AG KRITIS

Stellungnahme der AG KRITIS zur öffentlichen Anhörung im Landtag Nordrhein-Westfalens zum Antrag „Das Landesverwaltungsnetz weiterentwickeln, um der steigenden Bedeutung digitaler Verwaltungsprozesse gerecht zu bleiben“ auf Drucksache 17/14260

„Des Schusters Kinder tragen die schlechtesten Schuhe." [volkstümliches Sprichwort]

am 18.11.2021

Johannes Rundfeldt

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

Johannes Rundfeldt

E-Mail: jrundfeldt@ag.kritis.info

Twitter: @ijonberlin

Webseite: https://ag.kritis.info

Inhalt

Gesetzlicher Hintergrund

Für acht der zehn KRITIS-Sektoren gibt es klare, öffentlich einsehbare und verbindliche gesetzliche Regelungen (BSIG § 2, § 8a, § 8b, BSI-KRITISV usw.) Zwei der zehn Sektoren haben bisher keine klaren Regelungen – die Sektoren „Staat und Verwaltung“ sowie „Medien und Kultur“. Technische Einrichtungen aus dem Sektor Staat und Verwaltung, die zweifelsohne zur kritischen Infrastruktur zählen müssten, sind im April ausgefallen. Ein Teil der Leitungen des Landesverwaltungsnetzes (LVN) in Nordrhein-Westfalen waren gestört, für ca. zwei Tage waren ca. zehn Prozent der Behörden arbeitsunfähig. Unter anderem davon betroffen war behördliche E-Mail-Kommunikation, Zugriffe auf Akten sowie die Übermittlung der Corona-Zahlen.

Regelungen für die ersten acht Sektoren fallen in den Zuständigkeitsbereich des Bundes – über die verbleibenden zwei Sektoren hat der Bund keinen Einfluss, da dieser Einfluss im Verantwortungs- und Zuständigkeitsbereich der Bundesländer liegt.

Vereinfacht beschrieben, fällt eine Anlage dann unter die Regelungen der kritischen Infrastruktur, wenn sie zu:

- einem der acht KRITIS-Sektoren gehört,
- mehr als 500.000 Menschen versorgt und
- von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Alle drei Kriterien sehen wir für das Landesverwaltungsnetz Nordrhein-Westfalen als erfüllt an. Nichtsdestotrotz gibt es für den Sektor Staat und Verwaltung weder in NRW noch in anderen Bundesländern klar definierte Anlagenkategorien, noch eine klare gesetzliche Grundlage. Auch die Pflichten für Betreiber der kritischen Anlagen im Sektor Staat und Verwaltung sind nicht klar definiert.

Dies zu definieren und die Umsetzung in den Behörden zur kontrollieren, liegt im Zuständigkeitsbereich der Landesregierung Nordrhein-Westfalen. Der Bund hat sich mit dem UP BUND ein Regelwerk gegeben, dessen Schwammigkeit und dessen Interpretationsspielräume nur durch seine Unverbindlichkeit übertroffen werden. Auch ist keinem Mitglied der AG KRITIS eine vergleichbare Regelung für das Land NRW oder ein anderes Bundesland bekannt. Und dies, obwohl mehrere unserer Mitglieder eine dienstliche Zuständigkeit für Datenschutz oder IT-Sicherheit in Behörden des Landes NRW haben.

Bedauerlicherweise wurde die Zuständigkeit der Länder für KRITIS erstmalig im Rahmen der COVID-19-Pandemie öffentlich sichtbar, bei der die KRITIS-Verordnung und die Sektordefinition aus dem BSI-Gesetz als initiale Basis herangezogen wurde, um zu definieren, welche Personen auch bei einer Ausgangssperre zwingend Sonderrechte wie z. B. Kindernotbetreuung haben müssen, um die Funktion des Gemeinwesens nicht zu gefährden.

Die KRITIS-Regelungen wurden eigentlich geschaffen, um die IT-Sicherheit in kritischen Infrastrukturen zu verbessern und nicht um gesetzlich zu definieren, wer eine Kindernotbetreuung erhalten darf oder wer auch während einer Ausgangssperre noch die eigene Wohnung verlassen darf.

