Klausurtagung der CSU-Landesgruppe in Kloster Seeon
vom 4. bis 6. Januar 2017

GEFAHREN AUS DER VIRTUELLEN WELT WIRKSAM ENTGEGENTRETEN

5. JANUAR 2017

Wir alle sind heute mehr denn je darauf angewiesen, elektronische Informationssysteme und Kommunikationswege zuverlässig und sicher nutzen zu können. Die Bedrohungen nehmen dabei aber immer mehr zu. Angriffe auf unsere Systeme sind entweder krimineller Natur oder sie haben sogar terroristische, militärische oder nachrichtendienstliche Hintergründe.

Die Kriminalität im sogenannten Cyber-Raum, in der Welt der Netze und Computer, ist auf dem Vormarsch. Die Folgen von Attacken bleiben längst nicht mehr auf die virtuelle Welt beschränkt. Auch im realen Leben drohen erhebliche Gefahren: Sabotageakte gegen die Systeme von Energieversorgern und Finanzdienstleistern, automatisierte Fahrzeuge oder sogar das Gesundheitswesen können unsere öffentliche Sicherheit und Ordnung erheblich gefährden. Politik, Wirtschaft und Wissenschaft sind technisch immer versierteren elektronischen Spionageangriffen ausgesetzt. Diese untergraben die Stabilität des Gemeinwesens und verursachen nicht nur massive wirtschaftliche Schäden, sondern beschädigen auch das Vertrauen in unsere politische und soziale Infrastruktur. Das sogenannte Darknet, in dem Nutzer anonym bleiben und digitale Währungen als Zahlungsmittel verwenden können, dient als Umschlagplatz für beinahe jede Form von illegalen Gütern. Auch der Amokschütze von München hat sich seine Waffe dort beschafft.

Aber nicht nur Angriffe auf unsere Netze, unsere notwendige Infrastruktur und neue Geschäftsfelder gefährden unser Gemeinwohl. In Onlineforen und sozialen Medien erscheinen täglich neue menschenverachtende Beiträge, die ein nicht gekanntes Maß an sprachlicher Verrohung aufweisen. In diesen sogenannten Hassnachrichten und Hasskommentaren werden Bedrohungen, Nötigungen, Verunglimpfungen, extremistische Inhalte sowie Aufrufe zu Straf- und Gewalttaten verbreitet. Mobbing im Internet hat genauso wie die sexuelle Kriminalität gegenüber Kindern und Jugendlichen im Netz erheblich zugenommen. Immer häufiger werden auch gezielte Falschmeldungen, sogenannte Fake News, über das Internet in Umlauf gebracht. Gezielte Desinformationskampagnen gegen Einrichtungen der demokratischen Willensbildung sind zu einer ernsten Bedrohung geworden.

Schutz und Sicherheit für Bürger und Unternehmen auch im Cyber-Raum zu gewährleisten, ist eine originäre staatliche Aufgabe. Handlungsfähigkeit und Souveränität unseres Landes müssen auch im digitalen Zeitalter sichergestellt sein. Denn das Internet ist kein rechtsfreier Raum. Regierung, Parlament und Streitkräfte haben bereits eine Reihe von Maßnahmen für mehr Sicherheit im Cyber-Raum ergriffen. Insbesondere die Verabschiedung des IT-Sicherheitsgesetzes im Deutschen Bundestag und die damit verbundene Stärkung des Bundesamtes für Sicherheit in der Informationstechnik waren wichtige Schritte, um den Gefahren aus der virtuellen Welt wirksam entgegenzutreten. Die bereits getroffenen Vorkehrungen für mehr Sicherheit im Cyber-Raum müssen jedoch angesichts des rasanten technologischen Wandels beständig an neue Herausforderungen angepasst und weiter erhöht werden.

