LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/506

A09, A20

Stellungnahme

von

Ralf Benzmüller

(Vorstand eurobits, Executive Speaker G DATA SecurityLabs)

zum

Antrag der Fraktion der FDP, Drucksachen 18/2564

Kommunikation und IT-Sicherheit im Falle eines Katastrophenfalls durch einheitliche Planbarkeit sicherstellen

Bochum, 27.4.2023

Disclaimer:

Diese Stellungnahme habe ich eigenständig nach bestem Wissen und Gewissen verfasst. Sollte sie falsche Annahmen oder Fehler enthalten, dann verantworte ich das. Ich freue mich sehr, dass meine Rolle im Vorstand von eurobits, mir die Möglichkeit gibt, die Forderungen der FDP-Fraktion für den Innenausschuss des NRW-Landtags zu kommentieren. Die geäußerten Meinungen sind meine eigenen und sind weder repräsentativ für eurobits – Kompetenzzentrum für IT-Sicherheit noch für meinen Arbeitgeber G DATA.

Ausgangsbasis für meine Stellungnahme sind die Forderungen der FDP-Fraktion an den Landtag. Entsprechend ist dieses Dokument strukturiert. Auf Einzelheiten in der Herleitung, die nicht in Bezug zu den Forderungen stehen, gehe ich nicht weiter ein.

II. Beschlussfassung

Der Landtag stellt fest:

• Die Kommunikation sowie der Zugang zu Kommunikationssystem wie dem Mobilfunk, aber auch dem Internet, sind essenziell und haben Priorität bei einer Großschadenslage.

Dass insbesondere in einer Krisensituation die Kommunikation aufrechterhalten werden muss, ist unbestritten. In Notsituationen ist es wahrscheinlich, dass die Kapazitäten eingeschränkt sind. Daher sollten die Kommunikationskanäle für die Koordination der Einsatzkräfte und die Informationen für Betroffene entsprechend priorisiert werden.

• Schnelligkeit und Effizient sind essenzielle Grundlagen für eine angemessene Reaktion im Rahmen eines Angriffes auf oder eines Ausfalles von KRITIS

Schnell und effizient kann man in Krisensituationen nur reagieren, wenn man gut vorbereitet und mit den notwendigen Hilfsmaßnahmen vertraut ist. Regelmäßiges Training und Übung erhöhen die Leistungsfähigkeit im Krisenfall. Während es für Ausfälle (durch Naturkatastrophen) bereits Szenarien und Trainingsmöglichkeiten gibt, sind diese im Fall von Cyberattacken noch recht lückenhaft. Es gibt aber einige Ansätze, wie hier Abhilfe geschaffen werden kann und soll. Z.B. Das Konzept zum Cyberhilfswerk (CHW) der AG KRITIS, das Cybersicherheitsnetzwerk des BSI (eher für KMU geeignet) und das europäische CyberShield. Diese und ggf. weitere Lösungsansätze müssen aufeinander abgestimmt werden, um eine effiziente Umsetzung in Europa, in Deutschland, im Land und in den Städten, Kreisen und Kommunen zu gewährleisten.

• Kreise und Kommunen müssen bestmöglich beim Katastrophenschutz seitens der Landesregierung unterstützt werden.

Die Eltern des Grundgesetzes haben den Föderalismus aus gutem Grund festgeschrieben. Leider ist der Weg zum Konsens in föderalen Strukturen oft langwierig und umständlich. Es ist daher verständlich, dass in Krisensituationen, wo schnelle Entscheidungen notwendig sind, zentrale Entscheidungsinstanzen gefordert werden. Idealerweise bleiben aber die föderalen Strukturen intakt und greifen gut ineinander. Dazu braucht es aufeinander abgestimmte und geprobte Abläufe. So müssen in der Zeit vor einer Krise definierte Meldewege und klar zugeordnete Entscheidungskompetenzen entstehen, an der alle Ebenen der föderalen Struktur beteiligt sind und Informationswege und Meldeketten definiert und idealerweise automatisiert sind. Je mehr Entscheidungskompetenz vor Ort liegt, desto schneller können die Einsatzkräfte vor Ort reagieren - auch und gerade wenn Kommunikation eingeschränkt ist. Auch hier ist die Situation bei physisch begründeten Ausfällen etwas besser als bei Cyberattacken.