Es ist daher aus unserer Sicht mehr als überfällig, klare und verbindliche Regeln, sowie technische Standards für den KRITIS - Sektor „Staat und Verwaltung“ zu schaffen, diese dann umzusetzen und anschließend unabhängig aber transparent – sprich öffentlich – nachzuweisen.

Technische Details des Vorfalls

Am 28.04.2021 wurde der Vorfall im Plenum des Landtags NRW diskutiert. Die dort von Minister für Wirtschaft, Innovation, Digitalisierung und Energie Prof. Dr. Pinkwart gemachten Aussagen werden wir im folgenden Teil der Stellungnahme analysieren und mit den technischen Auflagen vergleichen, die der Staat privatwirtschaftlichen KRITIS-Betreibern macht. Wir beziehen uns hier auf das Plenarprotokoll 17/125, Seite 96 ff.

Kritische Infrastrukturen müssen gemäß BSIG § 8a den Stand der Technik bei:

- Vertraulichkeit
- Verfügbarkeit,
- Authentizität und
- Integrität

umsetzen.

Die Analyse, welche Datenleitungen durch den Ausfall betroffen waren, begann am 19.4. ab 18:30 Uhr und dauerte laut Minister Prof Dr. Pinkwart 7:45 Stunden. Dies scheint unzumutbar lang und legt nahe, dass solche Szenarien nicht ausreichend oft geübt wurden. Möglich ist des Weiteren, dass interne Ressourcen für solche Vorfälle nicht in ausreichendem Maße vorhanden sind. Auch gibt diese lange Zeitdauer Anlass zur Vermutung, dass die sogenannten Service Level Agreements unzureichend sind, in denen unter anderem die maximale Reaktionszeit im Krisenfall mit dem Betreiber der Datenleitung, der Deutschen Telekom, vereinbart sind. Für den Betrieb einer kritischen Infrastruktur sind höhere Verfügbarkeitsanforderungen zu stellen und diese auch mit allen DienstleisterInnen vertraglich abzusichern.

Die Verfügbarkeit ist eines der vier KRITIS-Schutzziele – wenn der Ausfall einzelner Datenleitungen zum Ausfall von Netzsegmenten führt, so wird das Schutzziel der Verfügbarkeit nicht angemessen eingehalten. In diesem Fall muss von fehlender Redundanz ausgegangen werden, da der Ausfall einzelner Leitungen eben nicht zum Ausfall von Netzsegmenten führen sollte, wenn ausreichende Redundanz-Maßnahmen ergriffen wurden, um das Schutzziel der Verfügbarkeit wirklich angemessen einzuhalten.

Der Minister Prof. Dr. Pinkwart erklärte weiterhin, dass es im Rahmen der Wiederherstellung der Leitungen zu Folgefehlern kam, die einen Neustart einer zentralen Netzwerkkomponente erforderten. Die Abhängigkeit von einer einzelnen zentralen Netzwerkkomponente ist wiederum ein starkes Indiz für fehlende Redundanz oder defekte Hochverfügbarkeit. Wenn Netzwerkverbindungen von der störungsfreien Funktion einer einzelnen zentralen Netzwerkkomponente abhängen, so ist es für jeden KRITIS-Verantwortlichen offensichtlich, dass diese Netzwerkkomponente redundant

vorhanden sein muss. Wie der Vorfall demonstriert, ist eine nur teilweise Redundanz in der Netzwerkinfrastruktur nicht ausreichend, um das Schutzziel Verfügbarkeit sicherzustellen.

Jeder privatwirtschaftliche KRITIS-Betreiber, der die gesetzlichen Schutzziele erfüllt, hätte eine solche Netzwerkkomponente redundant vorgehalten, so dass ein Umschalten ohne Serviceunterbrechung möglich gewesen wäre.

Falls es an mangelnder Redundanz der Netzwerkleitungen gelegen hat, ist die Planung für den Betrieb schon mangelhaft bewertet, vorgenommen und realisiert worden.

Der notwendige Neustart der Netzwerkkomponente, der auf die Tagesrandzeit verschoben wurde, sollte planmäßig nur 30min dauern – trotzdem dauerte es von 17 Uhr am 20.4. bis 6:20 Uhr am 21.4., bis dieser Neustart abgeschlossen war. Aus unserer Sicht ist es auf Basis der vorliegenden Informationen und Einlassungen des Ministers nicht nachvollziehbar, warum dieser Neustart nicht direkt in den frühen Morgenstunden des 20.04.2021 durchgeführt wurde, sondern erst in der Nacht des darauf folgenden Arbeitstages.

