BREMISCHE BÜRGERSCHAFT
Landtag
18. Wahlperiode

Drucksache 18/
18.07.2013

Antrag der Fraktion der CDU

Schutz vor virtuellen Angriffen verbessern

Die Digitalisierung unseres Alltags schreitet unaufhörlich voran. Internet und Mobilfunk sind die Grundlage für neue Formen der Kommunikation, des Handels, der Mobilität und der Unterhaltung geworden, die sich aus unserem Leben nicht mehr wegdenken lassen. Durch die rasante Verbreitung neuer Informations- und Kommunikationstechnologien und die Globalisierung entstehen aber auch neue Gefährdungslagen. Die deutsche Wirtschaft investiert große Summen in Forschung und Entwicklung und schafft damit die Grundlagen für Innovationen und technischen Fortschritt. Der Wettbewerbsvorteil, den sie sich hierüber erarbeitet, weckt Begehrlichkeiten bei Konkurrenzunternehmen und fremden Staaten. Diesem Risiko gilt es, innovative und ganzheitliche IT-Sicherheitskonzepte entgegenzusetzen.

Die Bedrohung durch virtuelle Angriffe mit kriminellem, terroristischem oder nachrichtendienstlichem Hintergrund auf Unternehmen, Behörden und lebenswichtige Infrastrukturen wird immer mehr zu einem zentralen Sicherheitsproblem. Dessen Bekämpfung erfordert die Zusammenarbeit von Staat, Wirtschaft und Gesellschaft. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt mit seinem Nationalen IT-Lagezentrum eine Schlüsselrolle bei der Bekämpfung der Cyber-Kriminalität in Deutschland ein. Zur besseren Koordinierung der Zusammenarbeit zwischen den verschienen Bundesbehörden wurde 2011 das Nationale Cyber-Abwehrzentrum gegründet. Unter der Federführung des BSI kooperieren dort die Nachrichtendienste des Bundes (BfV und BND), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA) und die Bundeswehr unter Wahrung ihrer jeweiligen rechtlichen Zuständigkeiten. Der Nationale Cyber-Sicherheitsrat, der sich aus Vertretern der zuständigen Bundesministerien, der Länder sowie der Wirtschaft zusammensetzt, koordiniert die übergreifenden Politikansätze für Cyber-Sicherheit. Das Land Bremen ist über den IT-Planungsrat von Bund und Ländern in den Informationsfluss eingebunden.

Das BSI hat ein Sicherheitsportal eingerichtet, auf dem interessierte Bürgerinnen und Bürger Hinweise, Warnungen und aktuelle Informationen für den sicheren Umgang mit IT und Internet erhalten. Der Verein Deutschland sicher im Netz e. V. (DsiN) fungiert als Ansprechpartner für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit. Er bündelt die Aktivitäten von Unternehmen, Branchenverbänden sowie Vereinen auf herstellerunabhängiger und produktneutraler Basis. Die Gewährleistung

der IT-Sicherheit in bremischen Behörden obliegt in erster Linie dem IT-Dienstleister Dataport (AöR) und der BREKOM GmbH (BREKOM). Für die IT-Sicherheit der kritischen Infrastrukturen im Land Bremen (Wasserver- und -entsorgung, Energieversorgung, öffentlicher Nahverkehr, Telekommunikation, Krankenhäuser etc). sind deren Betreiber verantwortlich.

Hacker- und Virenangriffe, Produktpiraterie und Cyber-Spionage machen keinen Halt vor Ländergrenzen oder Behördenzuständigkeiten. Aus diesem Grund ist auch das Land Bremen gehalten, die Schutz- und Abwehrmaßnahmen gegen Cyber-Kriminalität in seinem Einflussbereich zu verstärken, die Zusammenarbeit zwischen den Behörden untereinander und mit der Wirtschaft zu verbessern sowie kleine und mittelständische Unternehmen im Land Bremen dabei zu unterstützen, sich vor Angriffen aus dem Cyber-Raum effektiv zu schützen.