Der Landtag fordert die Landesregierung auf,

• ein Cyber- Hilfswerk (CHW) in NRW zu etablieren und mit den nötigen Strukturen zu versehen.

Die Bundesregierung hat die Umsetzung einer Cyberhilfe aus freiwilligen Helfern für Krisensituationen in KRITIS-Unternehmen bereits im Koalitionsvertrag festgeschrieben. Das Konzept ist inhaltlich sehr ausgereift und dessen Umsetzung hat das Potenzial die Resilienz von KRITIS deutlich zu erhöhen.

Die Governance des CHW ist noch offen. Eine Anlehnung oder Integration an die Strukturen des Technischen Hilfswerks (THW) ist aktuell das bevorzugte Szenario. Dann würde ein Großteil der Steuerung aber auf Bundesebene liegen und in den Ländern lägen eher die Koordinierungsaufgaben. Bevor hier aber keine klaren Verhältnisse geschaffen sind, ist eine Beschlussfassung spekulativ.

Das CHW rekrutiert sich aus freiwilligen Helfern, die entweder fundierte Computerkenntnisse mitbringen und/oder über Erfahrung mit den Abläufen und Technologien in KRITIS-Sektoren haben. Eine ähnliche Freiwilligen-Initiative wurde schon einmal vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem Namen "Cyberwehr" versucht. Die Konstellation wurde aber in der o.g. Gruppe nicht angenommen und kann als gescheitert gelten. Das Team der AG KRITIS ist deutlich besser in diesen Gruppen verankert und die Chance, dass sich genügend Freiwillige finden, stehen gut. Die Frage der Akzeptanz ist aber im Voraus schwer zu prognostizieren.

Europa geht einen anderen Weg zum Thema Resilienz gegen Cyberattacken auf KRITIS. Die europäische Digitalstrategie (https://commission.europa.eu/publications/european-commission-digital-strategy_en) sieht eine sichere und widerstandsfähige Infrastruktur vor. In einem ersten Entwurf zu einem Cyber Solidarity Act (https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2243) sollen mehrere Institutionen gegründet bzw. ausgebaut werden und mit nationalen Institutionen zusammenarbeiten. Dazu zählen die ENISA (das Pendant zum BSI auf EU-Ebene), das European Cyber Competence Center (ECCC) und der EU CyberShield. Letzterer ist Teil des "Cyber Emergency Mechanism" und soll ausgewählte Security Operation Center (SOC) koordinieren (pro Land eins, in DE ist es das CERT-Bund). Hier soll auch eine europäische Eingreiftruppe aus professionellen Cybervorfallsexperten entstehen, die Krisensituationen vermeiden, frühzeitig erkennen und möglichst schnell beheben soll. Diese (und ggf. weitere) europäische Aktivitäten sollten bei einer Umsetzung des Cyberhilfswerks in NRW berücksichtigt werden.

• durch die Erstellung eines Masterplanes dafür Sorge zu tragen, dass einheitliche Standards für die Ausarbeitung von Katastrophenschutzplänen gesetzt werden.

Die Formulierung "ein Masterplan" assoziiert, dass ein einziges Konzept für alle Katastrophenfälle anwendbar ist. Das entspricht m.E. nicht der immer wieder einzigartigen Natur von Katastrophen und Cyberangriffen. Im Bereich der Notfallpläne für Cybersicherheit haben sich Playbooks (https://apmg-international.com/article/what-are-cyber-incident-response-playbooks-why-do-you-need-them) für gängige Angriffe und deren Folgen bewährt. Hier kann man auch recht spezifisch auf einzelne Szenarien eingehen und auch ggf. auch Eventualitäten erfassen. Solche spezifischen Angriffsszenarien lassen sich auch effektiver trainieren. Und wenn alle Szenarien ausgiebig geübt wurden, können die Katastrophenhelfer in der Not effektiv und schnell agieren. Hier ist allerdings noch viel zu tun. Eine Reihe von wichtigen Maßnahmen sind im Konzept Cyberhilfswerk der AG KRITIS bereits berücksichtigt.

• dass in den Kreisen, in den Kommunen, in den Städten und Gemeinden Katastrophenschutzleuchttürme mit einheitlichen Mindeststandards etabliert werden.

