Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)793 F

Stellungnahme

des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI),

Arne Schönbohm,

in Vorbereitung der öffentlichen Anhörung zum Thema

"Bilanzierung des Bevölkerungsschutzes angesichts der Corona-Pandemie"

des Ausschusses für Inneres und Heimat des Deutschen Bundestages

am 12. April 2021.

Die Corona-Pandemie hat zu einem regelrechten Digitalisierungsschub geführt. Dieser beschleunigte und alles durchdringende Einsatz von Informationstechnologien sowie deren intelligente Vernetzung mit Dienstleistungs- und Produktionsprozessen stellt den Staat genauso wie die Wirtschaft und die Gesellschaft vor vielfältige Herausforderungen. IT-Sicherheit ist die Voraussetzung für eine gelungene und sichere Digitalisierung. Dies gilt jederzeit, insbesondere aber in Ausnahmesituationen wie nationalen Notständen oder Pandemien.

Der Terminus Bevölkerungsschutz ist umfassend; er beginnt mit einer möglichst breiten Lageanalyse als Voraussetzung zur Gefahrenabwehr: Nur wenn wir die Gefährdung unserer kritischen Infrastrukturen und in der Corona-Pandemie insbesondere von Impfherstellern, Laboren, dem Robert-Koch-Institut und anderen essentiellen Einrichtungen und Organisationen der Gesundheitsversorgung kennen, können wir diese eindämmen und ihnen begegnen.

Die Lage der IT-Sicherheit während der Corona-Pandemie

Der BSI- Bericht zur „Lage der IT-Sicherheit in Deutschland 2020“[1] zeigt, dass die Anzahl und Qualität der Cyber-Angriffe auf staatliche und zivile Ziele zugenommen hat. Auch die Kritischen Infrastrukturen sind verstärkt im Fokus der Angreifer. Die Abhängigkeit von der Verfügbarkeit der Kritischen Infrastrukturen v.a. im Gesundheitswesen ist durch etliche Rahmenbedingungen während der Corona-Pandemie (von Kurzarbeit bis hin zu Überlast,

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2

hohe Aus- und Belastung der Gesundheitssysteme, Arbeiten im Home-Office, Improvisation statt Regelprozesse, etc.) gestiegen.

Zahlreiche Maßnahmen im Kampf gegen die COVID-19-Pandemie stellen eine ökonomische und logistische Herausforderung für die globalisierte Weltwirtschaft und damit auch für Deutschland dar. Diese zeichnen sich durch engverzahnte und aufeinander in Abhängigkeiten aufbauende Lieferketten aus. Es ist davon auszugehen, dass diese Lieferketten unter enormen Stress stehen und nicht die Flexibilität mitbringen, die sie außerhalb einer Pandemie zeigen würden. In der Folge geht das BSI davon aus, dass die Folgen eines Cyber-Angriffs auf Organisationen, die eine Schlüsselrolle in der Versorgung der Bevölkerung einnehmen, drastischer, weil weitreichender, ausfallen werden. Dies umfasst auch Organisationen, die nur Teil einer Lieferkette sind, um ein endgültiges Produkt oder Dienstleistung der Bevölkerung anbieten zu können.

Im Kampf gegen die Pandemie und beim Schutz der Bevölkerung nimmt der Gesundheitssektor die zentrale Rolle ein. Das BSI hat bisher keine Zunahme an Angriffen gegen den Gesundheitssektor in Deutschland beobachten können. Die Cyberbedrohungslage ist jedoch in jedem Fall angespannt. Abhängig von der angegriffenen Institution im Gesundheitssektor und der Pandemieentwicklung können drastische Folgen aus einem Cyber-Angriff erwachsen, im Extremfall sogar für Leib und Leben der Bevölkerung.

Darüber hinaus stellt die COVID-19-Pandemie für Angreifer ein Thema dar, das auf unterschiedlichste Art und Weise missbraucht werden kann: Von der Nachahmung von amtlichen Portalen zur Beantragung von Corona-Hilfen über Desinformationskampagnen, das betrügerische Angebot von Produkten und Dienstleistungen bis hin zur Ausnutzung für Social Engineering bei Cyber-Angriffen. Auch die Verlagerung von Beschäftigten und Geschäftsprozessen ins Home-Office führte und führt zu Herausforderungen für die IT-Sicherheit. Das BSI unterstützt seit Beginn der Pandemie mit Empfehlungen zu technisch und organisatorischen Maßnahmen, auch um ad-hoc Lösungen in nachhaltige sichere Lösungen zum Arbeiten im „New Normal“ zu überführen.2

2 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/home-office_node.html

Bevölkerungsschutz geht nur gemeinsam: Das bewahrheitet sich auch in dieser Pandemie

Zum Schutz der Bevölkerung arbeitet das BSI seit Beginn der Pandemie eng mit dem Bundesministerium für Gesundheit (BMG), zentralen Institutionen wie PEI und RKI, den Branchenverbänden im Gesundheitswesen sowie mit sämtlichen Behörden des Nationalen Cyber-Abwehrzentrums zusammen. Im Frühjahr 2020 wurde die Versorgung mit Schutzausrüstung, technisch-medizinischen Geräten, Medikamenten, Laborbedarf und Diagnostika als neuralgische Punkte für die medizinische Grundversorgung von den Behörden des Nationalen Cyber-Abwehrzentrums und so auch des BSI identifiziert. Analog zur Dynamik des Pandemiegeschehens erfolgte in Abstimmung mit dem BMG eine kontinuierliche Risikoanalyse und Anpassung der Maßnahmen.

