Eingangsstatement Hearing NIS-2 Gesetz

Rede gehalten von Sebastian Kneidinger (Policy Advisor, epicenter.works)

Sehr geehrte Damen und Herren. Im Namen der unabhängigen Datenschutz-NGO epicenter.works bedanke ich mich herzlich für die Einladung.

Wie einige prominente Fälle in den letzten Jahren gezeigt haben, besteht in unserem Land ein dringender Nachholbedarf in Fragen der Cybersicherheit. Ein wichtiger Baustein dazu ist die Umsetzung der NIS-2-Richtlinie. Die Vorteile dieser Richtlinie können nur mit einer durchdachten und zielgerichteten Umsetzung realisiert werden. Der vorliegende Entwurf scheitert an diesen Anforderungen und sollte deshalb grundlegend überarbeitet werden.

Die Kritik von uns und anderen Stakeholdern aus der Begutachtung kann man auf folgende 4 Punkte reduzieren:

1.) Konstruktionsfehler: Ausgestaltung der nationalen Cybersicherheitsbehörde
2.) Überschießende Kompetenzen und Befugnisse beim Innenministerium
3.) Verpasste Chance: Schutz der verantwortungsvollen Offenlegung von Schwachstellen
4.) Überschießende Datenverarbeitungs- und Übermittlungskompetenzen

Erster Punkt: Konstruktionsfehler der nationalen Cybersicherheitsbehörde

- Die Ansiedlung beim Innenministerium führt zwangsläufig zu einem Zielkonflikt: Das notwendige Vertrauen für gute Zusammenarbeit von betroffenen Unternehmen und Sicherheitsforschung wird immer mit der Befürchtung der individuellen Strafverfolgung und allgemeinen Gefahrenabwehr zu kämpfen haben. Strafverfolgung bzw. allgemeine Gefahrenabwehr wird beim BMI immer Vorrang vor der allgemeinen IT-Sicherheit des Landes haben. Einen solchen Zielkonflikt sehen nicht nur wir, sondern z.B. auch der ehemalige CIO des Saarlandes im Rahmen der öffentlichen Anhörung im Deutschen Bundestag.

- Bereits bisher mangelnde Personalausstattung: Es ist kein Geheimnis, dass der öffentliche Dienst Schwierigkeiten hat, IT-Spezialisten als Mitarbeiter zu gewinnen. Dieses Problem hat auch der Rechnungshof kritisiert. Das mag an den Gehältern liegen, die in der Privatwirtschaft viel höher sind. Wir wissen, dass es hier erste

Bemühungen gibt, aber mit der vorliegenden Konstruktion bleibt auch die kulturelle Frage. Gute Hacker werden nicht beim Innenministerium arbeiten wollen, in einer unabhängigen Cybersicherheitsbehörde aber sehr wohl. Lernen wir von unseren Erfolgen und nehmen uns die Konstruktion ähnlich der KommAustria und RTR GmbH als Vorbild.

- Mangelnde Einbindung von Wissenschaft, Zivilgesellschaft und Wirtschaft: Wir haben viel Expertise zu IT-Sicherheit in Österreich, aber anstatt sie miteinzubeziehen, finden sich diese Akteure mit kritischen Stellungnahmen im Begutachtungsverfahren. Cyber Security ist eine Gemeinschaftsleistung. Gerade angesichts hybrider Bedrohungsszenarien, Stichwort Russland. Als positives Beispiel kann hier Italien genannt werden, das ein Technical Scientific Advisory Board mit Vertretern aus Wissenschaft, Wirtschaft und Interessenvertretung der IT-Sicherheitsexperten eingerichtet hat.

Der Konstruktionsfehler des NIS2-Gesetzes wird auch im europäischen Vergleich deutlich. Die führenden Staaten setzen auf andere Konstruktionen: In Deutschland gibt es mit dem Bundesamt für Sicherheit in der Informationstechnik ein eigenes Amt. In Litauen sind diese Kompetenzen beim Verteidigungsministerium angesiedelt. Unsere Empfehlung lautet, eine unabhängige Stelle - nach dem Vorbild der KommAustria - zu schaffen.

Zweiter Punkt: Überschießende Kompetenzen und Befugnisse der neuen Cybersicherheitsbehörde

- Die alleinige Ernennung des nationalen CSIRT durch das Innenministerium ist problematisch. Das nationale CSIRT ist die zentrale Anlaufstelle für Cyber-Notfälle in Österreich und hat daher eine herausragende Stellung. Es ist wichtig, dass die Ernennung des CSIRT daher gemeinsam mit anderen Ressorts erfolgt. Nur wenn die Stakeholder in Österreich Vertrauen zu dieser Stelle haben, kann sie funktionieren.

