Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Bundesministerium für Wirtschaft und Klimaschutz
Scharnhorststraße 34-37
10115 Berlin

Bundesministerium des Innern und für Heimat
Alt-Moabit 140
10557 Berlin

Bundesministerium der Justiz
Mohrenstraße 37
10117 Berlin

Bundesministerium für Gesundheit
Rochusstraße 1
53123 Bonn

Bundesministerium für Digitales und Verkehr
Invalidenstraße 44
10115 Berlin

Bundesministerium für Bildung und Forschung
Heinemannstraße 2
53175 Bonn

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat25@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 18.09.2023
GESCHÄFTSZ. 25-170/024#1249

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

79572/2023

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

BETREFF **Schwachstellen schließen – Sicherheit stärken**

Sehr geehrte Damen und Herren,

im aktuellen Referenten-Entwurf zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vom 03.07.2023 wird der Umgang mit Schwachstellen – also mit Sicherheitslücken, durch deren Ausnutzung sich Dritte unbefugt Zugang zu IKT-Produkten oder -Diensten verschaffen bzw. diese beeinflussen können – nicht hinreichend geregelt. Es fehlt eine Vorschrift zur konsequenten und sofortigen Schließung aller Schwachstellen. Der Weg von der Detektion einer Schwachstelle bis hin zu ihrer Schließung muss jedoch klar vorgezeichnet werden. Die anstehende Neufassung des BSI-Gesetzes bietet hierzu die Gelegenheit. Denn Datenschutz und IT-Sicherheit sind in der modernen Informationsgesellschaft eng verzahnt, weshalb ich auch aus der Datenschutzperspektive die Wichtigkeit dieses Themas betonen möchte.

Hier wird die Chance verpasst, die beabsichtigte Stärkung der IT-Sicherheit in Deutschland und der Rechte der Bürgerinnen und Bürger konkret zu verankern. Der aktuelle Koalitionsvertrag sieht solche Maßnahmen zur Stärkung explizit vor:

> *„Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. Wir führen ein Recht auf Verschlüsselung, ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, und die Vorgaben „security-by-design/default“ ein.“*

Durch das klare Vorzeichnen des Weges von der Detektion einer Schwachstelle bis hin zu ihrer Schließung wird das Vertrauen der Bürgerinnen und Bürger in digitale Infrastrukturen und Dienste gestärkt. Gleichzeitig wird durch den konkreten Einsatz für die Behebung von Schwachstellen die IT-Sicherheit in Deutschland insgesamt und auch die deutsche Wirtschaft gestärkt, indem eingesetzte IT-Produkte keine bekannten, aber geheim gehaltenen Schwachstellen enthalten.

Sicherheitslücken schließen, sobald sie bekannt werden: Diese Position ist unter Expertinnen und Experten aus dem Bereich IT-Sicherheit unstrittig und wird auch in Sachverständigenanhörungen immer wieder vorgetragen, wie sich unter anderem in der 27. Sitzung des Ausschusses für Digitales am 25. Januar 2023 gezeigt hat.[1]

[1] Siehe: https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/928388-928388.

Eine Geheimhaltung von Schwachstellen ist grundsätzlich genauso problematisch wie ein exklusiver Zugriff auf diese. Bestehende Schwachstellen können von anderen Angreifenden, Forschenden, feindlichen Nachrichtendiensten, ausländischen Polizeibehörden etc. gefunden und ebenfalls ausgenutzt werden. Legitime und illegitime Akteure beobachten zu jeder Zeit den Cyberraum und versuchen zu erkennen, ob (unbekannte) Schwachstellen ausgenutzt werden, damit sie diese missbrauchen oder auch schließen können. Das Auffinden der Schwachstellen ist grundsätzlich für alle Akteure und jederzeit möglich.

Schwachstellen zurückzuhalten führt weltweit zu erheblichen Gefahren für alle Anwenderinnen und Anwender von betroffenen IT-Produkten. Allein die Menge an verarbeiteten Daten, insbesondere mit Personenbezug, bedeutet eine sehr hohe Zahl Betroffener und Gefährdeter, ob bei Bürgerinnen und Bürgern, öffentlichen und nicht-öffentlichen Stellen oder auch bei der Bundesregierung und -Verwaltung selbst.

Gleichzeitig sorgt eine unklare Gesetzeslage dafür, dass Sicherheitsforschende zögern, entdeckte Schwachstellen zu melden, etwa, weil sie befürchten, dass entdeckte Lücken für Sicherheits- und Strafverfolgungsbehörden offengehalten werden könnten. Solche Chilling Effects gefährden die IT-Sicherheit massiv. Hier kann nur durch klare gesetzliche Vorgaben das Vertrauen dieser wichtigen Community gestärkt werden.

Aus meiner Perspektive als BfDI ist eine intakte, sichere und vertrauenswürdige IT-Landschaft von herausragender Bedeutung. In unserer bereits stark vernetzten und zunehmend digitalen Gesellschaft sind die Vertraulichkeit, Integrität und Verfügbarkeit von IT-Systemen zur Grundlage des freien Handelns geworden. Eine freie Entfaltung der Persönlichkeit erfordert sichere digitale Kommunikationsmittel und geschützte digitale Räume, in denen die freie Willensbildung stattfinden kann, wie es auch durch das Bundesverfassungsgericht bei der Entwicklung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betont wurde. Diese können nur vom Staat garantiert werden. Einen nachhaltigen Effekt auf die Verfügbarkeit von IT-Systemen hatten die Angriffe, die unter „Wannacry“ und „Notpetya“ bekannt sind. Diese basierten auf Schwachstellen, die von der NSA geheim gehalten wurden. Mit einem Leak der NSA-Angriffswerkzeuge wurden diese Sicherheitslücken bekannt und missbraucht. Die Folgen sowohl der direkten Angriffe als auch der Schäden, die durch die Verletzung oder den Verlust personenbezogener Daten entstanden sind, trafen letztlich Unternehmen und die Bürgerinnen und Bürger – nicht die anvisierten Überwachungssubjekte.

Bitte setzen Sie sich ebenfalls für das konsequente schließen von Sicherheitslücken durch staatliche Stellen ein.

Mit freundlichen Grüßen

Ulrich Kelber