19. Wahlperiode

Drucksache **19/418**

HESSISCHER LANDTAG

04. 09. 2014

Kleine Anfrage

des Abg. Hahn (FDP) vom 14.05.2014

betreffend Datensicherheit hessischer Behörden und Auswirkungen von Cyberkriminalität

und

Antwort

des Ministers des Innern und für Sport

Vorbemerkung des Fragestellers:

In der Antwort auf die Kleine Anfrage des Abgeordneten Wolfgang Greilich (FDP) betreffend millionenfacher Diebstahl von E-Mail-Kontodaten, Drs. 19/41, hat die Landesregierung unter anderem erklärt, dass auch öffentliche Stellen in Hessen von dem Diebstahl von Email-Kontodaten betroffen waren. Insgesamt seien dem hessischen Computer Emergency Response Team (CERT-HE) 50 betroffene Adressen aus dem Netz der Landesverwaltung mitgeteilt worden.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister für Finanzen und dem Minister für Wirtschaft, Energie, Verkehr und Landesentwicklung wie folgt:

Frage 1. Wie viele Cyberangriffe auf das Datennetz sowie den Datenverkehr der Landesregierung wurden in den Jahren 2009 bis 2013 sowie im 1. Quartal 2014 registriert?

Folgende Angriffe auf das IT-System am Internetübergang sind seit 2009 registriert worden:

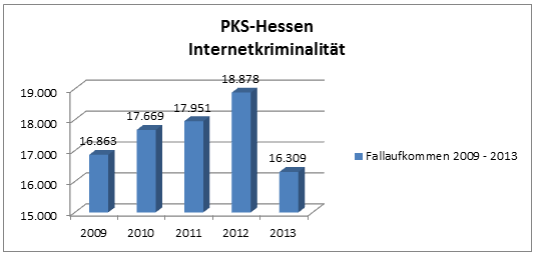
2009:	1
2010:	1
2011:	1
2012:	1
2013:	2
Q1‘ 2014:	2

Daneben werden zur Zeit jährlich ca. 200 Millionen SPAM-Mails bzw. Mails unklaren Ursprungs, ca. 250.000 Schadprogramme sowie viele tausend Portscans (feindliche Aufklärungsversuche) und andere unspezifische Angriffe mit steigender Tendenz von unterschiedlichen Sicherheitselementen am Internetübergang bzw. in der IT-Infrastruktur abgewehrt.

Es ist in vielen Fällen nicht möglich, zwischen gerichteten und ungerichteten Angriffen bzw. Angriffswellen zu unterscheiden.

Frage 2. Welche Delikte, die der Kategorie Cyberkriminalität zuzuordnen sind, wurden im unter Frage 1 genannten Zeitraum registriert und wie viele Delikte haben die hessische Landesverwaltung betroffen?

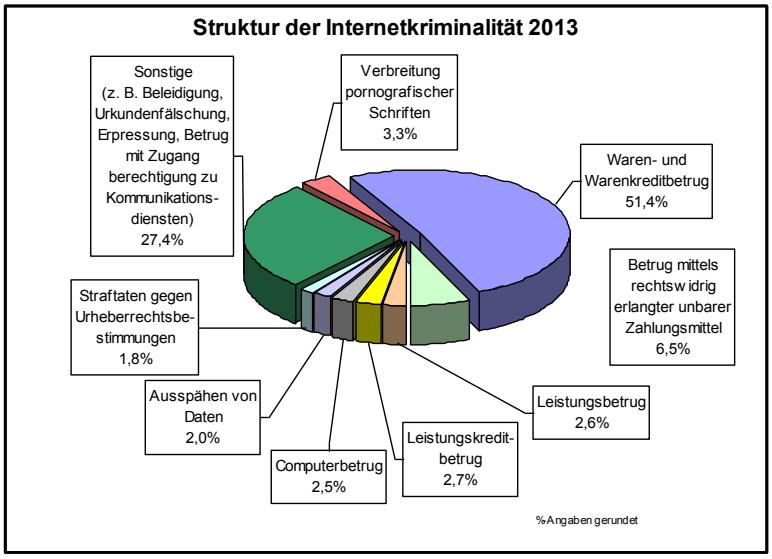
Die Fallzahlen im Bereich Internetkriminalität für die Jahre 2009 bis 2013 stellen sich wie folgt dar:



2009:	16.863
2010:	17.669
2011:	17.951
2012:	18.878
2013:	16.309

Eingegangen am 4. September 2014 · Eilausfertigung am 1. Januar 2014 · Ausgegeben am 8. September 2014
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Die Bandbreite der Delikte der Internetkriminalität und ihre prozentuale Verteilung in dem angefragten Zeitraum sind exemplarisch für das Jahr 2013 dargestellt.



Die Verteilung der registrierten Fälle der Cybercrime auf die einzelnen Phänomenbereiche im Zeitraum von 2009 bis 2013 stellt sich wie folgt dar:

	2009	2010	2011	2012	2013
Waren-/Warenkreditbetrug	7.285	7.722	7.015	7.625	8.376
Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel	1.303	1.789	1.588	2.189	1.060
Leistungsbetrug	487	711	620	354	419
Leistungskreditbetrug	786	715	668	665	442
Computerbetrug	778	1.050	1.059	854	400
Ausspähen von Daten	883	684	945	752	327
Straftaten gegen Urheberechtsbestimmungen	909	349	299	213	286
Verbreitung pornografischer Schriften	544	410	437	423	531
Sonstige Straftaten	1.884	1.965	2.526	2.754	2.001

In den Jahren 2009 bis 2013 wurden keine Ermittlungsverfahren der Cybercrime ge-führt, die sich gegen Datennetze/Computersysteme der Landesverwaltung richteten und in der Polizeilichen Kriminalstatistik (PKS) ihren Niederschlag gefunden hätten.

Seit Ende 2013 bearbeitet das Hessische Landeskriminalamt (HLKA) in der zuständigen Fachabteilung vier Ermittlungsverfahren, in denen es zur Infizierung bzw. dem Infizierungsversuch von Standardarbeitsplätzen der Landesverwaltung mit Schadsoftware (Trojaner) durch SPAM-Mails kam.

Die Zahlen für 2014 stehen erst Anfang 2015 zur Verfügung.

Frage 3. Wie hoch waren bzw. sind die Ausgaben des Landes Hessen in den Haushaltsjahren 2009 bis 2014 für Maßnahmen zur Abwehr von Cyberangriffen bzw. zur Sicherstellung der Integrität des Datennetzes und des Datenverkehrs der hessischen Landesverwaltung?

Die Ausgaben für Maßnahmen zur Abwehr von Cyberangriffen bzw. zur Sicherstellung der Integrität des Datennetzes und des Datenverkehrs der HZD werden im SAP-System der HZD nicht separat geführt und lassen sich daher in der gewünschten Form nicht exakt auswerten, sondern nur für die Kernbereiche der **IT** Sicherheit der HZD wie folgt **abschätzen**:

2009 ca. 4,2 Mio. €
2010 ca. 4,3 Mio. €
2011 ca. 5,6 Mio. €
2012 ca. 6,7 Mio. €
2013 ca. 8,2 Mio. €
2014 ca. 9,0 Mio. € (Hochrechnung auf Basis bislang vorliegender Zahlen).

Dabei ist anzumerken, dass Informationssicherheit ein integraler Bestandteil aller Leistungen der HZD und der IT-Teams der Dienststellen ist und somit bei jeder Leistungserbringung miterbracht bzw. mitbedacht wird.

Die Aufwendungen für die gesamte Landesverwaltung bestehen darüber hinaus aus einer Fülle von Aktivitäten und Leistungen, die von sicherheitsverantwortlichen Stellen in der Landesverwaltung erbracht werden sowie Bestandteil von Produktleistungen der IT-Dienstleister sind. (Vergl. hierzu auch Antwort auf die Frage 7).

Frage 4. Wie hoch ist der wirtschaftliche Schaden für das Land Hessen, der aus den Cyberangriffen bzw. der Delikte aus der Kategorie Cyberkriminalität im unter Frage 1 genannten Zeitraum resultiert?