Schwerpunkte bilden dabei seit Anfang Juli 2020 die Unternehmen der Impfstoffforschung und -herstellung. Im Rahmen der europäischen Impfallianz wurden ausgewählte Unternehmen mit Standorten in Deutschland priorisiert. Mit diesen Unternehmen stehen die zuständigen Behörden des Nationalen Cyber-Abwehrzentrums in intensivem Austausch.

Nach Anlaufen von Produktion sowie Verteilung der Impfstoffe sind neben der Forschung auch die produktionsrelevanten Lieferketten und Distributionskanäle von entscheidender Bedeutung. Daher hat das BSI in Zusammenarbeit mit den anderen Behörden des Nationalen Cyber-Abwehrzentrums sowie mit den priorisierten Unternehmen eine Evaluation der Lieferketten vorgenommen und relevante Akteure identifiziert. Die so identifizierten rund 160 Unternehmen sind fortan in einer prioritären Bearbeitung und können Unterstützungsangebote des Bundes in Anspruch nehmen. Dazu zählen insbesondere die unmittelbare Unterstützung bei Sicherheitsvorfällen, technische Maßnahmen zur Detektion von Angriffen und die kontinuierliche Versorgung mit aktuellen Informationen über Risiken und konkrete Bedrohungen.

Durch direkten Kontakt zu den Unternehmen über das BSI bzw. den Verfassungsschutzverbund soll insbesondere das IT-Sicherheitsniveau evaluiert werden, um daraus erforderliche Maßnahmen abzuleiten. So veranstaltet das BSI beispielsweise Threat-Assessment-Workshops mit relevanten Unternehmen oder hält regelmäßige Jour Fixes inkl. aktueller Bedrohungsanalysen ab.

In Absprache mit dem BMG erfolgte erstmals auch eine Einbindung des BSI in der AG AATB (Arzneimittel-, Apotheken-, Transfusions- und Betäubungsmittelwesen), um aus Perspektive

der IT-Sicherheit neuralgische Punkte zu identifizieren, die eine Verteilung des Impfstoffs gefährden könnten. Die aufgrund von Kühlketten zum Teil logistisch komplexe Distribution der Impfstoffe ist einer der gegenwärtigen Arbeitsschwerpunkte.

Sicherheit und Bevölkerungsschutz kann nur gemeinsam gewährleistet werden: Die im Kontakt mit den Unternehmen aber auch in nationalen wie internationalen Arbeitskreisen entstehenden Informationen und Erkenntnisse werden in einer gemeinsamen Arbeitsgruppe im Nationalen Cyber-Abwehrzentrum zwischen den zuständigen Behörden unmittelbar ausgetauscht, um im Zweifelsfall schnell Maßnahmen ergreifen zu können.

IT-Sicherheit von Beginn an mitdenken

Sei es die Bedrohungslage durch Ransomware-Vorfälle wie 2016 im Lukaskrankenhaus in Neuss, 2019 bei Einrichtungen der DRK-Trägergesellschaft Süd-West in Rheinland-Pfalz und im Saarland, sowie 2020 im Universitätsklinikum Düsseldorf, oder die Angriffe auf die Europäische Arzneimittelagentur, das Paul-Ehrlich-Institut und andere: All diese beispielhaften Vorfälle verdeutlichen, dass der Schutz der IT-Systeme im Gesundheitssektor von besonderer Relevanz für den Bevölkerungsschutz ist. Dies gilt in friedlichen Zeiten genauso wie in einer Pandemie.

Das in dieser Legislaturperiode verabschiedete Krankenhauszukunftsgesetz ist ein großer Schritt in die richtige Richtung. Es sieht vor, dass mindestens 15 Prozent der beantragten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit eingesetzt werden müssen. Gleichzeitig müssen Krankenhäuser, Gesundheitsämter, Impfhersteller, sowie Institute wie das RKI auch mit entsprechenden personellen Ressourcen ausgestattet werden, um die Sicherheit ihrer IT-Systeme vornehmen zu können. Aus Sicht des BSI muss IT-Sicherheit bei allen Digitalisierungsprojekten von Anfang an mitgedacht werden. Um „security by design“ und „security by deafult“ zu erreichen, müssen mindestens 20 Prozent der aufgebrachten Mittel in IT-Sicherheit investiert werden.