Der gesamte Zeitablauf legt nahe, dass Situationen wie die vorliegende nicht ausreichend geübt und trainiert worden sind. Unternehmen im Internet- und Kommunikationssektor haben, so äußerten sich Mitglieder der AG KRITIS intern, für das Umschalten von der einen auf die andere Leitung im Regelfall nur wenige Minuten vorgesehen.

Der Minister führte weiterhin aus, dass manche Behörden unabhängig von den zentralen Komponenten eigene Redundanzsysteme hatten. Dies deutet darauf hin, dass die Schutzziele für kritische Infrastruktur uneinheitlich und unvollständig umgesetzt wurden – ein Zustand, der für keinen privatwirtschaftlichen KRITIS-Betreiber akzeptabel wäre.

In der Plenardebatte fragte Herr Bolte-Richter laut Protokoll den Minister zur Übermittlung von Corona-Zahlen, die durch den Ausfall unterbrochen wurden. Dr. Pinkwart antwortete, dass es zwar zu Verzögerungen gekommen sei, aber dies nichts mit den anderen Themen zu tun gehabt hätte. Dieser Interpretation der Faktenlage können wir nicht zustimmen, denn in der Antwort erklärte der Minister, dass diese Daten sowohl per E-Mail, als auch über „sogenannte Web-Server“ und auch über das Bund-Länder-Kommunen-Verbindungsnetz übertragen werden.

Viele uneinheitliche Übertragungswege sind im Regelbetrieb zumindest zeitweise begrenzt tolerierbar. In der Krisenlage ist jedoch ein solcher uneinheitlicher Betrieb ein im Risikomanagement zu berücksichtigender Risiko-Faktor. Auf Nachfrage durch Frau Paul erklärte der Minister weiterhin, dass er zum Zeitpunkt der Frage – sieben Tage nach dem Vorfall – noch nicht in der Lage ist, zu erklären zu welchem Zeitpunkt welche Daten nachgemeldet oder weitergemeldet wurden.

Die Abwesenheit dieser Information interpretieren wir so, dass der Krisenstab auch am 28.04., also sieben Tage nach dem Vorfall, noch nicht „vor der Lage“ war. Dies sehen wir als deutlichen Hinweis auf tieferliegende Missstände in der Digitalisierung der Behörden des Landes NRW. Mit einem einheitlich umgesetzten Übertragungsweg unter der Nutzung verbindlicher APIs (standardisierte technische Schnittstellen für Anwendungen) wäre es trivial, diese Informationen direkt nach Beendigung der Verbindungsprobleme zu erhalten und entsprechend zu agieren. Mit hoher Wahrscheinlichkeit wäre auch die Verzögerung der Übertragung deutlich kürzer gewesen.

Es ist notwendig, im normalen Regelbetrieb für den Krisenfall vorzusorgen. Ein komplizierter Prozess, der je nach Behörde auf E-Mail, Web-Server, andere Netze des Staates oder sogar auf Fax setzt, wird in der Krise eher gestört werden, kaum nachvollziehbar sein und für längere Wiederanlaufzeiten sorgen, als ein vereinheitlichter und standardisierter Prozessablauf gemäß Stand der Technik.

Vor diesem Hintergrund stellen wir fest, dass die verzögerte Datenübertragung sehr wohl „etwas mit den anderen Themen zu tun hat“.

Allgemeine Empfehlungen

(IT)-Sicherheit ist ein kontinuierlicher Prozess und kein Zustand. Ein redundant ausgelegtes System, bei dem heute die IT-Sicherheit geprüft wird und bei dem heute eine Übung zum Umschalten auf die redundant vorgehaltene parallele Installation trainiert wird, gilt dadurch nicht automatisch auch morgen noch als sicher und redundant.