Der wirtschaftliche Schaden von Cyberangriffen wird im SAP-System nicht separat geführt, da eine spezifische Erfassung der damit verbundenen Kosten nicht angemessen bzw. nicht möglich ist.

Der Abwehr von Cyberangriffen und der Prävention können erhebliche Aufwendungen für Sach- und Personalkosten zugerechnet werden. So orientiert sich die IT-Sicherheit im DV-Verbund der hessischen Landesverwaltung insgesamt an den BSI-Grundschutzkatalogen und der DIN ISO-Norm 27.001. Demzufolge werden IT-Verfahren in der hessischen Landesverwaltung grundsätzlich einer Risikoanalyse unterzogen und - mit teils erheblichem Aufwand - angemessen geschützt.

Frage 5. Wie hoch ist der wirtschaftliche Schaden für die hessische Wirtschaft, der aus Delikten, die der Kategorie Cyberkriminalität zuzuordnen sind, im unter Frage 1 genannten Zeitraum entstanden?

Die Schäden die der hessischen Wirtschaft aus Delikten entstehen die der Kategorie Cyberkriminalität zuzuordnen sind, sind statistisch nicht erfasst. Demzufolge ist die Beantwortung der Frage nicht möglich.

Frage 6. Bedient sich die Landesregierung bei der Verbesserung der Cybersicherheit neben den bekannten Stellen wie dem Hessischen Zentrum für Datenverarbeitung (HZD), der Zentralstelle zur Bekämpfung von Internetkriminalität (ZIT) oder dem hessischen Computer Emergency Response Team (CERT-HE) weiterer Stellen, insbesondere auch privater Dienstleister?

Das CERT-Hessen ist mit dem Bund (insbesondere dem Bundesamt für die Sicherheit in der Informationstechnik (BSI)), den Ländern (Verwaltungs-CERT-Verbund), den Kommunen sowie Stellen aus Wissenschaft und Wirtschaft vernetzt. In diesem Kontext wurde eine formale Vereinbarung mit dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) zum vertraulichen Austausch von Informationen geschlossen, die auch für den Informationsaustausch im Verwaltungs-CERT-Verbund gilt (Nutzung des sog. Traffic-Light-Protokolls (TLP), um Vertrauensschutz bei der Verwendung bestimmter Informationen durch Dritte herzustellen).

Das Hessische Ministerium des Innern und für Sport (HMdIS) hat bereits im Jahre 2011 das Kompetenzzentrum für Cybersicherheit eingerichtet, welches den regelmäßigen Informationsaustausch zwischen allen im Bereich Cybersicherheit aktiven Dienststellen und Institutionen organisiert und fördert.

Teilnehmer sind:

(1) Abteilung VII des HMdIS
(2) Geschäftsführung des Landeskrisenstabes
(3) Landespolizeipräsidium
(4) Hessisches Landeskriminalamt
(5) Hessisches Landesamt für Verfassungsschutz
(6) Hessischer Beauftragter für Datenschutz
(7) Hessische Zentrale für Datenverarbeitung
(8) Hessisches Competence Center für Neue Verwaltungssteuerung
(9) Hessisches Immobilienmanagement
(10) Zentralstelle für Internet-Kriminalität bei der Generalstaatsanwaltschaft (ZIT)

(11) Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung

(12) Hessisches Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz

Anlass- und themenbezogen werden Vertreter der Cybersicherheits-Forschung insbesondere aus dem Umfeld der TU Darmstadt (Fraunhofer SIT, "center for advanced security research in Darmstadt" (CASED)) beigezogen.

Das HMdIS ist darüber hinaus Mitglied in der Allianz für Cybersicherheit, welche sich insbesondere dem Informationsaustausch mit der Wirtschaft in Fragen der Cybersicherheit widmet.

Grundsätzlich bedient sich die hessische Landesverwaltung für den Bereich Cybersicherheit eigener Mitarbeiter und der Dienstleistungen der HZD. Die HZD steht kontinuierlich mit Herstellern der von ihr eingesetzten Produkte zum Zwecke der sicheren Leistungserbringung in Verbindung.