Möglichkeiten zum Einsatz technischer Hilfsmittel verbessern

- Unsere Sicherheitsbehörden müssen rechtliche Handlungsmöglichkeiten zum Einsatz verfügbarer technischer Hilfsmittel erhalten. Dazu zählt vor allem auch die Befugnis zu Online-Durchsuchungen, also verdeckte Zugriffe auf fremde informationstechnische Systeme über Kommunikationsnetze im Rahmen der Strafverfolgung. Auch die Quellen-Telekommunikationsüberwachung (TKÜ), die Überwachung der Telekommunikation vor Verschlüsselung, stellt ein unverzichtbares Instrument der Strafverfolgung dar. Im Lichte der verfassungsgerichtlichen Rechtsprechung ist eine eigenständige Rechtsgrundlage für den verbesserten Einsatz der Quellen-TKÜ zu schaffen. Quellen-TKÜ und Online-Durchsuchungen müssen auch von Polizei und Verfassungsschutz durchgeführt werden können.
- Die Speicherung und Erhebung von Telekommunikationsverkehrsdaten muss praxisgerecht fortentwickelt werden. Einzubeziehen sind künftig auch der E-Mail-Verkehr und sonstige Kommunikationsdienste (WhatsApp, Skype). Die Speicherfrist muss verlängert werden. Die Zugriffsmöglichkeiten sind zu erweitern. Zudem ist eine Nutzung auch in weiteren Fällen, etwa bei Terrorismusfinanzierung, Zuhälterei und Wohnungseinbruchsdiebstahl unerlässlich. Es muss auch unseren Nachrichtendiensten unter klar definierten Voraussetzungen erlaubt sein, auf die gespeicherten Verkehrsdaten zugreifen zu können.
- Im Falle eines Cyber-Angriffs auf kritische, also wesentliche Informations- und Kommunikationsinfrastrukturen wie beispielsweise die Energie- oder Wasserversorgung, muss es deutschen Behörden im äußersten Fall technisch vollumfänglich möglich sein, die Attacke zu unterbinden und angreifende Server im Ausland vom Netz zu trennen. Wir wollen deshalb bei der Bundeswehr die Fähigkeiten zu Computer-Netzwerk-Operationen weiter ausbauen.

Licht in die Welt der dunklen Geschäfte bringen

- Auf der dunklen Seite des Internet ist viel Platz für illegale Geschäfte. Für die in diesem sogenannten Darknet häufig verwendeten Zahlungsmittel wie etwa Bitcoins, brauchen wir einen international geltenden Rechtsrahmen. Im Gegensatz zum über Banken abgewickelten Zahlungsverkehr wird der Einsatz digitaler Währungen im Internet bislang nur unzureichend kontrolliert. Er ist auch nur schwer zu überwachen. Kriminelle und Terroristen können weiter Finanztransaktionen tätigen, ohne dabei die eigene Identität offenlegen zu müssen. Wir begrüßen vor diesem Hintergrund, dass die europäischen Geldwäschevorschriften auf Umtausch-Plattformen für virtuelle Währungen und elektronische Geldbörsen ausgeweitet werden sollen. Weitere Schritte sind erforderlich, um auch beim Kauf von Waren und Dienstleistungen mit virtuellen Währungen die Identität der Nutzer feststellen zu können.
- Personal und Ausstattung der Sicherheitsbehörden müssen wir ständig den gewachsenen Erfordernissen anpassen, um Straftaten in der virtuellen Welt, dem Cyber-Raum, besser ahnden und bekämpfen zu können. Im Darknet, dem anonymen Marktplatz, sollen vermehrt auf das Internet spezialisierte Polizisten zum Einsatz kommen, die gezielt Geldwäsche, illegalen Waffenhandel oder die Kommunikation zwischen Terroristen aufklären.

