BREMISCHE BÜRGERSCHAFT
Landtag
19. Wahlperiode

Drs. 19/1932
27.11.2018

Große Anfrage der Fraktion der FDP

Cybersicherheit in Bremen

Die Sicherheit der Datenverarbeitung ist für Privatpersonen, Firmen sowie öffentliche Einrichtungen ein relevanter Teil gesellschaftlicher Sicherheit geworden. Laut einer repräsentativen Studie im Auftrag des Digitalverbandes „Bitkom“ ist jeder zweite deutsche Internetnutzer innerhalb eines Jahres Opfer von Cybercrime, also im weitesten Sinne Internetkriminalität, geworden. Am Häufigsten kam es dabei zur Infektion mit Schadprogrammen und zum Diebstahl von Zugangsdaten für Online-Dienste und Online-Shops. Cybercrime kann für den Einzelnen dramatische Folgen haben. Dabei spielt vor allem der Verlust von Geld und persönlichen Daten, Privatsphäre und Integrität eine Rolle. Jedes zweite Opfer von Cybercrime gibt an, dass ein finanzieller Schaden, beispielsweise durch das Hinzuziehen eines Reparaturdienstes, den Kauf von Soft- oder Hardware sowie nicht erhaltender Waren, entstanden ist. Laut der Bitkom-Studie erstattet aber nur jeder sechste Betroffene Anzeige gegen den oder die Betrüger. Das Bundeskriminalamt geht in seinem Bundeslagebild Cybercrime für das Jahr 2017 von Schäden in Höhe von mindestens 71,4 Mio. Euro im Bereich Computerbetrug aus. Das entspricht einer Steigerung gegenüber dem Vorjahr von fast 40 Prozent. Kaum vertreten in dieser Statistik sind Schäden von Firmen, denen bei Eindringen in ihre IT-Infrastruktur nicht selten wertvolles Wissen oder Kundendaten gestohlen werden. Schätzungen gehen davon aus, dass Unternehmen in Deutschland 55 Milliarden Euro für die Folgen der Angriffe durch Cybercrime ausgegeben haben.

Besonders wichtig ist die Sicherheit vor Cyberkriminalität bei kritischer Infrastruktur und öffentlichen Einrichtungen. In Erinnerung bleibt die Infizierung von 450 Rechnern bei der Deutschen Bahn, die 2017 zu tagelangen Ausfällen bei Anzeigetafeln und Ticketautomaten geführt hat. Bei öffentlichen Einrichtungen steht ganz besonders die Sicherheit der ihnen zugetragenen Daten und die Funktionsfähigkeit der Verwaltung im Mittelpunkt. Im Sinne der Cyber-Sicherheitsstrategie für Deutschland des Bundesinnenministeriums ist Cybersicherheit ein anzustrebender Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyberraums auf ein tragbares Maß reduziert sind. Dem Bremer Senat obliegt eine besondere Verantwortung zum Schutz der IT-Infrastruktur. Gezielte Cyberangriffe können auf Bremer Unternehmen, auf Versorgungsunternehmen, auf die Hafenwirtschaft, auf die Sicherheitsbehörden, auf die gesamte öffentliche Verwaltung inklusive Justiz und Gesundheitswesen und auf Privatpersonen abzielen. Solche Angriffe haben potenziell eine katastrophale Auswirkung.

Dennoch arbeitet die Bremer Verwaltung immer noch mit anfälligen Closed-Source-Betriebssystemen und proprietären Büroanwendungen vornehmlich auf Microsoft-Basis. Sie ignoriert dabei Sicherheitsbedenken und die massiven Warnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), verstößt dabei mutmaßlich gegen europäisches Wettbewerbs- und Vergaberecht und macht sich abhängig von einem amerikanischen Konzern mit nachgewiesenen Spionage-Hintertüren für den Geheimdienst NSA, die auch gerne von Cyber-Kriminellen ausgenutzt werden.

Vor diesem Hintergrund fragen wir den Senat:

1. Wie viele Cyberangriffe hat es jeweils in den vergangenen fünf Jahren auf die bremische Verwaltung, auf bremische Unternehmen sowie auf kritische Infrastruktur in Bremen gegeben?
   a) Auf welche Art und Weise haben diese Angriffe stattgefunden?
   b) Welche Schäden haben diese Angriffe jeweils verursacht?
   c) Wie hoch waren die Kosten zur Behebung der Schäden durch den jeweiligen Angriff?
   d) Welche Dauer haben diese Angriffe jeweils verzeichnet?
   e) Welche Störung wurde jeweils durch den Angriff verursacht?
2. Wie hoch schätzt der Senat das Risiko von Cyberangriffen auf die öffentliche Verwaltung bzw. auf die kritische Infrastruktur in Bremen ein, die zu erheblichen Folgen (beispielsweise Ausfall des Stromnetzes oder Ausfall des öffentlichen Nahverkehrs) führen kann?
3. Inwieweit gibt es bei den zuständigen Behörden ein „Worst-Case-Szenario“ für einen Cyberangriff? Wenn ja, wie zeichnet sich dieses aus und liegen entsprechende Abwehrpläne beziehungsweise Einsatzpläne vor? Wenn nein, warum nicht?
4. Inwieweit arbeitet der Senat mit externen Hackern zusammen, die regelmäßig Angriffe („friendly attacks“) auf die Bremer Verwaltung ausüben, um Sicherheitslücken aufzudecken? Wenn ja, wie oft? Wenn nein, plant er dieses?
5. Welche Behörden und Ämter befassen sich mit jeweils wie vielen Stellen mit dem Thema Cybersicherheit und inwieweit wird dabei zwischen Cyberangriffen, Cyberspionage und Cyberkriminalität unterschieden?
6. Welche Qualifikationen haben die Mitarbeiter, die sich in den Behörden und Ämtern mit dem Thema Cybersicherheit beschäftigen und können alle Planstellen mit Fachkräften besetzt werden?
7. Inwieweit sind die bremischen Institutionen nach Ansicht des Senats im Bereich der Cyberkriminalität ausreichend gut aufgestellt und wo sieht der Senat aus welchem Grund welchen Nachholbedarf?
8. Inwiefern hat der Senat beziehungsweise haben welche zuständigen Behörden ein Konzept bezüglich einer sicheren Kommunikation der Behörden und Organisationen mit Sicherheitsaufgaben, welches vor Cyberangriffen geschützt ist?
9. Welche Aufgabe nimmt das Unternehmen Dataport im Bereich der Cybersicherheit wahr und wie gestaltet sich die Zusammenarbeit mit den Behörden und Ämtern?
10. Inwieweit kooperiert Bremen bei dem Thema Cybersicherheit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder mit den zuständigen Behörden anderer Bundesländer?
11. Inwieweit ist Bremen durch welche Institute oder Dienststellen im Bereich der Forschung und Entwicklung zum Schutz vor Cyberangriffen mit welchem Aufwand (Personal und Kosten) tätig beziehungsweise beteiligt?
12. Welche Präventionsmaßnahmen mit der Prävention zum Schutz vor Cyberangriffen nimmt der Senat beziehungsweise die zuständige Behörde vor, insbesondere bei den
    - Sicherheitsbehörden,
    - Dienststellen der öffentlichen Verwaltung,
    - den öffentlichen Versorgungsunternehmen,
    - den öffentlichen Verkehrsunternehmen,
    - der in Bremen angesiedelten Industrie und Wirtschaft sowie
    - den Hochschulen und Forschungsinstituten in Bremen?
13. Inwieweit bieten die zuständigen Behörden Beratungsgespräche für welche Zielgruppen an und in welcher Häufigkeit und von wem bzw. wie wurden diese Beratungsgespräche jeweils in den vergangenen fünf Jahren angenommen?

14. Inwieweit arbeitet der Senat beim Thema Cybersicherheit insbesondere mit kleinsten, kleinen und mittleren Unternehmen zusammen, die häufig nicht über die Ressourcen verfügen, eigene IT-Sicherheitsprogramme aufzulegen?
15. Wie viele Betroffene von Straftaten im Bereich der Cyberkriminalität erstatten jährlich bei der Bremer Polizei Anzeige und welche Schadenssummen werden dabei ermittelt?
16. Welche Erklärungen hat der Senat dafür, dass nur etwa jeder sechste Betroffene Anzeige erstattet und welche Aufklärungsmaßnahmen hält er insoweit für erforderlich?
17. Inwieweit hat der Senat Informationen darüber, ob und in welchem Umfang Geschädigte auf zivilrechtlichem Weg Ersatz der ihnen zugefügten Schäden erhalten (haben)?
18. Wie ist die Polizei Bremen sachlich und personell bei den Ermittlungen zu Cyberkriminalität aufgestellt und hält der Senat hier aufgrund des offensichtlichen Anstiegs der kriminellen Aktivitäten eine Aufstockung der Mittel für notwendig?
19. Wieviel Ermittlungsverfahren hat es im Bereich Cyberkriminalität in den letzten fünf Jahren jeweils bei der Staatsanwaltschaft mit welchem Ausgang gegeben?
20. Wie wird das Personal zur Bearbeitung von Cyberkriminalität bei der Polizei und der Staatsanwaltschaft ausgebildet?
21. Wie häufig hat man sich in den vergangenen fünf Jahren für die sachgerechte Ermittlungsarbeit externer Sachverständiger bedient, welche Kosten sind dabei jeweils entstanden und wird dies gegebenenfalls zukünftig (weiter) für notwendig erachtet?
22. Wie stellt sich die Bearbeitungssituation (bezogen auf Anzahl der Verfahren, die durchschnittliche Bearbeitungsdauer und die Rückstände) bei der KTU für Ermittlungsverfahren im Zusammenhang mit IT-Sicherheit dar?

Peter Zenner, Lencke Steiner und Fraktion der FDP