Darüber hinaus werden punktuell - insbesondere von der HZD - private IT-Sicherheitsdienstleister genutzt, um die eigene Kompetenz gezielt zu ergänzen oder Kapazitätsengpässe auszugleichen.

Frage 7. Was unternimmt die Landesregierung, um die Sicherheit der IT-Infrastruktur der hessischen Landesverwaltung weiter zu verbessern?

Gemäß der im Kabinett verabschiedeten Informationssicherheitsleitlinie des Landes (StAnz 4/2010 S. 106) sind in allen Verwaltungen in Hessen IT-Sicherheitsbeauftragte benannt, die über den Arbeitskreis IT-Sicherheit von der Geschäftsstelle IT-Sicherheit im HMdIS organisiert sind. Dort nehmen u.a. Vertreter des Hessischen Datenschutzbeauftragten, der HZD, der ekom21, des Rechnungshofs, des Landtags, des Landesamtes für Verfassungsschutz und des Hessischen Landeskriminalamtes teil.

Darüber hinaus baut die Landesregierung das CERT-Hessen weiter aus. Der Warn- und Informationsdienst des CERT-Hessen wird noch in 2014 auch den hessischen Kommunen zur freiwilligen Nutzung angeboten. In einem weiteren Schritt sollen auch vor allem kleine und mittlere Unternehmen in Hessen (KMU) die Möglichkeit erhalten, Dienste des CERT-Hessen in Anspruch nehmen zu können.

Gemeinsam mit dem Hessischen Datenschutzbeauftragten untersuchen das HMdIS und der CIO der Landesregierung derzeit die IT-Sicherheitsarchitektur mit dem Ziel, sie auch mit Blick auf die Erkenntnisse aus der NSA-Spähaffäre, weiter zu entwickeln. Eine Maßnahme in diesem Kontext ist die Prüfung, wie der bisher begrenzte Piloteinsatz von Detektionssystemen (Intrusion Detection Systemen - IDS) im HMdIS und der HZD auf die gemeinsame Infrastruktur (Landesnetz, zentrale Betriebsbereiche in der HZD) ausgeweitet werden kann.

Frage 8. Hält es die Landesregierung für erforderlich, zukünftig die Forschung im Bereich der Cybersicherheit sowie die Zusammenarbeit mit anderen Bundesländern, dem Bund und EU-Institutionen zu intensivieren, um die Sicherheit der Datensysteme und des Datenverkehrs zu verbessern?

Die Landesregierung begrüßt und unterstützt länderübergreifende Vorhaben. Verstärkte Zusammenarbeit mit anderen Bundesländern bietet die Möglichkeit, die knappen Ressourcen zu bündeln und effektiv einzusetzen. So hat der hessische Innenminister in der Frühjahrssitzung 2014 der Innenministerkonferenz (IMK) die Initiative für die Bildung von Kooperationen im Bereich der operativen Cybersicherheit ergriffen; die IMK hat entsprechende Prüfaufträge beschlossen und das Land Hessen gebeten, die Prüfungen im Kontext der länderoffenen IMK-Arbeitsgruppe Cybersicherheit - dort hat Hessen den Vorsitz - vorzunehmen.

Die Landesregierung teilt im Übrigen die im nationalen Cyber-Sicherheitsrat der Bundesregierung - hier vertritt Hessen gemeinsam mit dem Land Baden-Württemberg die Bundesländer - formulierte Auffassung, dass Deutschland seine im internationalen Vergleich gute Position in der Cybersicherheitsforschung nutzen sollte, um die nationalen und europäischen Interessen auf dem Gebiet der Cybersicherheit besser wahren zu können. Die bisherige Konzentration auf wenige Forschungszentren, wie beispielsweise das LOEWE-geförderte center for advanced security research in Darmstadt (CASED), ist in diesem Kontext ein zielführender Ansatz.

Wiesbaden, 22. August 2014

In Vertretung:
Werner Koch