IT-Sicherheit wird nicht alleine durch technische Maßnahmen erreicht – ebenso wichtig wie das Schließen von Sicherheitslücken ist, dass die zuständigen MitarbeiterInnen und DienstleisterInnen regelmäßig geschult werden und auch Krisenübungen durchführen. Eine Organisations- und Fehlerkultur der engen, transparenten und offenen internen Abstimmung erhöht die Effizienz der Abläufe und fördert die Kommunikation von Problemen bevor daraus eine Krise entstehen kann. Unverzichtbare Grundlage ist die ausreichende Ausstattung mit technischen wie personellen Ressourcen und der kritischen Infrastruktur angemessene Service Level Agreements in Verträgen mit externen DienstleisterInnen.

Redundant vorgehaltene Komponenten sind nur dann hilfreich beim Erhalt der Versorgungssicherheit mit kritischen Dienstleistungen, wenn das Umschalten für den Krisenfall regelmäßig geübt wird. Auch unter verschiedenen Vorzeichen, wie z. B. teilweise weggebrochene Netzsegmente oder externe Störfaktoren. Wenn die Verfügbarkeit kritischer Infrastrukturen vom reibungslosen Ablauf der Umschaltprozesse und Notfallpläne abhängt, fehlt im Krisenfall die wertvolle Zeit, in der Handbücher studiert werden oder den Hersteller-Support kontaktiert wird.

Weiterhin empfehlen wir erneut dringend, das vorgelegte Konzept zum Aufbau eines Kommunal-CERTs umzusetzen. Dieses Konzept wurde unter dem Titel: „Stellungnahme für die Anhörung des Landtags Nordrhein-Westfalen – Kommunale IT-Sicherheit sicherstellen – Aufbau eines zentralen Kommunal-CERT am 24.06.2021“ durch Manuel Atug als Sachverständiger der AG KRITIS vorgestellt. Die dort enthaltenen Empfehlungen würden für einen engeren Austausch und mehr Krisenreaktionskapazitäten sorgen, welche wiederum bei einer Störungssituation wie am 21.04.2021 die Bewältigung der Krise beschleunigt und deren Auswirkungen reduziert.

Darüber hinaus hat sich in der Wirtschaft das Konzept der sog. „Bug Bounty“ etabliert. Hier wird für Mitarbeitende, DienstleisterInnen oder auch externe Dritte eine Belohnung ausgelobt, falls sie Fehler („Bugs“) oder Sicherheitslücken („Vulnerabilities“) finden und koordiniert melden. Diese Belohnung könnte z. B. eine bestimmte Summe Geld sein oder für Mitarbeitende ein zusätzlicher Urlaubstag.

Neben der Schaffung passender CERTs, der Etablierung von Bug Bountys und der Schaffung echter, einheitlicher Redundanz für alle Landesbehörden dürfen zwei weitere Punkte nicht unerwähnt bleiben.

Einerseits ist es notwendig, dass alle (IT-) MitarbeiterInnen der Behörden sowie der externen DienstleisterInnen gemeinsam regelmäßige Krisenübungen durchführen. Andererseits ist es aber auch notwendig, vertrauenswürdige Gesprächs- und Feedback-Runden zu etablieren. Fast alle Probleme in der IT sind den unteren Hierarchieebenen, die täglich mit dem Betrieb der IT zu tun haben, bekannt und bewusst. In vielen Fällen werden diese Probleme in abgeschwächter Form unregelmäßig auch an höhere Hierarchieebenen kommuniziert. Gerade in der Wirtschaft hat es sich als äußerst effektiv erwiesen, mehrere Hierarchieebenen zusammenzufassen und eine Bestandsaufnahme aller bekannten Mängel durchzuführen. Auch und gerade dann, wenn die Behördenleitung diese Themen lieber weniger groß aufhängen möchte.

Das aktive Beheben und Verbessern vieler scheinbarer „Kleinigkeiten“, wie z. B. inkonsistente und nicht harmonisierte Übertragungswege von Daten zwischen Behörden sorgt im dadurch strukturierten und standardisierten Regelbetrieb für mehr freie Personalressourcen und im Krisenfall für weniger Auswirkungen oder Folgen der Krise. Jede Krise entsteht nicht für sich alleine, sondern ist eine Verkettung von vermeidbaren Kleinigkeiten, die dann eskaliert und zu einer Krise anwächst, wenn sie nicht vermieden (Prävention) oder rechtzeitig entdeckt (Detektion) und dann gezielt unterbrochen (Reaktion) wird.

