der Arbeitsorganisation zu kommen.

Handlungsfeld 4 – Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

„Eine wirksame europäische Cyber-Sicherheitspolitik aktiv gestalten“ (S. 40)

- In diesem Teil der CSS fehlt der explizite Wille, die deutsche Cybersicherheitsstrategie mit europäischen Strategien zu harmonisieren. Eine angestrebte Vorreiterrolle in diesem Bereich entbindet nicht von der Pflicht, unsere europäischen Vereinbarungen innerstaatlich zu fördern und harmonisch in die deutschen Strategien einzubinden.

„Die Cyber-Verteidigungspolitik der NATO weiterentwickeln“ (S. 40)

- Die Offensiv-Fähigkeiten der NATO, insbesondere der USA, widersprechen den Zielen der CSS. Deutschland sollte deshalb im Rahmen der Nato auf eine strikt defensive Cyber-Sicherheitsstrategie hinwirken.

„Cyber-Sicherheit international aktiv mitgestalten“ (S. 41)

- Deutschland muss bei der Entwicklung und Umsetzung einer strikt defensiven Cybersicherheitsstrategie die Vorreiterrolle einnehmen, welche die Cyberresilienz stärkt.
- Verbot der Geheimhaltung von Sicherheitslücken und Vorbildstellung in der Behebung von erkannten Schwachstellen anstreben.
- Verbot oder Ächtung der Entwicklung von Cyberwaffen ähnlich wie vorhandene ABC-Waffen-Verbote. Die möglichen Kollateralschäden von Cyberwaffen können den Kollateralschäden von ABC-Waffen entsprechen oder diese übersteigen. Eine gleichwertige Behandlung wie ABC-Waffen im internationalen Diskurs durch internationale Verträge ist notwendig.

Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building) (S. 42)

- Deutschland hat die Chance, sich durch die Umsetzung des "Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen" als Vorreiter zu positionieren. Ein so geschaffenes Cyber-Hilfswerk kann auch als Leuchtturm bei der Unterstützung des Cyber Capacity Building im Rahmen der Entwicklungshilfe als Best-Practice-Beispiel genutzt werden. Vergleichbar mit der Strahlkraft des Auslands-THW kann das Cyber-Hilfswerk zu einer Institution mit Vorbildfunktion werden.