Das Bild des Leuchtturms ist für mich hier eher verwirrend. Die Grundidee eines Schutzraums, der a) vor Ort leicht erreichbar und b) mit einer einheitlichen Grundausstattung ausgerüstet ist, halte ich für zweckmäßig.

o Es muss an allen Leuchttürmen Internet (Satelliteninternet) mit Hotspotfunktion vorhanden sein.

o Es muss an allen Leuchttürmen die Möglichkeit bestehen, die Einsatzkräfte der Polizei, der Feuerwehr, Krankenhäuser sowie die kommunalen Behörden zu erreichen.

o Es muss an allen Leuchttürmen die Möglichkeit bestehen, akkubetriebene Kommunikationsmittel laden zu können.

o Es muss an allen Leuchttürmen eine Versorgung mit Frischwasser gewährleitet sein.

o Es muss an allen die Möglichkeit bestehen, pflegebedürftige Menschen zu versorgen.

Zwei Anmerkungen dazu:

1. Das sind alles gute Vorschläge. Es sollten aber auch Lebensmittel, Decken, Schlafgelegenheiten etc. zur Verfügung stehen. Es gibt sicher auch einschlägige Vorschriften und Pläne, die hier berücksichtigt sein wollen
2. Pflegebedürftige Menschen impliziert oft alt und gebrechlich. Dazu gehören aber auch Kleinkinder und Säuglinge.

• in den Rathäusern, bei den Einsatzkräften der Polizei, Feuerwehr, bei der kommunalen Daseinsfürsorge sowie bei den Gerichten und Staatsanwaltschaften Satelliteninternet für den Notfall zu installieren.

• in den Rathäusern, bei den Einsatzkräften der Polizei, Feuerwehr, der kommunalen Daseinsfürsorge, bei den Gerichten und Staatsanwaltschaften ausreichend Notstromaggregate für den Notfall vorzuhalten.

Notstromaggregate und Internet & Telefonie über Satellit sollten zur Ausstattung für alle Beteiligten in Notsituationen gehören. Es gibt sicher Notsituationen, wo nicht alle Bereiche der Verwaltung und Strafverfolgung mit der Beseitigung der Folgen einer Katastrophe befasst sind. Die können dann auch mal ein paar Tage aussetzen, bis wieder ein Regelbetrieb möglich ist. Entsprechende Priorisierungen sollten im Rahmen des oben geforderten "Masterplans" (bzw. in den jeweiligen Szenarien eines differenzierteren Notfallplans) getroffen werden.

• weitere KRITIS-Betreiber mit Landesmittel dabei zu unterstützen, Satelliteninternet sowie Notstrom für den Notfall bereitzuhalten

Hieraus geht leider nicht hervor welche KRITIS-Betreiber für wen Notstrom und Satelliteninternet bereitstellen sollen. Diese Forderung reicht von a) Stromversorger schaffen Kapazitäten für Notstrom und Telefonieanbieter stellen sicher, dass sie auf Satellitenkommunikation umstellen können. Mindestanforderung wäre die Versorgung der Rettungs- und Koordinierungskräfte und der Schutzräume (um nicht Leuchtturm zu sagen). Bei einer weiten Auslegung müssten b) Banken, Logistikunternehmen und Krankenhäuser Notstrom und Satellitenkommunikation für alle bereitstellen. Ohne weitere Spezifikation ist diese Forderung m.E. nicht beschlussfähig.

Es könnte sich im Notfall als hilfreich erweisen, wenn die KRITIS Unternehmen dazu verpflichtet werden, Vorkehrungen zu treffen, dass die Angebote aufrecht erhalten werden können, die in Krisensituationen unabdingbar sind. Das sind nicht nur Strom und Telefon. Auch für Krankenwagen, Bargeld, Trinkwasser, Lebensmittel und Medikamente etc. sollten Basiskontingente definiert und bereitgehalten werden.

Ob und wie viele Landesmittel man dafür bereitstellt, hängt von der Haushaltslage ab. Ich könnte mir aber vorstellen, dass die damit verbundenen Kosten seitens der KRITIS-Unternehmen ohnehin eingepreist und auf die Verbraucher umgelegt werden können (würden Landesmittel das verhindern?) oder sich dadurch rechnen, dass das KRITIS-Unternehmen in der Krisensituation durch eine rasche Wiederherstellung des Betriebs das investierte Geld einspart.

