19. Wahlperiode

Drucksache **19/3005**

HESSISCHER LANDTAG

17. 03. 2016

Kleine Anfrage

der Abg. Barth, Faeser, Hofmann, Holschuh und Waschke (SPD) vom 16.12.2015

betreffend Bot-Netz-Kriminalität

und

Antwort

des Ministers des Innern und für Sport

Vorbemerkung der Fragesteller:

Mit dem Begriff Bot-Netz (Roboter-Netzwerk) wird ein Zusammenschluss mehrerer Rechner durch einen Kontrollrechner verstanden. Häufig wird der Begriff im Zusammenhang mit kriminellen Taten verwendet. Dabei werden Rechner durch Kriminelle ohne das Wissen der Benutzer dafür verwendet, Schäden zu verursachen und Straftaten zu verüben. Über das Ausspähen von Passwörtern, den massenhaften Versand von Spam-Nachrichten oder DDoS-Attacken auf Webserver hinaus, ist eine Vielzahl von Gefahrenquellen bekannt.

Vorbemerkung des Ministers des Innern und für Sport:

Bot-Netze dienen Tätern in vielfältigen Deliktsfeldern der Cybercrime als mittelbare oder unmittelbare technische Infrastruktur. Die Infektion der einzelnen Computer mit Schadsoftware und deren Zusammenschluss zu einem Bot-Netz (Vortatphase) werden dabei nicht zwangsläufig von den Tätern einer angezeigten Straftat selbst durchgeführt. Vielmehr werden Bot-Netze häufig anlassbezogen von anderen Tätergruppierungen als "Dienstleistung" im Sinne von "Crime-as-a-Service" (CaaS) vermietet.

Da Bot-Netze vielfach "nur" bloße Tatmittel zur technischen Umsetzung darstellen, spielen sie bei der Aufklärung der angezeigten Delikte (z.B. Verwertungstaten bei Vermögens- und Fälschungsdelikten) eine höchst unterschiedliche, in der Regel untergeordnete Rolle.

Bot-Netz-Kriminalität ist dem Phänomenbereich der Internetkriminalität zuzuordnen. Sowohl die hessische Polizei als auch die hessische Justiz verfügen über erprobte Konzepte zur Bekämpfung der Internetkriminalität und sind in diesem Bereich bundesweit führend.

Bereits 2007 waren in Hessen flächendeckend Fachkommissariate zur Bekämpfung der Internetkriminalität eingerichtet und für die Bekämpfung dieses Deliktsbereiches externe IT-Spezialisten eingestellt worden. Ziel war und ist es, die fachliche Kompetenz der Polizei bei den Ermittlungen im Zusammenhang mit Internetkriminalität und der Auswertung sichergestellter Datenträger zu erweitern. Das Hessische Landeskriminalamt gewährleistet die Koordinierung innerhalb der Polizei und hat seit fast zehn Jahren eine "Task Force Internet" zur Durchführung anlassunabhängiger Recherchen in Datennetzen eingerichtet.

Die zur Bekämpfung von Internetkriminalität erforderliche Aus- und Fortbildung sowie das Vorhalten der Ausstattung und deren dauerhafte Anpassung an die technische Entwicklung werden mit großem finanziellem Aufwand nachhaltig gewährleistet. Seit 2012 ist im Hessischen Landeskriminalamt eine Fachabteilung zur Bekämpfung von Cybercrime eingerichtet worden, in der Ermittlungen, Auswertung und die einschlägige Einsatzunterstützung gebündelt sind.

Bei der Justiz sind Sonderdezernate für Internetkriminalität bei nahezu allen landgerichtlichen Staatsanwaltschaften eingerichtet. Das erste Sonderdezernat zur Verfolgung von Internetstraftaten wurde in der Staatsanwaltschaft Frankfurt am Main bereits Ende 1999 eingerichtet. Bei der Generalstaatsanwaltschaft Frankfurt am Main ist seit dem 1. Januar 2010 die Hessische Zentralstelle zur Bekämpfung der Internetkriminalität (nachfolgend: ZIT) als eine Außenstelle mit Sitz in Gießen eingerichtet worden.

