19. Wahlperiode

Drucksache **19/3507**

HESSISCHER LANDTAG

21. 06. 2016

Plenum

Dringlicher Antrag
der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN
betreffend digitale Agenda für das Recht - Digitalen Hausfriedensbruch bestrafen

Der Landtag wolle beschließen:

1. Der Landtag stellt fest, dass Daten und Informationen die neue Währung der modernen Informationsgesellschaft sind. Sie haben oft einen messbaren finanziellen bzw. persönlichen Gegenwert und so ist es nicht überraschend, dass das Internet und digitale Kommunikationswege sowohl Tatort als auch Tatmittel für Kriminelle geworden sind. Die Cyberkriminalität ist seit Jahren eines der am schnellsten wachsenden Kriminalitätsfelder weltweit. In strafrechtlicher Hinsicht eröffnet die "Industrie 4.0" neue Angriffsflächen für kriminelle Aktivitäten in einem bisher nie da gewesenen Ausmaß. Auf diese Herausforderungen muss auch im rechtlichen Bereich angemessen reagiert werden. Der Staat hat hier insbesondere auch angesichts vielfacher Verletzungen verfassungsrechtlich garantierter Persönlichkeitsrechte der Bürgerinnen und Bürger durch Kriminelle eine Schutzpflicht.

2. Der Landtag bittet die Landesregierung, weiterhin für eine digitale Agenda für das Straf- und Strafprozessrecht einzutreten. Dazu gehören eine Überprüfung sämtlicher relevanter Straftatbestände sowie eine gründliche Bestandsaufnahme strafprozessualer Maßnahmen im Bereich der Internetkriminalität. Ziel ist es, der durch kriminelle Innovationsschritte bedingten Erosion des Schutzniveaus für die Bürgerinnen und Bürger im Internet und der vernetzten Welt entgegenzuwirken.

3. Der Landtag stellt fest, dass als Werkzeug zur Begehung gezielter krimineller Hacker-Attacken regelmäßig "Botnetze" zum Einsatz kommen, bei denen mittels Schadsoftware unbemerkt die Computersysteme von Bürgern zusammengeschlossen und als verbundenes Netzwerk durch den Täter ferngesteuert gemeinschaftlich Angriffe zur Überwindung von Sicherungssystemen ausführen. Bei diesen sog. DDoS-Attacken ("Dienstblockade") kontrollieren Cyberkriminelle infizierte Opfersysteme vollständig. Ist ein Opfercomputer durch die Täter mit Schadsoftware infiziert und Teil des Botnetzes, kann der gesamte Internetverkehr der Opfer durch die Straftäter abgehört und manipuliert werden. Auch die Computerhardware des Opfersystems kann unbeschränkt ferngesteuert werden. So können zum Beispiel Webcam und Mikrofon unbemerkt eingeschaltet werden, um aus den Räumen der Opfer heimlich Videos und Töne zu übertragen. Damit wird der heimische Laptop oder das Mobiltelefon zu einem machtvollen Ausspähwerkzeug in den Händen international agierender Cyberkrimineller. Die Integrität und Vertraulichkeit des informationstechnischen Systems des Opfers ist vollständig aufgehoben. Weitreichende Rückschlüsse auf die Persönlichkeit bis in den Kernbereich höchstpersönlicher Lebensgestaltung sind möglich.

4. Der Landtag begrüßt deshalb die Absicht der Landesregierung, den Gesetzentwurf zur Bekämpfung sogenannter Botnetzkriminalität in den Bundesrat einzubringen. Beabsichtigt ist, unter Heranziehung des Rechtsgedankens des § 123 StGB (Hausfriedensbruch) und des § 248b StGB (Unbefugter Gebrauch eines Fahrzeugs) das ausschließliche Gebrauchsrecht der Nutzer von Computern, Laptops und Mobiltelefonen an ihren Geräten unter strafrechtlichen Schutz zu stellen. Ein neuer § 202 e StGB soll die unbefugte Nutzung informationstechnischer Systeme unter Strafe stellen und damit das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme schützen. IT-Systeme sind angesichts ihrer Allgegenwärtigkeit und der zentralen Bedeutung für die Lebensführung vieler Bürger mindestens ebenso schutzwürdig wie das Hausrecht und das ausschließliche Benutzungsrecht an Fahrzeugen. Der bisherige strafrechtliche Schutz informationstechnischer Systeme weist angesichts des technischen Fortschritts und der damit einhergehenden stärkeren Bedrohung durch Cyberkriminelle Lücken auf, da nicht alle Angriffsarten abgedeckt werden.

Eingegangen am 21. Juni 2016 · Eilausfertigung am 21. Juni 2016 · Ausgegeben am 23. Juni 2016
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Begründung:

In den letzten vier Jahrzehnten veränderte das Internet nahezu jeden Bereich unserer Gesellschaft. Ob Arbeitsprozesse, die öffentliche Verwaltung, Onlinehandel, Partnersuche oder medizinische Versorgung: Das Internet dringt in nahezu jeden Teil unseres täglichen Lebens vor.

Daten und Informationen sind die neue Währung der modernen Informationsgesellschaft. Sie haben oft einen messbaren finanziellen bzw. persönlichen Gegenwert und so ist es nicht überraschend, dass das Internet und digitale Kommunikationswege sowohl Tatort als auch Tatmittel für Kriminelle geworden sind. Die Cyberkriminalität ist seit Jahren eines der am schnellsten wachsenden Kriminalitätsfelder weltweit.