• mit einer Bundesratsinitiative darauf hinzuwirken, den Aufbau eines zentralen Informations- und Datenmanagements „Bevölkerungsschutz" entsprechend der Zentralstellenfunktion des BKA beim BBK zu forcieren.

Diese Forderung wirft einige Fragen auf, die geklärt werden sollten, bevor man viel Energie in Initiativen steckt, die am Ende nicht zielführend sind. Und Ziele sollten der Ausgangspunkt sein. Ich vermute hinter diesem Vorschlag den Wunsch, von Landes- und Bundespolitikern auf das Krisengeschehen vor Ort sinnvoll einwirken zu können. Es gibt sicher noch weitere Ziele. In dieser pauschalen Form ist dieses Ziel aber nicht umsetzbar. Immer wieder findet man den Irrglauben, dass man mit möglichst vielen Daten die aufkommenden Probleme lösen kann. So pauschal funktioniert das aber nicht (zumindest nicht datenschutzkonform). Ausgangspunkt für die Arbeit mit Daten ist üblicherweise eine Fragestellung, ein fest umrissenes Problem oder ein vorher definiertes Ziel. Ausgehend davon werden die passenden Daten ausgewählt. Was soll mit den Daten erreicht werden? Welche Erkenntnisse und Schlussfolgerungen sollen möglich sein? Wie werden die Daten solide erhoben, gesäubert und mit welchen Methoden werden sie dann verarbeitet und visualisiert? Die Zahl der Fragestellungen für die dieser Prozess durchlaufen werden muss, ist insbesondere für Krisensituationen kaum absehbar. Hier könnten wieder die oben bereits angedeuteten spezifischen Szenarien (analog zu Cybersecurity Playbooks) als Ausgangsspunkt für jeweils spezifische Datenkonzepte dienen. Wenn die wichtigsten Szenarien ausgewählt sind, können sie nach und nach umgesetzt werden. In diesem Prozess sollten Privacy-By-Design und Security-By-Design tragende Prinzipien sein. Niemand möchte, dass die verfügbaren Informationen dazu genutzt werden können, Angriffe vorzubereiten (profanes Beispiel: die Fluchtpläne, die in öffentlichen Gebäuden aushängen, können zur gezielten Vorbereitung von Angriffen genutzt werden).

Die Forderung bezieht sich aber nur implizit auf die Daten. Explizit wird ein Management der Informationen und Daten im Kontext Bevölkerungsschutz gefordert. Ob damit der im vorherigen Absatz skizzierte Prozess gemeint ist, geht auch aus den begleitenden Ausführungen nicht hervor. Ein Management ist sicher notwendig. Die zuständige Behörde sollte ja nur in der Krisensituation Zugriff auf die notwendigen Daten haben. Hier stellen sich einige Aufgabenbereiche:

- Zugriffsrechte und Reporting. Wer hat wann auf welche Daten zugegriffen? Wer darf unter welchen Bedingungen auf Daten zugreifen und wie erfolgt im Notfall die Freigabe (kann ohne Strom und Telefon kompliziert werden). Wie wird mit vertraulichen oder klassifizierten Informationen umgegangen? Wie wird Missbrauch der Daten verhindert? (Diese Liste ist nicht vollständig, zeigt aber hoffentlich die Richtung)
- Es ist vielleicht möglich diese Verwaltungs- und Administrierungsfragen zentral zu managen. Ich halte es für utopisch zu glauben, man könnte alle notwendigen Daten für alle denkbaren Krisensituationen zentral zusammentragen. Was eventuell erreicht werden kann, ist die lokal verfügbaren Daten in einer Krisensituation an eine zentrale Stelle weiterzuleiten. Wenn das mehr oder weniger automatisiert erfolgen soll (weil man in der Krisensituation ja schnell agieren möchte), dann steht ein umfangreicher Standardisierungsprozess bevor. Die potentiellen Informationsquellen, müssen in einem Format vorliegen, das auch in der Zentrale genutzt werden kann. Mit der aktuellen Vielfalt an Datenformaten ist eine zentrale Erfassung, Aufarbeitung und Darstellung allenfalls mit viel Aufwand möglich. Auch hier ist nicht klar, ob dies durch den Begriff "Management" abgedeckt ist.