Mobbing, sexuelle Gewalt und Desinformation im Internet zurückdrängen

- Auch zur Bekämpfung des sogenannten Cyber-Mobbings und sexueller Kriminalität gegenüber Kindern und Jugendlichen im Internet müssen wir die Fahndung durch verdeckte Ermittler im Netz drastisch intensivieren. Wir fordern zudem schärfere Strafen für Cyber-Mobbing, beispielsweise indem eine gesetzliche Grundlage für besonders schwere Fälle von Beleidigungen im Internet geschaffen wird. Solche Fälle müssen zudem in sozialen Netzwerken einfacher gemeldet und angezeigt werden können.
- Die Betreiber von sozialen Medien und sonstigen Kommunikationsdiensten müssen dabei ihrer Verantwortung gerecht werden. Sie stehen in der Pflicht, die Weiterverbreitung von Hassnachrichten und strafbaren Inhalten über ihre Internetplattformen zu unterbinden. Solche Inhalte müssen unmittelbar gelöscht, Konten gesperrt und die Sicherheitsbehörden informiert werden. Kommen die Betreiber dem nicht nach, muss dies – zum Beispiel mit Bußgeldern – sanktioniert werden können.
- Auch der Weiterverbreitung bewusst falscher Nachrichten, sogenannter Fake News, müssen wir entgegentreten. Wir müssen gegen zielgerichtete Desinformationskampagnen aus der virtuellen Welt des Internets vorgehen und Plattformbetreiber zu Richtigstellungen bzw. Gegendarstellungen verpflichten. Es darf keinesfalls hingenommen werden, dass unsere rechtsstaatlichen Strukturen gezielt

destabilisiert bzw. Einzelpersonen oder Personengruppen durch unwahre Tatsachenbehauptungen diffamiert werden. Wir fordern eine Kennzeichnungspflicht von Beiträgen in sozialen Netzwerken, die von Social-Bots, also von computerbasierten Systemen, auf Plattformen veröffentlicht werden. Wo erforderlich, werden wir dazu auch Strafbarkeitslücken schließen.

Zusammenarbeit von Behörden und Wirtschaft stärken

- Die Verantwortung für die Cyber-Sicherheit liegt in Friedenszeiten beim Bundesministerium des Innern. Sie geht im Spannungs- und Verteidigungsfall auf die Bundeswehr über. Damit ein solcher Übergang im Ernstfall reibungslos funktionieren kann, muss die Bundeswehr auch in Friedenszeiten eng im Betrieb des Nationalen Cyber-Abwehrzentrums mit eingebunden sein. Darüber hinaus ist eine enge Vernetzung des Zentrums mit den zuständigen Bundes- und Landesbehörden, internationalen Partnern, Internetdiensteanbietern und den Betreibern kritischer Infrastrukturen unabdingbar.
- Das Nationale Cyber-Abwehrzentrum soll zu einem rund um die Uhr besetzten Lagezentrum ausgebaut werden. Es soll in die Lage versetzt werden, die Cyber-Sicherheitslage in Deutschland zu erfassen, zu bewerten und im Fall eines groß angelegten Angriffs Gegenmaßnahmen einzuleiten.
- An der Universität der Bundeswehr in München entsteht ein europaweit einzigartiges Kompetenzzentrum für Cyber-Sicherheit. Wir wollen die Vernetzung von Sicherheitsbehörden, IT-Sicherheitsunternehmen sowie der Wissenschaft weiter vorantreiben und schlagen vor, den Standort München beim IT-Gipfel 2017 zum „Digital Hub“ für den Bereich IT-Sicherheit zu erklären. Langfristig soll in München und Umgebung das digitale Ökosystem für den Sicherheitsbereich in Deutschland entstehen.

Standards für Hard- und Software erhöhen

- Künftig sollen Sicherheits-Gütesiegel für internetfähige Geräte Auskunft darüber geben, dass Mindestanforderungen an die Sicherheit eingehalten werden. Die Verbraucher können zur Verbesserung der Sicherheit von IT-Produkten beitragen, indem sie diese bei der Kaufentscheidung stärker ins Kalkül ziehen.
- Auch die Hersteller und Vertriebspartner von in Deutschland verkaufter Hard- und Software müssen mehr Verantwortung für die Sicherheit ihrer Produkte übernehmen. Wir wollen eine gesetzliche Grundlage schaffen, die sie verpflichtet, Sicherheitsmaßnahmen entsprechend dem aktuellen Stand von Wissenschaft und Technik umzusetzen und Sicherheitsaktualisierungen bei bekannten Schwachstellen in ihren Produkten schnellstmöglich bereitzustellen.