LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/6835**

21.11.2023

Antrag

der Fraktion der AfD

IT-Sicherheit auch bei Kommunen verbindlich und robust stärken - Die NIS-2-Richtlinie darf nicht verwässert werden

I. Ausgangslage

In der Nacht zum 30. Oktober entdeckten Mitarbeiter von Südwestfalen-IT (SIT), einem IT-Dienstleister für Kommunen, verschlüsselte Fragmente auf ihren Servern. Es wurde vermutet (und letztendlich auch bestätigt), dass Südwestfalen-IT Opfer eines erpresserischen Hackerangriffs geworden war oder dies kurz davorstand. Infolgedessen wurden aus Sicherheitsgründen sämtliche Server abgeschaltet und Netzwerkverbindungen gekappt.

Die Auswirkungen auf die betroffenen Kommunen haben dabei dramatische Züge angenommen. Mittlerweile wird von 131 betroffenen Organisationen ausgegangen: Neben 103 Gemeinden in NRW sind es 9 Unternehmen und Verbände, 11 Kreisverwaltungen sowie mindestens 7 Standesämter in Niedersachsen.

Mittlerweile sind sogar die Finanzen mancher Kommunen durch den IT-Ausfall in extreme Mitleidenschaft gezogen worden, da es den betroffenen Kommunen nicht mehr möglich ist, Steuern, Beiträge und Gebühren einzuziehen. So muss zum Beispiel die Stadt Bergisch Gladbach einen Kredit aufnehmen, um die Verluste aus den nicht eingezogenen Gewerbesteuern und Grundbesitzabgaben auszugleichen. Die Stadt Leichlingen kann keine Gelder für Kitas und Schulen einziehen oder die Hundesteuer abbuchen.

Der Schaden dieses Cyberangriffs durch die Hackergruppe Akira, die ihre Leistung als „Ransomware-as-a-Service“ (RaaS) für Kriminelle anbietet, geht mittlerweile in mehrere Millionen. Dabei war es nicht die Hackerattacke an sich oder die beabsichtigte Erpressung durch Ransomware, sondern die präventive Abschaltung aller Server, die letztendlich die digitale Verwaltung der betroffenen Kommunen zum Erliegen brachte.

Dieser Vorfall reiht sich ein in viele ähnliche Fälle in Deutschland, bei denen durch Hackerangriffe auf Kommunen oder deren IT-Dienstleister die digitale Verwaltung zusammenbrach. Zuletzt gab es am 15. November 2023 einen Hackerangriff auf die Telekommunikationsinfrastruktur der Neusser Stadtverwaltung.

Eine Studie des Digitalverbandes Bitkom von 2023 sieht den jährlichen Schaden durch Cyberangriffe und Datendiebstähle allein für Unternehmen bei ca. 206 Mrd. Euro. Aber auch Kommunen geraten immer mehr in den Fokus erpresserischer Hacker.

Datum des Originals: 21.11.2023/Ausgegeben: 21.11.2023

2022 sind laut Bericht des BSI 27 Kommunen Cyberangriffen zum Opfer gefallen. Dieses Jahr sind bereits vielfach mehr Kommunen betroffen.

Die Vielzahl an erfolgreichen Angriffen auf die IT-Infrastruktur der Städte und Gemeinden zeigt, dass vor allem die kommunale IT-Infrastruktur und Verwaltung sowohl technisch und organisatorisch als auch personell zunehmend überfordert ist, um eine zeitgemäße robuste IT-Sicherheit zu entwickeln und durchzusetzen.

Besitzen Kommunen oder deren IT-Dienstleister engagiertes und fachlich gut ausgebildetes Personal, sind Hardware und Software auf dem neuesten Stand, ist eine Multi-Faktor-Authentisierung Pflicht und Standard, existiert ein belastbares Notfall- und Sicherheitskonzept das durch mehrfache Übungsabläufe robust und schnell abgearbeitet werden kann, gibt es eine Segmentierung der jeweiligen Netzwerke und gibt es virtuelle Trennungen von Anwendungen und Kunden, dann sind die Systeme resilient genug, dass Cyberangriffe nur einen Bruchteil der Wucht und der Kosten als sonst entfalten.

Mittlerweile ist Cybersicherheit in der Mitte der digitalpolitischen Agenda angekommen. Auch hat sich mittlerweile ein komplexes System an IT-Security-Akteuren in Europa, Deutschland, den Bundesländern und auch auf kommunaler Ebene herausgebildet. Die Bundesregierung hat mit dem IT-Sicherheitsgesetz 2.0 bereits wesentliche Vorkehrungen für robustere Cybersicherheits-Maßnahmen gesetzt.

Aber auch die Europäische Union hat mit der neuen Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) und der Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) die Cybersicherheitsarchitektur in den EU-Mitgliedsländern wesentlich vorangetrieben. Vor allem die am 16.01.2023 in Kraft getretene neue NIS-2-Richtline mit ihrem wesentlich erweiterten Anwendungsbereich, vielfältigen Meldevorschriften aber auch einem umfangreichen Bußgeldkatalog wird die Cybersicherheitsarchitektur in Deutschland wesentlich verbindlicher und auch tiefer in die Fläche gehend prägen.
Bis zum 17. Oktober 2024 müssen die EU-Mitgliedstaaten diese Richtlinie in eigene Gesetze eingebracht haben. Neu an der NIS-2-Richtlinie ist unter anderem, dass zu den 18 Sektoren, die von der Richtlinie betroffen sein sollen, auch die öffentlichen Verwaltungen auf zentraler und regionaler Ebene sowie deren Rechenzentren gehören.