Eingegangen am 17. März 2016 · Ausgegeben am 22. März 2016

Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Die ZIT übt wie die weiteren Zentralstellen bei der Generalstaatsanwaltschaft Frankfurt am Main Koordinierungs- und Ausbildungsfunktionen aus und ist darüber hinaus in fachlicher Hinsicht unmittelbarer Ansprechpartner für die landgerichtlichen Staatsanwaltschaften in Fragen der Internetkriminalität und damit zusammenhängender Ermittlungsmaßnahmen. Die ZIT gibt zudem einen bundesweit bekannten Leitfaden zu dem Thema "Internetermittlungen" heraus, der allen hessischen Staatsanwaltschaften zur Verfügung steht und elektronisch bundesweit allen Polizeibediensteten verfügbar gemacht wurde.

Da für die Qualität der beschriebenen Koordinierungstätigkeit - insbesondere in Bezug auf die sich stetig und rasch verändernden Phänomene, Kriminalitätsformen und Kriminalitätstechniken von Internetkriminalität - die Erfahrung durch die Bearbeitung eigener Ermittlungsverfahren von besonderer Bedeutung ist, bearbeitet die ZIT auch nach § 145 GVG zugewiesene Einzelverfahren aus allen Bereichen der Internetkriminalität, soweit es sich um Verfahren von besonderer Schwierigkeit, besonderer Bedeutung und/oder besonderem Umfang handelt.

Die ZIT führt zudem eigeninitiativ zahlreiche gemeinsame bundesweite Sammelverfahren mit mehreren tausend Beschuldigten mit verschiedenen Ermittlungsreferaten des Bundeskriminalamts sowie verschiedenen Landeskriminalämtern. Auch über EUROPOL bzw. EUROJUST koordinierte europaweite bzw. weltweite Ermittlungsoperationen mit Bezügen zu Deutschland bearbeitet die ZIT gemeinsam mit dem Bundeskriminalamt.

Das Hessische Landeskriminalamt war ebenfalls verantwortlich an internationalen Operationen zur Bekämpfung von Cyberkriminalität beteiligt. Wegen Rauschgifthandels im sogenannten "Darknet", einem verdeckten Bereich des Internet, gelang 2014 gemeinsam mit dem US-amerikanischen FBI, EUROPOL und weltweit zahlreichen Polizeibehörden ein großer Erfolg. Tatverdächtige konnten ermittelt, umfangreiche Beweismittel und elektronische Währung (Bitcoin) sichergestellt und illegale Handelsplattformen durch das koordinierte Zusammenwirken geschlossen werden.

Seit Juni 2011 ist die ZIT aufgrund einer Absprache der Generalstaatsanwältinnen und Generalstaatsanwälte bundesweit zuständig für die beweissichernden Erstmaßnahmen in Internet-Ermittlungsverfahren des Bundeskriminalamts, sofern eine örtlich zuständige Staatsanwaltschaft noch nicht festgestellt werden kann.

Die von Hessen in der Justizministerkonferenz im Juni 2015 eingebrachte Bot-Netz-Initiative greift die Gefährdung der Bürgerinnen und Bürger sowie kritischer Infrastrukturen durch dieses Phänomen auf. Einstimmig wird das Erfordernis gesehen, diesen Risiken und Bedrohungen mit allen rechtlichen Mitteln entgegen zu treten und sich der Thematik unter verschiedenen rechtlichen Aspekten unter Berücksichtigung der Belange des Daten- und Opferschutzes anzunehmen.

Unter hessischer Federführung wird insbesondere geprüft, ob die geltenden Strafgesetze ausreichen, um der Bot-Netz-Kriminalität wirksam begegnen zu können. Die gewonnenen Erfahrungen in der Bekämpfung von Bot-Netzen gründen sich auf die bundesweit einzigartige Konstellation und den daraus gewonnenen Erfahrungen der hessischen Justizpraxis.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit der Justizministerin wie folgt:

Frage 1. Welche Informationen liegen der Landesregierung hinsichtlich der Bedrohungslage durch Bot-Netze für
a) Privatanwender
b) Unternehmen
c) öffentliche Einrichtungen
vor?

Die Gefährdung durch Bot-Netze ergibt sich aus ihren vielfältigen Einsatzmöglichkeiten für Cyberangriffe und wird für alle gesellschaftlichen Gruppen als außerordentlich hoch bewertet. Ein Bot-Netz bietet Cyberkriminellen vielfältige Möglichkeiten, da die eigentliche Schadwirkung bedarfs- und zeitgerecht aus der Ferne angepasst werden kann.

Das ZIT hat bereits mehrere große Ermittlungsverfahren im Zusammenhang mit Bot-Netz-Kriminalität geführt. Beispielhaft ist hier die internationale Operation gegen das ZeroAccess-Bot-Netz Ende 2013 zu nennen.