Die Bremische Bürgerschaft (Landtag) möge beschließen:

Die Bremische Bürgerschaft (Landtag) fordert den Senat auf,

1. gemeinsam mit den Kammern im Land Bremen, dem Verband für Sicherheit in der Wirtschaft Norddeutschland e.V. (VSWN) und – wenn möglich – mit den norddeutschen Küstenländern eine Sicherheitspartnerschaft gegen Wirtschaftsspionage / Wirtschaftskriminalität ins Leben zu rufen, die den Unternehmen als kompetenter Ansprechpartner in Fragen der Wirtschafts- und Cyber-Kriminalität dient, die Vernetzung fördert und folgende Themenstellungen abdeckt:
   a. Sensibilisierungen von Unternehmen und Behörden für die Gefahren durch Cyber-Angriffe und mögliche Gegenstrategien;
   b. Bereitstellung unternehmensbezogener Informationen zur Gefährdung durch Wirtschaftsspionage, Wirtschaftskriminalität, Produkt- und Markenpiraterie, Computerkriminalität, politisch motivierte Kriminalität und IT-Sicherheit;
   c. Zurverfügungstellung aktueller Lagebilder;
   d. Durchführung von Fortbildungsveranstaltungen, Beratungsgesprächen und Sicherheitstagungen sowie Hinweis auf externe Veranstaltungen und Beratungsangebote;
   e. Bereitstellung umfassender Informationsmaterialien.

2. die Medienkompetenz der Bürgerinnen und Bürger in allen Altersstufen durch geeignete Maßnahmen zu fördern; hierbei müssen staatliche Angebote noch besser mit denen der Wirtschaft verzahnt werden;

3. die Spionageabwehr des Landesamtes für Verfassungsschutz Bremen im Bereich der Cyber-Kriminalität zu verstärken und zu einem regelmäßigen Berichtspunkt im jährlichen Verfassungsschutzbericht zu machen;

4. sicherzustellen, dass die IT-Strukturen und Schutzmaßnahmen in der bremischen Verwaltung dem aktuellen Stand der Technik entsprechen, ein Höchstmaß an

Verlässlichkeit und Vertrauenswürdigkeit bieten und nach einheitlichen Standards arbeiten, die nach dem Best-Practice-Ansatz regelmäßig weiterentwickelt werden;

5. bei DATAPORT, der BREKOM und den Dienststellen mit eigener IT-Infrastruktur ausreichende personelle und technische Ressourcen für Computer Emergency Response Teams (CERT-Teams) sicherzustellen;

6. bei der Bekämpfung der Cyber-Kriminalität den Informationsaustausch und die Zusammenarbeit der bremischen Behörden untereinander, mit ihren nationalen und internationalen Partnern sowie den Betreibern kritischer Infrastrukturen im Land Bremen zu stärken und dabei das Know-how der CERT-Teams und der Wirtschaft einzubeziehen;

7. sicherzustellen, dass Polizei und Justiz im Land Bremen über die notwendigen Mittel und Kompetenzen zur Bekämpfung der Cyber-Kriminalität verfügen;

8. sich über den Bundesrat für eine Harmonisierung der unterschiedlichen rechtlichen Rahmenbedingungen für „Cloud Computing“ in den EU-Mitgliedstaaten einzusetzen mit dem Ziel, das in Deutschland geltende hohe Schutzniveau im Bereich der Datensicherheit und des Datenschutzes auch für Cloud-Anwendungen zu implementieren;

9. sich über den Bundesrat für den Abschluss eines globalen Datenschutzabkommens einzusetzen, etwa in Form eines Zusatzprotokolls in Artikel 17 des UN-Paktes für politische und bürgerliche Rechte;

10. sich über den Bundesrat für die Etablierung eines internationalen Kodex’ für staatliches Verhalten im Cyber-Raum (Cyber-Kodex) einzusetzen; bei nachrichtendienstlichen Maßnahmen muss sichergestellt sein, dass der Grundsatz der Verhältnismäßigkeit gewahrt wird.

Jörg Kastendiek, Wilhelm Hinners, Elisabeth Motschmann, Gabriela Piontkowski, Thomas Röwekamp und Fraktion der CDU