Verbraucher schützen, Prävention stärken

Die Gewährleistung von Cybersicherheit ist eine gesamtstaatliche Aufgabe. Jede und jeder Einzelne kann hierbei einen entscheidenden Beitrag leisten. Als Cybersicherheitsbehörde des Bundes schützt das BSI Staat, Wirtschaft und Gesellschaft durch Prävention, Detektion und Reaktion. Die neue BSI-Aufgabe des digitalen Verbraucherschutzes sowie die Einführung des

ebenfalls im IT-SiG 2.0 vorgesehenen freiwilligen IT-Sicherheitskennzeichens sind wichtige Schritte, VerbraucherInnen transparent über die Sicherheitseigenschaften von IT-Produkten zu informieren und dadurch gleichzeitig in hohem Maße in ihrer Beurteilungsfähigkeit von IT-Produkten zu stärken. Das BSI leistet bereits heute im digitalen Verbraucherschutz einen wichtigen Beitrag zur Stärkung der Akzeptanz und des Vertrauens in digitale Dienstleistungen und Technologien.

Ziel ist, das Bewusstsein für die Gefahren im Netz zu erhöhen und zugleich Wege aufzuzeigen, wie sich jeder Einzelne effektiv schützen kann. Dies streben auch die auf zwei Jahre angelegte Informations- und Sensibilisierungskampagne zur IT-Sicherheit von BMI und BSI und das gemeinsam mit dem Verein Deutschland sicher im Netz e.V. (DsiN) herausgegebene Standardwerk für digitale AufklärerInnen, die „Cyberfibel“, an.

Prävention, Detektion, Reaktion: Das Prinzip der Corona-Warn-App

Für einen gelingenden Bevölkerungsschutz in der Pandemie müssen Informationen innerhalb von Infektionsketten rasch geteilt und dabei die persönlichen Daten gut geschützt werden. Das leistet die Corona-Warn-App.

Seit Beginn der Arbeiten an der Corona-Warn-App (CWA) führt das BSI kontinuierlich, ergänzend zum Entwicklungsprozess, Sicherheitsanalysen durch. Diese Analysen umfassen Code-Reviews und Penetrationstests. Die Entwicklung der Corona-Warn-App findet transparent in einem öffentlich zugänglichen Quellcode-Verwaltungs-System (github) statt. Dort meldet das BSI, ebenfalls transparent, die identifizierten Schwachstellen an die Entwickler. Seit der Veröffentlichung der Corona-Warn-App wurden in enger Zusammenarbeit zwischen RKI, Deutscher Telekom AG, SAP und BSI vierzehn Erweiterungen inklusive der Funktion eines Kontakt-Tagebuchs und der Abwärtskompatibilität für iOS 12.5 freigegeben und veröffentlicht. Die Erweiterungen erhöhen den Funktionsumfang der CWA und beheben identifizierte Schwachstellen. Mehr als 60 Schwachstellen konnten bereits identifiziert und behoben werden, keine davon war als „kritisch“ eingestuft.

Die Corona-Warn-App wird kontinuierlich aktualisiert und mit neuen Funktionen wie der Cluster-Erkennung oder der Einbindung der Ergebnisse von Corona-Schnelltests versehen. Das BSI begrüßt zudem die Idee, das Frontend des digitalen Impfzertifikats in die CWA einzubinden und ist, in seiner Eigenschaft als ressortübergreifender Dienstleister, bei der Entwicklung der deutschen Lösung zum Impfzertifikat beteiligt.

Fazit

Bevölkerungsschutz ist eine gesamtstaatliche Aufgabe. Bund und Länder sind gefordert, hier eng zu kooperieren, eine Zusammenarbeit aller Akteure ist für das Gelingen entscheidend. Als Cybersicherheitsbehörde des Bundes arbeitet das BSI im Rahmen der gesetzlichen Möglichkeiten eng mit den Ländern zusammen. In den vergangenen Jahren wurden bereits mit elf Bundesländern Kooperationsvereinbarungen geschlossen. Regionale Cybersicherheitsnetzwerke, wie beispielsweise das neu gegründete Kompetenzzentrum in NRW für Cybersicherheit in der Wirtschaft, unterstützen wir. Ein einheitliches, möglichst hohes länderübergreifendes Cybersicherheitsniveau ist unser aller Ziel.

Das BSI als die Cyber-Sicherheitsbehörde des Bundes definiert IT-Sicherheit als gesamtgesellschaftliche Aufgabe und gestaltet diese entsprechend partizipativ. Wir sind überzeugt, dass Sicherheit, Selbstbestimmung und Souveränität in Staat, Wirtschaft und Gesellschaft nur über einen breiten interdisziplinären, gesamtgesellschaftlichen Dialog erreicht werden kann. Wir wollen IT-Sicherheit zusammen mit Kooperationen von staatlichen, wirtschaftlichen und zivilen Akteuren stärken.
Das BSI, zuständig für die IT-Sicherheit bei Kritischen Infrastrukturen, wird selbstverständlich auch bei sämtlichen zukünftigen IT-Sicherheitsvorfällen seine gebündelte Fachexpertise bei der Bewältigung einsetzen. Damit dies bestmöglich auch in Zukunft gelingt, wäre die Verabschiedung des zweiten IT-Sicherheitsgesetzes (IT-SiG 2.0), insbesondere im Hinblick auf die kritischen Infrastrukturen sowie Unternehmen in besonderem öffentlichem Interesse, ein wichtiger Schritt.

Präsident Arne Schönbohm
Bundesamt für Sicherheit in der Informationstechnik