In strafrechtlicher Hinsicht eröffnet die "Industrie 4.0", also die beginnende umfassende Vernetzung unterschiedlicher IT-Systeme wie etwa Produktionsanlagen, Marketing, Vertrieb und Einkauf, neue Angriffsflächen für kriminelle Aktivitäten in einem bisher nie da gewesenen Ausmaß. Es werden IT-Systeme angreifbar, die bislang aus dem Internet nicht erreichbar waren. Dadurch vergrößert sich das Risiko existenzgefährdender Situationen durch Ausfall oder Fehlfunktion von Produktions- oder Geschäftsprozessen erheblich.

Auf diese Herausforderungen muss auch im rechtlichen Bereich angemessen reagiert werden. Deutschland braucht eine digitale Agenda für das Straf- und Strafprozessrecht. Dazu gehören eine Überprüfung sämtlicher relevanter Straftatbestände sowie eine gründliche Bestandsaufnahme strafprozessualer Maßnahmen im Bereich der Internetkriminalität. Ziel ist es, der durch kriminelle Innovationsschritte bedingten Erosion des Schutzniveaus für die Bürgerinnen und Bürger im Internet und der vernetzten Welt entgegenzuwirken.

Eine verbesserte Medienkompetenz von Wirtschaft und Nutzer sowie technische Verbesserungen des Sicherheitsniveaus im Bereich informationstechnischer Systeme allein werden nicht reichen, um die Bürgerinnen und Bürger dauerhaft zu schützen. Erschwerend kommt hinzu, dass ein wirkungsvoller technischer Selbstschutz angesichts des Komplexitätsgrads informationstechnischer Systeme vor allem den privaten Nutzer überfordern kann. Zudem werden viele Selbstschutzmöglichkeiten wirkungslos, wenn Dritten die Infiltration des Systems gelungen ist. Darüber hinaus sind trotz aller Sicherheitsschlösser und Alarmanlagen in der realen Welt Handlungen wie der Einbruchsdiebstahl strafrechtlich sanktioniert. Eine solche vollumfängliche strafrechtliche Absicherung fehlt im Bereich der unbefugten Nutzung informationstechnischer Systeme ("Digitaler Hausfriedensbruch").

So häufen sich in letzter Zeit die Angriffe auf Internetseiten mittels sogenannter "Distributed Denial of Service (DDoS)"-Attacken, bei denen eine Vielzahl von in krimineller Absicht ausgelösten Anfragen, die an Webseiten gerichtet werden, dazu führen, dass diese vorübergehend unerreichbar sind.

Die bekanntesten Fälle in jüngster Zeit waren die Internet-Angriffe auf den deutschen Bundestag im Jahr 2015, auf ein deutsches Stahlwerk im Jahr 2014, bei dem ein Hochofen beschädigt wurde, sowie die Attacken auf den französischen Sender TV5 und die belgische Zeitung "Le Soir" im Jahr 2015. Die letzten beiden Begebenheiten zeigen, dass sich auch Terroristen dieses Mittels bedienen.

Die Werkzeuge, mit der die Täter diese Handlungen begehen, sind regelmäßig sogenannte "Botnetze". Als ein Botnetz bezeichnet man eine große Anzahl von mit dem Internet ständig oder zeitweise verbundener informationstechnischer Systeme wie Computer oder Mobiltelefone, die - von ihrem rechtmäßigen Nutzer unbemerkt - mit Schadprogrammen infiltriert sind und daher einzeln oder in ihrer Gesamtheit einer fremden Kontrolle unterliegen. Große Botnetze umfassen mehrere Millionen Opferrechner, die von dem jeweiligen sie kontrollierenden Täter einzeln oder zusammen ferngesteuert werden können.

Welches Ausmaß die heimliche Infiltration der Bürger durch Schadsoftware, die von international agierenden Straftätern eingesetzt wird, hat, wurde im Jahre 2014 offenbar, als im Rahmen von Botnetzermittlungen über 14 Millionen ausgespähte Datensätze aufgefunden wurden.

Ist ein Opfercomputer durch die Täter mit Schadsoftware infiziert und Teil eines Botnetzes, kann der gesamte Internetverkehr der Opfer durch die Straftäter abgehört und manipuliert werden. Auch die Computerhardware des Opfersystems kann unbeschränkt ferngesteuert werden, so können z.B. Webcam oder Mikrofon unbemerkt eingeschaltet werden, um aus den Räumen der Opfer heimlich Videos und Töne zu übertragen. Damit wird der heimische Laptop oder das Mobiltelefon zu einem machtvollen Ausspähwerkzeug in den Händen international agierender Cyberkrimineller. Die Integrität und Vertraulichkeit des informationstechnischen Systems des Opfers ist vollständig aufgehoben. Weitreichende Rückschlüsse auf die Persönlichkeit bis in den Kernbereich höchstpersönlicher Lebensgestaltung sind möglich.

Botnetze sind auch Handelswaren, die über kriminelle Märkte im Internet in Gänze oder in Teilen verkauft, verliehen oder vermietet werden. Wer wirksam gegen diese Handlungen vorgehen will, muss deshalb auch gegen die Hintermänner, die "Werkzeugmacher" der Kriminellen vorgehen.

Wiesbaden, 21. Juni 2016

Für die Fraktion
der CDU
Der Fraktionsvorsitzende:
Boddenberg

Für die Fraktion
BÜNDNIS 90/DIE GRÜNEN
Der Fraktionsvorsitzende:
Wagner (Taunus)