GESELLSCHAFT
FÜR INFORMATIK

Berlin, 14. April 2021

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zu den Eckpunkten für die Cyber-Sicherheitsstrategie 2021

des Bundesministeriums des Inneren, für Bau und Heimat (BMI)

Ad 3.1. Handlungsfeld 1:

> *S. 7: „soll in der CSS 2021 das bereits in der CSS 2016 benannte Ziel „Wissenschaft und Forschung im IT-Sicherheitsbereich vorantreiben“ um Aspekte der Ausbildung und des Wissenstransfers ergänzt und hinsichtlich der zu behandelnden Themen und einzubeziehenden Akteure geschärft werden.“*

Die Gesellschaft für Informatik unterstützt diese Ergänzung und regt an, eine entsprechende Sensibilisierung für Sicherheitsfragen und den Wissenstransfer bereits frühzeitig in der Ausbildung zu verankern, etwa bereits in der Schule. Dies würde helfen, einerseits die Medienkompetenz allgemein zu stärken und andererseits die Risikowahrnehmung der Heranwachsenden frühzeitig zu entwickeln und den Selbstschutz zu stärken. Hierfür könnten geeignete Formate mit Partnern entwickelt und umgesetzt werden.

Ad 3.2. Handlungsfeld 2:

Ergänzend zu den genannten Eckpunkten sollte die CSS 2021 das Thema Internet of Things (IoT) und Verbraucherschutz explizit adressieren. Die Frage (fehlender) Update-Fähigkeit von IoT-Produkten stellt ein wachsendes Problem der IT-Sicherheit dar. Daneben stellt die fehlende Update-Fähigkeit auch ein Datenschutz- sowie ein Nachhaltigkeits- und Umweltproblem dar und muss daher mit einem kohärenten Ansatz adressiert werden.

Ad 3.3. Handlungsfeld 3:

> *S. 8: „In der CSS 2021 sollen der vertrauensvolle Austausch, das zeitnahe Schließen von Sicherheitslücken und die Abwehr von Cyber-Angriffen als unverzichtbare Bausteine des gemeinsamen Auftrags von Staat und Wirtschaft zur Erhöhung der Cyber-Sicherheit Deutschlands adressiert werden.”*

Um das zeitnahe Schließen von Sicherheitslücken zu befördern, sollte das BSI explizit dazu verpflichtet werden, ihm bekannt gewordene Sicherheitslücken im Sinne einer Responsible Disclosure zu veröffentlichen. Dies ist unverzichtbar für das Sicherheitsniveau von Unternehmen und Einzelpersonen und stärkt zudem das Vertrauen in die staatlichen Stellen. Im Übrigen verweisen wir auf unsere nachfolgenden Ausführungen.

> *S. 10: „Um die effektive Zusammenarbeit zwischen Bund und Ländern weiter zu vertiefen, wird angestrebt, das BSI in seinem bestehenden Aufgabenbereich zu einer Zentralstelle im Bund-Länder-Verhältnis auszubauen und somit – neben dem BKA im Polizeiwesen und dem BfV im Verfassungsschutzverbund – zur dritten Säule einer föderal integrierten Cyber-Sicherheitsarchitektur weiterzuentwickeln."*

Die Weiterentwicklung des BSI zur Zentralstelle unterstützen wir. Gleichzeitig sollte die Behörde weisungsunabhängig vom Bundesministerium des Inneren, für Bau und Heimat (BMI) werden, um sich ohne Interessenskonflikte dem Schutz der IT-Sicherheit widmen zu können. Interessenskonflikte sehen wir insbesondere zwischen der Aufgabe, die Schutzfähigkeit deutscher IT-Systeme zu erhöhen und der Befugnis, ihm bekannte oder gekaufte Sicherheitslücken nicht zu veröffentlichen, weil andere Sicherheitsbehörden wie BKA, BfV etc. diese ausnutzen wollen. In Folge dessen kann das Sicherheitsniveau von Unternehmen und Privaten stark eingeschränkt werden.

> *S. 12: „Die bereits in der CSS 2016 festgehaltene Rolle des Nationalen Cyber-Sicherheitsrats (NCSR) als höchstrangig besetztes Gremium in der deutschen Cyber-Sicherheitsarchitektur gilt es zu konkretisieren"*

Wie u.a. die Übersicht der Stiftung Neue Verantwortung (SNV) zu der deutschen Cybersicherheitspolitik zeigt[1], sind in den letzten Jahren entstanden – und entstehen weiterhin – zahlreiche Beiräte, Räte, Kommissionen, Expertenkreise (der Bundesregierung, der Ministerien, des BSI etc.) mit dem Schwerpunkt IT-Sicherheit, Cybersecurity, Informationssicherheit, etc. Die Anfragen bei BSI und BMI haben bestätigt, dass keine Übersicht über die Gremien, ihre Zuständigkeiten, Arbeitsergebnisse oder etwaige Mitglieder besteht. Sie sind verschiedenen Ressorts unterstellt und haben oft sich überschneidende Zielsetzungen und Aufgaben. Mit der wachsenden Popularität des Themas entsteht bisweilen der Eindruck einer Hypertrophie an Expertenkreisen und Experten für Cyber-Sicherheit[2].

