AG KRITIS

Rede von Manuel Atug von der AG KRITIS

für die Anhörung des Bundestagsausschusses für Inneres und Heimat

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme 2.0 (IT-Sicherheitsgesetz 2.0)

am 01.03.2021

Manuel Atug

Gründer und Sprecher der unabhängigen AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen Expert:innen der AG KRITIS und den vielen Sicherheitsforscher:innen aus der Community für ihre Unterstützung.

Kontakt

Manuel Atug

E-Mail: HonkHase@ag.kritis.info

Twitter: @HonkHase

Webseite: https://ag.kritis.info

Vielen Dank Frau Vorsitzende.

Meine Damen und Herren,

es geht in dieser Anhörung um die Erhöhung der IT-Sicherheit. Dazu haben sich bereits initial bei der Analyse des IT-SiG 2.0 zwei Kernpunkte aufgedrängt:

Zum einen die augenscheinliche Strategie- und Ziellosigkeit im gesamten bisherigen Verfahren, kombiniert mit der fehlenden Evaluierung des IT-SiG 1.0, als ein Beispiel hierfür.

Zum anderen der offensichtliche Konflikt zur Sichtweise auf die IT-Sicherheit.

Über 2 Jahre wurde vor sich hin gewerkelt. Interessierte und Betroffene konnten sich in der Zeit nur durch geleakte Referentenentwürfe informieren. Beteiligung sieht anders aus.

Im Dezember letzten Jahres ging es dann Schlag auf Schlag. 5 Referentenentwürfe innerhalb von wenigen Tagen. Und zuletzt lediglich 26 Stunden als Frist zur Einreichung einer Stellungnahme zu über 100 Seiten Gesetzestext. Beteiligung, meine Damen und Herren, sieht einfach anders aus.

Cybersicherheit in Deutschland endet nicht bei den Zuständigkeiten in und um das Bundesministerium des Inneren. Dies gilt es daher dringend auch im IT-SiG 2.0 zu beachten.

Das IT-SiG 2.0 zeigt aufgrund dieser Vorgehensweise starke Defizite auf. Deutlich wird dies an vielen Stellen durch den erwähnten Konflikt zur Sichtweise auf die „IT-Sicherheit“.

- Zum einen blicken Sicherheitsbehörden und Nachrichtendienste im Kontext der Befugniserweiterung auf IT-Sicherheit. Also beispielsweise durch Staatstrojaner oder durch invasive Eingriffe in IT-Systeme aufgrund der Gefahrenabwehr, im Volksmund auch Hackback genannt. Und damit einhergehend auch durch die Verpflichtung des vermeintlich unabhängigen BSI zur aktiven Zurückhaltung von Sicherheitslücken für unbestimmte Zeiträume.
- Und auf der anderen Seite IT-Sicherheit im Kontext der Erhöhung der Cyberresilienz aus Sicht der Zivilgesellschaft und den Kritischen Infrastrukturen. Denn die Zivilbevölkerung benötigt robuste und widerstandsfähige Versorgung, beispielsweise mit Strom und Wasser, unabhängig von einer steigenden Digitalisierung in den Produktionsanlagen.

Eine einfache Regel in der IT-Sicherheit lautet:

Das Zurückhalten von Schwachstellen betrifft immer(!) die Zivilgesellschaft – und zwar weltweit(!) - sowie auch die private Wirtschaft und Betreiber kritischer Infrastrukturen – ebenfalls weltweit(!). IT-Sicherheit bedeutet daher im Umgang mit Sicherheitslücken ausnahmslos, diese schnellstmöglich loszuwerden.

Im Hinblick auf drohende Folgen dieser Zurückhaltung von Sicherheitslücken oder gar von IT-System-Ausfällen aufgrund des invasiven Einwirkens auf IT-Systeme kann das absichtliche Offenhalten oder Zurückhalten von Sicherheitslücken daher in einer Gesamtabwägung niemals angemessen sein. Findet dies in der Gesetzgebung keine Berücksichtigung, wird der Staat seiner Verantwortung in der IT-Sicherheit Deutschlands nicht gerecht.

Untermauert wird besagte Strategie- und Ziellosigkeit darüber hinaus durch die immer noch ausstehende - und nebenbei angemerkt: gesetzlich vorgeschriebene - Evaluierung der Wirksamkeit des bereits 2015 eingeführten Gesetzes. Eine Überarbeitung vorzunehmen, ohne den aktuellen Stand zu analysieren und den daraus resultierenden Erkenntnisgewinn als Feedback einzubringen, zeugt von einer grundsätzlichen und prozessbedingt verminderten Qualität durch Kardinalsfehler im Prozessablauf.

Durch die fehlende Evaluierung kann beispielsweise nicht nachvollzogen werden, ob die aktuellen Schwellenwerte die vorgegebenen Schutzziele erreichen. Denn im KRITIS Sektor Wasser sind derzeit unter 50 von ca. 5.000 Wasserwerken als KRITIS Betreiber einstuft.

Eine Trennung von defensiven Handlungen durch das BSI - und den invasiven, offensiven Maßnahmen durch die Sicherheitsbehörden und Nachrichtendienste - würde das kontinuierlich bröckelnde Vertrauen in das BSI wieder erhöhen. Hier wurde aber erneut die Chance vertan, das BSI möglichst unabhängig aufzustellen und dadurch die IT-Sicherheit zu erhöhen. Stattdessen wird das BSI immer Stärker zum Handlanger - oder wahlweise auch dem verlängerten Arm - von Sicherheitsbehörden und Nachrichtendiensten.

Werden beispielsweise Systeme zur Angriffserkennung gesetzlich gefordert, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die aufgrund einer Risikoanalyse der KRITIS Betreiber dringender nötig gewesen wären.

Ein freiwilliges IT-Sicherheitskennzeichen einzuführen, doppelt sich mit der verpflichtenden Umsetzung des EU Cyber Security Act. Ein Nutzen dieses zusätzlichen freiwilligen Kennzeichens erschließt sich darüber hinaus ebenfalls nicht.

Das ganze IT-SiG 2.0 steht daher symptomatisch dafür, wie unsystematisch das Thema IT-Sicherheit in Deutschland adressiert wird. Eine übergreifende und strategische Vorgehensweise, die auch Kommunen, Länder, Wissenschaft & Forschung, Bildung, Wirtschaft, Zivilgesellschaft und die Community der Sicherheitsforscher:innen sinnvoll in die Digitalisierung und damit in die Cybersicherheit als auch in die digitale Souveränität Deutschlands einbettet, fehlt leider völlig.

Danke sehr.