Auch ist Rechtssicherheit für IT-SicherheitsforscherInnen, MitarbeiterInnen oder MitarbeiterInnen externer DienstleisterInnen extrem wichtig. Wir fordern hier eine Korrektur des § 202c StGB, der dahingehend angepasst werden soll, dass die Strafbarkeit, ähnlich wie beim Straftatbestand des Betrug, an die Intention oder Absicht der Handlung geknüpft wird. Leider hat gerade die CDU durch die Klage gegen Lillith Wittmann hier jegliches Vertrauen verspielt. Hier können wir der Landesregierung nur empfehlen, sich auf Ebene der Bundesregierung für Änderungen dieser Art stark zu machen und von dem gemeinsamen vertraulichen Austausch auf Augenhöhe mit der SicherheitsforscherInnen Community zu profitieren.

Herrn Minister Pinkwart empfehlen wir hier die Übernahme der Forderungen des Antrags auf Bundestagssdrucksache 19/7698, insbesondere Unterpunkt 8, in den Koalitionsvertrag, den er für die Fraktion der Freien Demokraten im Bundestag mitverhandelt.

Gesetzliche Empfehlungen

Wir empfehlen der Landesregierung Nordrhein-Westfalen, für den Sektor „Staat und Verwaltung“ eine Verwaltungsvorschrift zu erlassen, die verbindliche Regelungen für kritische Infrastrukturen im Sektor Staat und Verwaltung in NRW schafft. Hier sollte sich die Landesregierung an den Regelungen in der KRITIS-Verordnung orientieren. Selbstverständlich steht die AG KRITIS als unabhängige Interessengemeinschaft hierfür auf Wunsch beratend zur Verfügung.

Gesetzliche Regelungen, die vom Staat für privatwirtschaftlichen Unternehmen den Stand der Technik als zumutbar, verhältnismäßig und angemessen angesehen werden, sollten den Mindeststandard für den Staat darstellen.

Die zu schaffenden Vorgaben im Sektor „Staat und Verwaltung“ sollten über den Mindeststandard hinaus gehen, denn bei privaten Betreibern kann der Staat die Einhaltung der Gesetze mittels Sanktionen erzwingen – bei Behörden ist das so nicht möglich.

So kann, auch im Fall einer mangelhaften Umsetzung, ohne Sanktionsmöglichkeiten der erreichte Mindeststandard über dem Standard liegen, der bei privatwirtschaftlichen Betreibern per Sanktionierung erzwungen werden kann.

Der Aufbau eines BCM (Business Continuity Management, bspw. nach ISO 22301), sowie der Aufbau eines ISMS (Informationssicherheitsmanagementsystem, bspw. ISO 27001) beziehungsweise die Umsetzung des ISMS nach BSI IT-Grundschutz sind für alle privatwirtschaftlichen KRITIS-Betreiber gesetzlich verpflichtend. Gleichlaufend sollten ähnlich konkrete Regelungen und Vorschriften auch für den Sektor Staat und Verwaltung gelten. Aus unserer Sicht ist es unerträglich, dass der Staat es gegenüber der Wirtschaft für zumutbar und verhältnismäßig hält, diese zur Umsetzung des jeweils aktuellen „Stand der Technik“ zu verpflichten, diese Umsetzung in der eigenen Infrastruktur jedoch nicht durchsetzt.

Darüber hinaus halten wir es weiterhin für notwendig, das Bundesamt für Sicherheit in der Informationstechnik aus seinem Interessenskonflikt zu lösen und es vom BMI unabhängig zu gestalten. Die Rechts- und Fachaufsicht unter dem selben Ministerium, dass auch die Interessen der Sicherheitsbehörden vertritt, führt zu einem Interessenskonflikt, der die eigentlich notwendige Wahrnehmung des BSI als vertrauenswürdigen Partner auf dem Weg zu einer sicheren und resilienten IT-Infrastruktur schwächt.

Herrn Minister Pinkwart empfehlen wir in diesem Zusammenhang die Übernahme der Forderungen des Antrags auf Bundestagssdrucksache 19/7698, insbesondere Unterpunkt 2, in den Koalitionsvertrag, den er für die Fraktion der Freien Demokraten im Bundestag mitverhandelt.tischen Parteien zur Verfügung.