



AG KRITIS

Rede von Manuel Atug von der AG KRITIS

für die Anhörung des

**Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des
Europäischen Parlaments**

(EU Parliament Committee on Civil Liberties, Justice and Home Affairs)

zur

Stärkung des Katastrophenschutzes in der EU und Erhöhung der

Widerstandsfähigkeit kritischer Infrastruktur in Europa

(Strengthening EU Civil Protection and European Critical Infrastructure Resilience)

am 01.06.2026

Manuel ‚HonkHase‘ Atug

Gründer und Sprecher der unabhängigen AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen Expertinnen der AG KRITIS und den vielen Sicherheitsforscherinnen aus der Community für ihre Unterstützung.

Kontakt

Manuel ‚HonkHase‘ Atug

E-Mail: HonkHase@ag.kritis.info

Webseite: <https://ag.kritis.info>

Vielen Dank, liebe Vorsitzende.

Liebe Zuhörende,

die AG KRITIS ist ein unabhängiger Zusammenschluss von Expertinnen aus dem KRITIS Umfeld. Wir erhalten keine Gelder von der Wirtschaft oder vom Staat und machen das alles im Ehrenamt aus Überzeugung. Denn mit Wissen kommt Verantwortung.

Unser einziges Ziel ist die Erhöhung der Versorgungssicherheit der Bevölkerung.

Die EU hat sich vor vielen Jahren durch die EU NIS1 und EU NIS2 aber auch mit der EU CER Richtlinie sinnvolle Gedanken gemacht, wie wir kritische Infrastrukturen schützen wollen. Vor Unfällen oder Naturereignissen, vor gesundheitlichen Notlagen wie Pandemien, vor hybriden Bedrohungen und andere feindliche Bedrohungen (wie terroristischen Straftaten), vor krimineller Unterwanderung und vor Sabotage. Berücksichtigt werden sollen auch sektorübergreifende und grenzüberschreitende Risiken.

Es geht also um Naturereignisse, Unfälle und Vorsatzhandlungen. Egal ob als Cyber-Physische Auswirkung oder direkt im Physischen Raum. Die Versorgung der Bevölkerung soll gewährleistet werden.

Was wir als AG KRITIS genau darum fordern, ist defensive Resilienz in kritischen Infrastrukturen zu gewährleisten. Stattdessen erhalten wir immer mehr offensive Befugnisserweiterungen für Geheimdienste und Strafverfolgungsbehörden. Und die Erklärung, dass Cybersicherheit und physische Absicherung gegen Naturereignisse doch so kompliziert seien.

Was ist defensive Resilienz?

KRITIS Betreiber müssen dazu verpflichtet werden, echte Basis-Sicherheitsmaßnahmen permanent umsetzen, was bereits durch EU CER und EU NIS2 regulatorisch abgebildet wurde. Darüber hinaus muss aber durch Rechtsdurchsetzung auch sichergestellt werden, dass diese Maßnahmen ergriffen werden. Und das steht in ganz Europa massiv aus. Die Checks & Balances sind nicht gegeben, Aufsichtsbehörden sanktionieren kaum bis gar nicht. Teilweise wurden die beiden Richtlinien in EU-Mitgliedsstaaten nicht mal verabschiedet.

Lange vor dem Angriffskrieg von Putin wurden in der Ukraine Menschen ausgebildet, schnell zu entstören und Materiallager wurden angelegt. Ausfälle werden dadurch selbst in Kriegsgebieten zeitnah behoben. Auswirkungen von KRITIS Beeinträchtigungen werden dadurch seit Jahren erfolgreich minimal gehalten.

Das ist defensive Resilienz.

KRITIS Betreiber in der EU nutzen im Jahre 2026 allerdings immer noch nicht überall 2 Faktor gesicherte Fernwartung (siehe VIASAT wegen dem KA-SAT Angriff der Russen). Sie betreiben dafür aber oft archaisch wertvolle Systeme direkt am Internet, statt Sicherheitsupdates strukturiert und kontinuierlich einzuspielen. Sie haben auch oft kein funktionales Business Continuity Management, um in einer Krise die kritische Versorgungsleistung schnellstmöglich wieder herzustellen.

Bei einer Sturzflut im Ahrtal in Deutschland in 2021 starben über 180 Menschen unnötig. Denn wirksame Maßnahmen gab es und diese hätten ergriffen werden können - wurden sie aber nicht.

Diese ganzen ausbleibenden Handlungen sind grob fahrlässig und nicht gesetzeskonform.

Aufsichtsbehörden schauen dabei oftmals nur tatenlos zu, statt Rechtsdurchsetzung auszuüben und die Behebung dieser Fahrlässigkeit einzufordern. Die Verantwortlichen Ministerien und Regierungen

geben den Aufsichtsbehörden weder genug Stellen für die Rechtsdurchsetzung, noch ist der politische Wille da, diese wirksam einzufordern.

Dieses erhebliche Defizit hat sogar die EU Kommission bereits 2020 im Vorschlag für die EU NIS2 Richtlinie festgestellt:

„Die Aufsichts- und Durchsetzungsregeln der NIS-Richtlinie sind nicht wirksam. Die Mitgliedstaaten zögern beispielsweise sehr, Sanktionen gegen Einrichtungen zu verhängen, die keine Sicherheitsanforderungen festlegen oder Sicherheitsvorfälle nicht melden. Dies kann nachteilige Auswirkungen auf die Cyberresilienz einzelner Einrichtungen haben.“¹

Wir betonen daher ausdrücklich, dass durch eine solche Vorgehensweise durchaus auch vorsätzlich Menschenleben riskiert werden, wenn keine Anpassungen zur Behebung dieser erheblichen Mängel vorgenommen werden.

Was wir stattdessen erhalten, sind Massenüberwachung und offensive Maßnahmen wie Hackback und Staatstrojanern. Um diese nutzen zu können, müssen Strafverfolgungsbehörden und Geheimdienste Schwachstellen finden und zurückhalten. Oder als Abo-Dienst (meist aus Israel) einkaufen, so dass diese Lücken in Software (auf Windows, iPhone, Android usw.) offengehalten und ausgenutzt werden sollen. Diese Lücken sind dann auch in europäischer KRITIS Infrastruktur enthalten und schwächen die Resilienz, statt sie zu erhöhen.

Lücken, die in Software und im Betrieb von KRITIS geschlossen werden, können nicht von organisierten kriminellen, Geheimdiensten und anderen staatlichen Akteuren ausgenutzt werden. Angriffe und ihre Auswirkungen verpuffen damit wirkungslos.

Das ist defensive Resilienz.

Danke sehr.

¹ https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0007.02/DOC_1&format=PDF