Große Bot-Netze umfassen mehrere Millionen Opferrechner, die von dem jeweiligen sie kontrollierenden Täter einzeln oder zusammen ferngesteuert werden können. Bot-Netze sind auch Handelswaren, die über kriminelle Märkte im Internet in Gänze oder in Teilen verkauft, verliehen oder vermietet werden. Dabei muss man indes im Blick behalten, dass jeder "Bot" ein einzelnes, kompromittiertes System darstellt, mithin also die Opferzahl bei Bot-Netz-Kriminalität

in die Millionen geht. Ein Bot ist letzten Endes ein durch Dritte unerkannt fernsteuerbarer "Zombie"-Computer, dessen Funktionen und Daten dem Täter offenstehen.

Die Infektion der Opferrechner kann insbesondere durch Anklicken von Verweisen in Spam-E-Mails, durch bloßes Aufrufen einer täterseitig verdeckt infizierten Internetseite erfolgen. Die Täter schleusen auf diesen Wegen Schadprogramme auf die geschädigten Rechner, die meist unbemerkt für kriminelle Zwecke ferngesteuert als "Bot" missbraucht werden können. Die Täter haben vielfach unbegrenzten Zugriff auf die infizierten Rechnersysteme selbst, das heißt sie können über die Daten, die Internetkommunikation als auch die Steuerung des Rechners einschließlich Mikrofon und Webcam bestimmen. Damit wird der heimische Laptop oder das geschäftliche Mobiltelefon zu einem machtvollen Ausspähwerkzeug in den Händen in der Regel international agierender Cyberkrimineller.

Gegen diese Infektionen kann sich auch der aufmerksame Computernutzer kaum zur Wehr setzen. Zurzeit gehen Schätzungen davon aus, dass etwa 40% aller internetfähigen Computersysteme in Deutschland mit Schadsoftware verseucht sind und damit potentielle Bots darstellen.

Bot-Netze werden durch die Cyberkriminellen für Erpressungen von Unternehmen (über so genannte distributed Denial of Servcie-Angriffe (dDoS)) genauso verwendet wie zum Versand von SPAM- und Phishing-Mails, die Verbreitung von weiterer Schadsoftware oder als Zwischenstationen für zielgerichtete Angriffe. Auch beim Ausspähen von Zielen im Rahmen sogenannter advanced persistent threats (zu Deutsch: fortgeschrittene, andauernde Bedrohung; Begriff für einen komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen) werden Bot-Netze verwendet, hier insbesondere um über die E-Mail-Postfächer auf den Bot-Netz-"Clients" etablierte Kommunikationsbeziehungen zu finden; dieses Wissen wird anschließend für social engineering-Angriffe gegen hochwertige Ziele verwendet.

Da ein und dasselbe Bot-Netz für ganz unterschiedliche Angriffe verwendet werden kann und da die Nutzung von Bot-Netzen mittlerweile als kriminelle Dienstleistung stunden- oder tagesweise im Untergrundnetz angeboten wird, ist es nicht möglich, das Gefährdungspotenzial nach Opfergruppen zu differenzieren. Bei der Beurteilung der Gefährdung durch Bot-Netze muss auch die hohe Dunkelziffer im Bereich der Cyberkriminalität berücksichtigt werden. Bot-Netz-gestützte Angriffe gegen Unternehmen oder Organisationen haben eine größere Wahrscheinlichkeit öffentlich zu werden als eine Vielzahl von Einzelangriffen gegen Privatpersonen.

Aktuell dürften Erpressungen mit Bot-Netz-gestützten dDoS-Angriffen gegen Unternehmenswebseiten und Angriffe gegen finanzielle Transaktionen (Online-Bezahlsysteme, Online Banking) sowohl von der Zahl der Fälle als auch hinsichtlich der wirtschaftlichen Schäden Schwerpunkte der Bot-Netz-Kriminalität bilden.

Die Tatmittel-Relevanz hängt somit weniger von unterschiedlichen Zielen wie a) Privatanwender, b) Unternehmen, c) öffentliche Einrichtungen ab, sondern vielmehr vom konkreten Angriffsziel und der gewählten Methode.

Frage 2. Wie hoch beziffert die Landesregierung den durch Bot-Netz-Kriminalität verursachten finanziellen Schaden für
a) Privatanwender
b) Unternehmen
c) öffentliche Einrichtungen
jeweils in den Jahren 2005 bis heute?