- Die Einsichts- und Kontrollrechte sind überschießend. Diese neuen Kompetenzen sind ausufernd und viel zu ungenau bestimmt. Der Entwurf vom 13. Juni brachte zwar gewisse Verbesserungen, aber die grundlegende Kritik bleibt aufrecht. Das wurde auch in unterschiedlichen Stellungnahmen im Begutachtungsverfahren kritisiert. Neben uns kritisiert auch die ÖRAK deren Umfang als „unklar" und sieht ihn *„angesichts der potenziellen Eingriffsmöglichkeiten in sensible Unternehmensbereiche jedenfalls" als „problematisch" und im vorliegenden Wortlaut als „unverhältnismäßig".*[1]

1https://www.parlament.gv.at/PtWeb/api/s3serv/file/1800fcc7-ca3e-4350-9080-10e1b9ab3be7

Dritter Punkt: Verpasste Chance: Absichern von responsible disclosure

Mit § 11 wird zwar dem Wortlaut nach den Vorgaben der NIS-2-Richtlinie entsprochen, dem Ziel und Zweck der Bestimmung, nämlich die koordinierte Offenlegung von Schwachstellen zu erleichtern, wird diese Minimalvariante der Umsetzung jedoch nicht gerecht. In Österreich ist es immer noch so, dass der moralisch richtige Umgang mit Sicherheitslücken – nämlich das Melden an die Verantwortlichen – nicht belohnt sondern bestraft wird.

In anderen Ländern gibt es schon längst einen sicheren Rechtsrahmen für gemeldete Schwachstellen. Auch die EU-Behörde für Netzwerksicherheit (ENISA) empfiehlt klar ethical Hacker abzusichern. Trotz Erlass des BMJ fehlt eine solche Absicherung in Österreich, es braucht daher dringend eine Anpassung der straf- und datenschutzrechtlichen Bestimmungen.[2]

Vierter Punkt: Weitreichende Datenverarbeitungen und Übermittlungsmöglichkeiten

- § 17 kennt eine Verpflichtung des BMI zum Betrieb von IKT Lösungen zur Früherkennung von Cyber Bedrohungen. Wesentliche Einrichtungen können daran teilnehmen. Angesichts der fraglichen IT-Sicherheitssituation in Österreich werden wohl auch viele Unternehmen daran teilnehmen wollen. Wir sehen die Gefahr einer anlasslosen Massenüberwachung aufgrund der textlichen Ausgestaltung.

- § 42 sieht vor, dass eine Datenverarbeitung nicht nur zu Zwecken der Umsetzung des NIS-2-Gesetz erfolgen darf, sondern auch zum *„Schutz vor und zur Abwehr von Gefahren für die öffentliche Sicherheit".*

- § 43 kennt eine ungenau determinierte Übermittlungsmöglichkeit von personenbezogenen Daten an andere in- und ausländische Behörden oder Stellen

- Wir und viele andere Stakeholder orten in der ungenauen Bestimmung die Gefahr des Abflusses von personenbezogenen Daten oder von *Geschäfts- oder Betriebsgeheimnissen. Auch wenn mit dem Entwurf vom 13. Juni minimale Verbesserungen*

2 Weitere Informationen dazu sind in folgenden Dokumenten zu finden: https://epicenter.works/fileadmin/import/epicenter.works_-_verschaerfungen_computerkriminalitaet_stgb2023.pdf ; https://epicenter.works/fileadmin/user_upload/EMS-Hintergrundpapier.pdf

durch das auflisten der Datenkategorien erfolgt sind, sind die genannten Bestimmungen aus Datenschutzsicht weiterhin klar abzulehnen. [3]

Um zum Abschluss zu kommen:

Aus diesen Überlegungen heraus empfehlen wir daher die Neuausarbeitung des Gesetzes unter breiter Einbindung aller relevanten Stakeholder in Österreich aus Forschung, Zivilgesellschaft und Wirtschaft. Es geht hier nicht um ein abstraktes oder theoretisches Thema. Bei IT-Sicherheit geht es um den Schutz von Krankenhäusern, der öffentlichen Verwaltung, Schulen, der Privatsphäre von allen Menschen in unserem Land und auch dem Schutz der Wirtschaft vor Angriffen aus dem Ausland. Das Thema hat es verdient ernsthafter und ehrlicher behandelt zu werden, als dieser Entwurf es probiert hat.

3https://www.parlament.gv.at/PtWeb/api/s3serv/file/1800fcc7-ca3e-4350-9080-10e1b9ab3be7