Bevor die Rolle des NCSR „konkretisiert" wird, sollte daher ein Überblick dieser Gremien erstellt und ihre Zuständigkeiten auf Überschneidungen und Synergien hin untersucht werden. Etwaige Redundanzen sollten im Sinne der Effektivität und Effizienz aufgedeckt und behoben werden, die Beziehungen der Gremien gen NCSR transparent konkretisiert, die Aufgaben und Sub-Aufgaben entsprechend verteilt und die Reportingwege geklärt werden.

---

[1] https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik
[2] https://www.frankfurter-hefte.de/artikel/sommer-der-digitalraete-2728/

Auf dieser Basis können anschließend „Vorschläge erarbeitet“ werden, „wie der NCSR seine Bündelungsfunktion als Multi-Stakeholder Gremium weiterentwickeln und bestmöglich nutzen kann, um die vielfältigen, auf die Stärkung der Cyber-Sicherheit in Deutschland gerichteten Akteure und Aktivitäten zu unterstützen.“ (S. 12). Ein weiteres Ziel wäre, auf Grundlage dieser Analyse bestimmte Aufgaben von den Gremien an den NCSR zu übertragen, die Gremien zu entschlanken und ihre Anzahl zu reduzieren.

Ad 4 (4.1 und 4.2) Definition, Umsetzung und Controlling der Cyber-Sicherheitsstrategie

Anstelle des betriebswirtschaftlichen Controllings scheint eine Kombination aus Monitoring und Audit geeigneter, um das Ziel der Erfolgsmessung der CSS 2021 zu erreichen. Zwecks Erfolgsmessung der strategischen Ziele sind Key Goal Indicators (KGIs) zu definieren. Umsetzung kann auf Grundlage der noch zu definierenden Key Performance Indicators (KPIs) oder Metriken gemessen und gesteuert werden.

Im Rahmen des Monitorings sollte eine laufende Überwachung der (strategischen und operativen) Zielerreichung auf Grundlage der o.g. Kennzahlen erfolgen. Das Monitoring kann dabei direkt beim BMI erfolgen, durch Erfassung intern generierten Kennzahlen sowie Abfrage bzw. Meldung der vereinbarten Kennzahlen durch die betroffenen Ressorts an das BMI (vgl. 4.1).

Das Audit bzw. die Prüfung (vgl. 4.2) sollte dagegen nicht vom BMI, sondern nach dem Vorbild einer Revision, durch eine unabhängige, objektive, dritte Stelle erfolgen, der sowohl die Ergebnisse des Monitorings als auch ausführliche Informationen zur Beurteilung und Bewertung der Erfolge und/oder Fortschritte der Strategie (Umsetzung und Grad der Zielerreichung) zur Verfügung zu stellen sind. Das Ergebnis der Prüfung, Feststellungen, Empfehlungen oder Hinweise, wird in einem Bericht zusammengefasst.

In dem unter Punkt 4 zusammengefassten Abschnitt kann auf erprobte Instrumente und Methoden aus dem Kennzahlenmanagement, der IT-Prüfung und -Revision und des Monitorings zurückgegriffen werden, wie bspw. die Methodik der Ordnungsmäßigkeitsprüfung (subsumiert und 4.2. „strategisches Controlling“), der Wirksamkeitsprüfung (ebenda, „operative Umsetzung“)[3], sowie auf die Libraries mit KPIs und KGIs aus den gängigen Standards zur Informationssicherheit[4].

Es wäre ebenfalls ratsam, die Ergebnisse der regelmäßigen Audits zur Umsetzung der CSS 2021 bspw. in dem jährlich erscheinenden Lagebericht des BSI zu publizieren und der breiten Öffentlichkeit zugänglich zu machen.

GESELLSCHAFT
FÜR INFORMATIK

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.

[3] Sowa, A. (Hrsg.) 2020. IT-Prüfung, Datenschutzaudit und Kennzahlen für die Sicherheit. Neue Ansätze für die Arbeit der IT-Revision. Springer Verlag.
[4] U.a. ISO/IEC 27004, NIST SP 800-55, ETIS Information Security Working Group. 2012. „ETIS Library of Information Security KPIs". Reference document for the ETIS community.