Exakte Zahlen zu durch Bot-Netze entstandenen Schäden liegen weder der Polizei noch bei der hessischen Justiz vor.

Der Landesregierung ist keine Erhebung bekannt, die durch Bot-Netz-Kriminalität entstandene Schäden gesondert ausweist. Die polizeiliche Kriminalstatistik weist explizit darauf hin, dass aufgrund uneinheitlicher Erhebungsweise und aufgrund von Abgrenzungsproblemen zu klassischen Deliktarten (z.B. Erpressung vs. dDoS-Erpressung) keine belastbaren Aussagen zu Gesamtschäden durch Cyberkriminalität getroffen werden können.

Bereits im Jahr 2011 wurde der jährliche, weltweit von für Bot-Netze verantwortlicher Schadsoftware verursachte Schaden in einer Studie, die das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) im Auftrag der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) erstellt hat, auf rund 10 Mrd. USD geschätzt.

Den Medien sind für Deutschland Schadenssummen von 3,4 Mrd. € (DIW für 2014), über 54 Mrd. (Wirtschaftsberatungsgesellschaft KPMG für 2013/2014) bis hin zu 102 Mrd. € (Bitkom für 2013/2014) zu entnehmen. Diese Angaben basieren allerdings auf Hochrechnungen, die auf Grundlage von Befragungen und Schätzungen durch Hersteller von Cybersicherheitsprodukten und Wirtschaftsberatungsunternehmen vorgenommen wurden. Aus Kreisen der Telekommunika-

tionsprovider wird die Bandbreitennutzung des Internets durch Bot-Netze mit 80% beziffert. Auch hier dürfte von sehr hohen Schadenssummen auszugehen sein.

Laut Angaben eines US-amerikanischen IT-Sicherheitsdienstleisters aus dem Jahr 2013 habe das Bot-Netz "Chameleon" ab 2012 beispielsweise einen Schaden von rund sechs Millionen US-Dollar im Monat für die Werbebranche verursacht. Über dieses Bot-Netz verbreitete Schadsoftware habe automatisiert Klicks auf Werbebanner simuliert, wobei für jeden Klick eine entsprechende Vergütung für den Internetdienstleister festgelegt war. Von 14 Milliarden Klicks auf ausgewählten Webseiten seien neun Milliarden auf dieses Bot-Netz zurückzuführen.

Allein der Schaden, der für Internet-Werbetreibende durch das ZeroAccess-Bot-Netz verursacht worden sein soll, wurde Ende 2013 auf rund 2,7 Mio. USD monatlich beziffert.

In den Jahren 2010 bis 2013 ermittelte die ZIT gemeinsam mit dem BKA in einem bundesweiten Verfahrenskomplex wegen einer Vielzahl von Erpressungen von Online-Shops mittels DDos-Attacken. Insgesamt konnten nach intensiven Ermittlungen fünf Beschuldigte identifiziert und vor Gericht gestellt werden, die in unterschiedlicher Zusammensetzung für die Erpressungen verantwortlich waren. Insgesamt konnten 40 Fälle aufgeklärt werden, in denen Betreiber von Webshops mit DDoS-Attacken bedroht oder tatsächlich angegriffen wurden. Die von den geschädigten Unternehmen auf die DDoS-Angriffe zurück zu führenden, geschätzten Umsatzeinbußen beliefen sich zusammen auf Beträge im mittleren sechsstelligen Bereich. Ein Unternehmen aus Hessen erlitt ein Schaden in Höhe von ca. 65.000 €.

Frage 3. Wie beurteilt die Landesregierung die Entwicklung im Bereich der Smart-Home-Technologien hinsichtlich der Sicherheit der dabei verwendeten Datennetze?

Die Landesregierung beobachtet die Entwicklung von Smart-Home-Technologien sorgfältig. Den Chancen für neue Produkte und Dienstleistungen stehen noch nicht voll erfasste Risiken gegenüber. Besorgniserregend ist dabei der Umstand, dass die sogenannten smarten Lösungen ganz häufig aus der Kombination von klassischen Industrieprodukten mit neuen, überwiegend zugekauften digitalen Schnittstellen entstehen und Cybersicherheitsaspekte dabei nicht systematisch betrachtet werden. Dies birgt Risiken sowohl hinsichtlich der Funktionalität dieser Produkte als auch hinsichtlich eines möglichen Missbrauchs der smarten Produkte für Bot-Netze.

