

07.12.2020

Antwort

der Landesregierung

auf die Kleine Anfrage 4661 vom 9. November 2020
des Abgeordneten Frank Neppe FRAKTIONSLOS
Drucksache 17/11730

Wie steht es um die IT-Sicherheit der Kritischen Infrastruktur in NRW?

Vorbemerkung der Kleinen Anfrage

Am 20. Oktober 2020 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik seinen Lagebericht: „Die Lage der IT-Sicherheit in Deutschland 2020“.¹ Neben den bereits bekannten Gefährdungsaspekten wurden dabei insbesondere die zusätzlichen Herausforderungen durch die Corona-Pandemie herausgestellt.

Hinter den aufgeführten „Cyberangriffen“ stecken zum Beispiel finanzielle Bereicherungsabsichten, aber auch Versuche gesellschaftlicher oder staatlicher Destabilisierung. (Mit „Cyberangriffen“ sind hier, abweichend von der Risikomatrix UP KRITIS², alle Arten von digitalen Angriffen gemeint, nach der vorgenannten Risikomatrix also alle Kategorien der „Branchenspezifischen Bedrohungen“ sowie der „Sektorenübergreifenden Bedrohungen“ mit Ausnahme der Kategorie „Höhere Gewalt“.

Eine herausragende staatliche Bedeutung haben hier Angriffe auf die Kritische Infrastruktur des Landes, also auf Organisationen, Einrichtungen, Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Gesundheit, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung sowie Staat und Verwaltung.

Der Minister des Innern hat die Kleine Anfrage 4661 mit Schreiben vom 7. Dezember 2020 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten sowie allen übrigen Mitgliedern der Landesregierung beantwortet.

- 1. Wie viele Cyberangriffe gab es in den vergangenen 12 Monaten gegen Organisationen beziehungsweise Einrichtungen der Kritischen Infrastruktur in NRW? (Bitte nach KRITIS-Sektoren aufschlüsseln.)***
- 2. In wie vielen Fällen konnten die Angriffe erfolgreich abgewehrt werden?***
- 3. Welcher finanzielle Schaden ist den betroffenen Organisationen beziehungsweise Einrichtungen durch die Angriffe entstanden?***

Datum des Originals: 07.12.2020/Ausgegeben: 11.12.2020

- 4. In wie vielen Fällen handelte es sich bei den Angriffen um „Hybride Bedrohungen“ nach der Definition des Lageberichtes?**
- 5. Welche staatlichen oder nichtstaatlichen Akteure waren Ausgangspunkt beziehungsweise Urheber der hybriden Bedrohungen?**

Die Fragen 1 bis 5 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Cyberangriffe auf Organisationen und Einrichtungen der Kritischen Infrastruktur werden nicht explizit in der Polizeilichen Kriminalstatistik erfasst. Darüber hinaus führt die Landesregierung diesbezüglich keine spezifische Statistik. Für eine vollständige Erhebung hätte es insoweit der manuellen Auswertung sämtlicher Cybercrime-Ermittlungsverfahren bedurft. Dies ist in der zur Verfügung stehenden Zeit nicht möglich.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann keine Zahlen zu den eingegangenen Meldungen durch KRITIS-Betreiber nennen, die für das Bundesland Nordrhein-Westfalen spezifiziert werden könnten. Für das BSI steht der technische Sachverhalt inklusive der möglichen oder bereits eingetretenen Folgen für die kritischen Dienstleistungen im Fokus. Die Herkunft ist zunächst nachrangig, zumal betroffene Anlagen und der Hauptsitz eines Betreibers oftmals auseinanderfallen und daher statistisch nicht erfasst bzw. automatisiert auswertbar sind.

In Bezugnahme auf den vom Fragesteller zitierten Bericht des BSI („Die Lage der IT-Sicherheit in Deutschland 2020“) und die dort auf Seite 54 aufgeführten 419 bundesweiten Meldungen ist festzuhalten, dass das IT-Sicherheitsgesetz eine Meldepflicht der KRITIS-Unternehmen gegenüber dem BSI festlegt. Die Meldepflicht umfasst nicht nur Cyberangriffe, sondern generell Störungen, die zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen geführt haben oder führen können. Als Beispiele für IT-Störungen, die nicht auf Cyberangriffe zurückzuführen und trotzdem meldepflichtig sind, gibt das BSI folgende Beispiele an:

- ein Bagger, der ein Kabel durchtrennt,
- ein Ausfall der Kühlung eines Rechenzentrums,
- ein falsch konfiguriertes System,
- ein fehlerhaftes Update oder ein fehlerhafter Patch, der eingespielt wird.

Im Übrigen wird zur grundsätzlichen Bedeutung des Themas der Kritischen Infrastrukturen für die Landesregierung in Nordrhein-Westfalen auf die Vorbemerkungen der Landesregierung in den Antworten auf die Kleinen Anfragen 3108 (Drucksache 17/8141) und 889 (Drucksache 17/2455) verwiesen.