In Deutschland wird das Artikelgesetz „NIS2UmsuCG“ die NIS-2-Richtlinie in bestehende Gesetze implementieren. Jedoch werden in dessen 3. Entwurf schon wesentliche Punkte der NIS-2-Richtlinie aufgeweicht. So soll es keine Schulungspflicht für Mitarbeiter bei den betreffenden Unternehmen geben, auch wurden die Anforderungen an die Lieferkettensicherheit gelockert und der Finanzsektor wird weniger streng reguliert.

Die größte Lücke in der IT-Sicherheit wurde jedoch am 03.11.2023 gerissen. Der IT-Planungsrat, eine zentrale, länderübergreifende Koordinierungsinstanz zur Steuerung eines flächendeckenden Aufbaus der Digitalen Verwaltung, hat an dem Tag beschlossen, die Bundesregierung und die Länder zu bitten, dass die NIS-2-Richtlinie nicht für Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen gelten soll[1] – vier Tage nach dem Desaster, den der Hackerangriff auf die kommunale Infrastruktur in Südwestfalen angerichtet hatte.

[1] https://www.it-planungsrat.de/beschluss/beschluss-2023-39

Die Onlineausgabe der WirtschaftsWoche berichtete über den Vorfall und sah darin eine „Bankrotterklärung für die IT-Sicherheit kommunaler Behörden“[2]. Ein im selben Beitrag zitierter IT-Sicherheitsexperte kritisierte: „Was der IT-Planungsrat da verabschiedet hat, ist Ausdruck kompletter Realitätsverweigerung.“

Der Tagesspiegel bedauert, dass durch die Intervention des IT-Planungsrates die verbindliche und robuste Regelung der NIS-2-Richtlinie nicht für die Kommunen gelten soll.[3] Die Cybersicherheit der Kommunen scheitere dabei an verwaltungsrechtlichen Unwägbarkeiten und fehlender Kongruenz der Länder. Weitere Gründe für das Ausklammern der Kommunen aus der Umsetzung der NIS-2-Richtlinle scheinen auch die drohenden Strafzahlungen, die bis zur persönlichen Haftung gehen können, zu sein, wenn ein Nichteinhalten der neuen Vorschriften zur Cybersicherheit festgestellt wird.

Angesichts der offensichtlichen Vulnerabilität der kommunalen IT-Infrastruktur muss jede Gelegenheit genutzt werden, die eine robustere, resilientere und auch verbindlichere IT-Sicherheitskonzeption verspricht. Die EU-Richtlinie NIS-2 setzt genau diese Notwendigkeit um und darf keinesfalls aufgeweicht werden.

II. Der Landtag stellt fest,

- Der Prozess der Digitalisierung der Verwaltung auf allen Ebenen gelingt nur mit einer robusten IT-Sicherheit und IT-Infrastruktur.
- Besonders finanzielle und personelle Defizite der Kommunen fördern das Auslagern ihrer IT in zentrale Rechenzentren und beschleunigt damit deren Bedeutung als besonders schützenswerte kritische Infrastrukturen der Region – auch wenn diese noch unterhalb der KRITIS-Schwellenwerte liegen.
- Cyberangriffe und deren langwierige Schäden, insbesondere auf die kommunale Verwaltung, torpedieren das Vertrauen der Bürger in die Digitalisierung unmittelbar und schwerwiegend.
- Eine robuste IT-Sicherheitsstrategie benötigt vor allem hochqualifizierte und engagierte Führungskräfte und Mitarbeiter auf allen Ebenen.

III. Der Landtag fordert die Landesregierung auf,

- sich auf allen Ebenen dafür einzusetzen, dass die Umsetzung der NIS-2-Richtlinie Kommunen und IT-Infrastrukturen auf kommunaler Ebene im Anwendungsbereich berücksichtigt;
- eng mit den kommunalen IT-Dienstleistern und den kommunalen Spitzenverbänden sowie mit Fachleuten für Cybersicherheit aus Bundes- und Landeseinrichtungen zusammenzuarbeiten, um einen Leitfaden sowie verbindliche Hilfsangebote für die Kommunen und kommunalen IT-Rechenzentren hinsichtlich der Erfüllung der Vorschriften der NIS-2-Richtlinie zu erstellen;
- ein regelmäßiges Monitoring über den Stand der Umsetzung der NIS-2-Richtlinie für betroffene Landeseinrichtungen und Kommunen und deren gemeinsame Rechenzentren zu erstellen;
- dem Parlament einen Bericht vorzulegen, der aufzeigt, welche Hilfsmaßnahmen durch welche Landesreinrichtungen an das vom Hackerangriff getroffene Südwestfalen-IT gingen und gehen;

[2] https://www.wiwo.de/unternehmen/it/neue-it-sicherheitsregeln-der-eu-wir-sind-hier-doch-nicht-bei-pippi-langstrumpf/29486958.html
[3] https://background.tagesspiegel.de/cybersecurity/nis-2-umsetzung-ohne-kommunen

- dem Parlament einen Bericht über den Stand beim Aufbau des Kommunal-CERTs vorzulegen.

Sven W. Tritschler
Dr. Martin Vincentz
Andreas Keith

und Fraktion