Frage 4. Wie hoch sind die in den jeweiligen Jahren 2005 bis heute durch die Landesregierung verausgabten Personal- und Sachmittel der mit der Bekämpfung von Bot-Netz-Kriminalität beteiligten Institutionen?

Der Personal- und Sachmitteleinsatz orientiert sich an den deliktischen Brennpunkten und den daraus abgeleiteten strategischen Schwerpunktsetzungen. Insbesondere werden Ermittlungen, die sich mit Bot-Netzen befassen, durch das HLKA und die Fachkommissariate zur Bekämpfung der Internetkriminalität in den Polizeipräsidien vorgenommen. Personelle und technische Ressourcen lassen sich jedoch nicht explizit der Bekämpfung der Bot-Netz-Kriminalität zuordnen. Gleiches gilt für die zuständigen Staatsanwaltschaften, die weder Personalkosten noch Kosten für die Auswertung im Zusammenhang mit Ermittlungen wegen Bot-Netz-Kriminalität sichergestellter Datenträger dezidiert ausweisen können.

Frage 5. Welche Maßnahmen sind zur Bekämpfung der Bot-Netz-Kriminalität erforderlich? Wenn nein, warum nicht?

Neben der Verbesserung der grenzüberschreitenden Zusammenarbeit der Strafverfolgungsbehörden erscheint es insbesondere sinnvoll, Bestrebungen auf europäischer Ebene zur Harmonisierung einschlägiger gesetzlicher Bestimmungen zu forcieren.

Ferner hat sich auf Initiative der hessischen Ministerin der Justiz die Frühjahrskonferenz der Justizministerinnen und Justizminister am 17. und 18. Juni 2015 in Stuttgart mit der Thematik befasst und das Land Hessen gebeten, sich der verschiedenen rechtlichen Aspekte anzunehmen und insbesondere zu prüfen, ob die geltenden Strafgesetze ausreichen, um der Bot-Netz-Kriminalität wirksam begegnen zu können.

Auf Grundlage dieses Beschlusses nimmt das Hessische Ministerium der Justiz derzeit eine umfassende Prüfung der Rechtslage vor, um Vorschläge für einen verbesserten Opfer- und Datenschutz im Bereich der Bot-Netz-Kriminalität zu unterbreiten.

Die Bekämpfung von Bot-Netzen kann derzeit im nationalen Kontext allenfalls partielle Erfolge erzielen, da die Angreifer, egal ob Bot-Netz-Client oder Bot-Netz-Master, in der Regel international operieren.

Unmittelbare technische Eingriffsmöglichkeiten auf nationaler Ebene bestehen nur bei den Betreibern der internationalen Netzebene ("tier 1") und bei den Internetzugangsprovidern, beispielsweise in der Unterdrückung der Kommunikation zu bekannten Command & Control-Servern der Bot-Netze. Angesichts der fortgeschrittenen, resilienten Architektur bekannter Bot-Netze ist die Wirksamkeit solcher Maßnahmen nur begrenzt.

Erste polizeiliche Überlegungen, die insbesondere die zentrale Verantwortung der Internetwirtschaft zum Gegenstand hatte, waren bereits im Jahr 2010 bundesweit durch die Landeskriminalämter unter Federführung des Bundeskriminalamtes erarbeitet worden. Ziel war es, den weiteren Missbrauch der infizierten Systeme zu unterbinden. Nach den bisherigen Erfahrungen zeigte sich diese Verfahrensweise grundsätzlich als funktionsfähig und auch anwendbar, jedoch wurde Optimierungsbedarf deutlich.

Derzeit wird ein Konzept erarbeitet, dass ergänzend die Bereinigung von infizierten Systemen im Zusammenhang mit dem durch Sicherheitsbehörden gesteuerten Herunterfahren und Abschalten von Bot-Netzen ermöglicht und für die Ermittlungen erforderliche Daten komfortabel und zeitnah bereitstellen soll.

Den größten Beitrag im Kampf gegen Bot-Netze können allerdings die Betreiber und Nutzer der informationstechnischen Geräte leisten:

- Betriebssysteme und sämtliche eingesetzte Software müssen aktuell gehalten, Sicherheitsaktualisierungen zeitnah installiert werden.
- Firewalls und Virenschutzsoftware müssen aktiviert und aktuell gehalten werden.
- Benutzer müssen bei Nutzung von Internetdiensten aufmerksam und vorsichtig agieren.

Wiesbaden, 5. März 2016

Peter Beuth