Es wird eine Zentralstellenfunktion gefordert, wie das BKA sie innehat. Der Antrag bezieht sich aber auf zwei Bereiche, die aktuell von unterschiedlichen Bundesbehörden betrieben werden. Für den Ausfall von Kritischer Infrastruktur werden im Antrag entweder physische Ursachen oder aber Cyberattacken als Ursache herangezogen. Der Effekt für die Bevölkerung ist letztlich derselbe. Das Kraftwerk oder das Wasserwerk funktioniert nicht mehr. Ob das aber an einem Erdrutsch oder einer Gruppe von politisch motivierten Computerspezialisten liegt, macht aber für die Beseitigung der Krisensituation einen großen Unterschied. Auch für die Zuständigkeiten. Für Naturkatastrophen ist das BBK zuständig, für Cyber-Vorfälle eher das BSI (oder das BMI oder das Verteidigungsministerium oder das NRW-Innenministerium). Die pauschale Forderung danach diese zentrale Struktur beim BBK anzusiedeln, steht im Widerspruch zur aktuellen Aufteilung der Ressorts. Ich halte es für unsinnig im BBK die im BSI bereits vorhandenen Kompetenzen neu aufzubauen. Anstelle eines Kompetenzgerangels wäre ein Koordinierungsprozess angebracht, bei dem sich die beiden Bundesämter auf ein Prozedere einigen, das im Krisenfall für eine reibungslose Zusammenarbeit sorgt.

• Risikokommunikation auszubauen und eine einheitliche sowie moderne Kommunikationsstrategie zu entwickeln.

In dieser Forderung geht es nur mittelbar darum, wie in der Krisensituation kommuniziert werden soll (als Teil der zu entwickelnden modernen Kommunikationsstrategie). Die Risikokommunikation findet im Vorfeld von Krisen statt, zu einem Zeitpunkt, wo die Krise noch keine Auswirkungen auf die Verfügbarkeit von Strom und Telefonie etc. hat. Die Risikokommunikation kann also über die üblichen Kommunikationskanäle erfolgen, die auch in der alltäglichen Bürokommunikation zur Verfügung stehen (mal abgesehen von Übungen). Diese Forderung ist m.E. redundant und mit der Forderung zur Erstellung eines Masterplans mit einheitlichen Standards bereits abgedeckt.

Zur Krisenkommunikation selbst. In vielen Einsatzzentralen gibt es bereits Kommunikationssysteme, die für die Benachrichtigung und die Koordination von Einsätzen genutzt werden. Stellvertretend sei hier DAKSpro von der Firma tetronik genannt (https://www.tetronik.com/de/produkte/daks-pro.html). Solche Systeme können mit entsprechenden Modulen auch für Krisensituationen ohne Strom und ohne terrestrischen Mobilfunk (via Satellit oder DECT) konzipiert werden. D.h. technische Lösungen für die Krisenkommunikation auch in speziellen Situationen sind am Markt vorhanden und müssen "lediglich" angeschafft und konfiguriert werden. Möglicherweise lassen sich bereits vorhandene Anlagen erweitern.

Schlussbemerkung

Prinzipiell ist es begrüßenswert, dass die Landesregierung sich darum kümmert, dass Vorkehrungen getroffen werden, die zur besseren Bewältigung von Krisensituationen führen. Einheitlich ausgestattete Schutzräume flächendeckend in ganz NRW und Infrastruktur zur Gewährleistung von Notfallkommunikation sind sicher wichtige Bausteine. Aber insbesondere im Bereich von Cyberattacken auf KRITIS-Unternehmen ist noch viel zu tun. Das Konzept Cyberhilfswerk der AG-KRITIS ist ein ausgezeichneter Ausgangspunkt für die Verbesserung der Resilienz im Cyberkrisenfall und sollte – wie im Koalitionsvertrag angekündigt – lieber heute als morgen umgesetzt werden. Dabei ist allerdings Augenmaß gefragt und eine kluge Integration des CHW in ähnliche Initiativen auf EU-, Bundes- und Landesebene.