



HESSISCHER LANDTAG

15. 04. 2014

Kleine Anfrage

des Abg. Greilich (FDP) vom 29.01.2014

betreffend millionenfacher Diebstahl von E-Mail-Kontodaten

und

Antwort

der Ministerin der Justiz

Vorbemerkung des Fragestellers:

Mitte Januar 2014 wurde bekannt, dass Kriminelle massenhaft Online-Zugangsdaten zu E-Mailkonten von Bürgerinnen und Bürgern über Schadsoftware ausgespäht haben. Insgesamt sind bei der Analyse von automatisierten Computer-Netzwerken (sog. "Bot-Netzwerken") Daten von 16 Millionen E-Mail-Konten entdeckt worden. Falls die Zugangsdaten identisch mit anderen Nutzerkonten der Betroffenen sind, beispielsweise bei Onlineshopping-Portalen oder sozialen Netzwerken, können die Täter ebenfalls auf diese zugreifen und immensen Schaden verursachen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat deshalb eine Internetseite eingerichtet, auf der Nutzer überprüfen können, ob ihre Zugangsdaten ausgespäht wurden. BSI-Präsident Michael Hange räumte allerdings ein, dass die Behörde bereits mehrere Wochen vor der offiziellen Bekanntgabe und Bereitstellung des Sicherheitschecks von dem Datendiebstahl wusste. Die Vorbereitungen eines entsprechenden Prüfprogrammes und die Klärung von Datenschutzfragen seien jedoch so umfangreich gewesen, dass ein schnelleres Handeln nicht möglich gewesen sei.

Diese Vorbemerkungen des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister des Innern und für Sport wie folgt:

Frage 1. Seit wann war der Hessischen Landesregierung die massenhafte Ausspähung von E-Mail-Kontozugangsdaten bekannt?

Der Vorgang wurde der Landesregierung durch die Presseveröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 21. Januar 2014 bekannt.

Frage 2. Gibt es derzeit Erkenntnisse, ob die Angriffe auch von Hessen aus bzw. über in Hessen befindliche Server ausgeführt wurden?

Dem Hessischen Ministerium der Justiz und dem Hessischen Ministerium des Innern und für Sport liegen keine Hinweise darüber vor, dass von Hessen aus bzw. über in Hessen lokalisierte Server eine Ausspähung von Daten im Zusammenhang mit den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldeten Sachverhalten erfolgte.

Frage 3. Gibt es in der Sache Ermittlungen durch hessische Strafverfolgungsbehörden?

Frage 4. Wie viele Nutzer aus Hessen sind betroffen? Wie hoch sind die bisher bekannten finanziellen Schäden?

Die Fragen 3. und 4. werden zusammen beantwortet. Das Ermittlungsverfahren im Zusammenhang mit dem millionenfachen Ausspähen von E-Mail-Kontodaten wird von der niedersächsischen Staatsanwaltschaft Verden geführt.

Wie bereits in der Antwort zu Frage 2. ausgeführt, liegen keine Hinweise dafür vor, dass das Ausspähen der Daten auch von Hessen aus bzw. über in Hessen befindliche Server ausgeführt wurde. Daher werden insoweit durch die hessischen Polizeidienststellen derzeit keine entsprechenden Ermittlungen geführt.

Anzeigen einzelner Geschädigter sind der Generalstaatsanwaltschaft - Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) - bislang nicht bekannt geworden. Nach Auskunft des Hessischen Landeskriminalamtes sind dort vier geschädigte Nutzer aus Hessen bekannt. Bei einem

dieser Fälle soll es zu einer missbräuchlichen Verwertung der unrechtmäßig erlangten Daten mit einem Schaden von 50 € gekommen sein (Stand: 29. Januar 2014).

Frage 5. Sind auch öffentliche Stellen in Hessen von dem Datendiebstahl betroffen?

Das Computer Emergency Response Team Niedersachsen (N-CERT) hat dem hessischen Computer Emergency Response Team (CERT-HE) im Rahmen der Amtshilfe am 4. Februar 2014 insgesamt 50 betroffene Adressen aus dem Netz der Landesverwaltung mitgeteilt. Diese Adressen wurden nach Abstimmung des Verfahrens mit dem Hessischen Datenschutzbeauftragten den IT-Sicherheitsbeauftragten der jeweiligen Dienststellen persönlich und verschlossen übergeben.

Frage 6. Was unternimmt die Landesregierung, um die Datensicherheit im Internet zu erhöhen und hessische Nutzerinnen und Nutzer vor solchen digitalen Übergriffen zu schützen?

Die Hessische Landesregierung hat ihre Anstrengungen im Bereich Cybersicherheit in den letzten Jahren konsequent fortgeführt. Derzeit werden die bestehenden IT-Sicherheitsprozesse (CERT-HE) ausgebaut, um deren Dienste auch den hessischen Kommunen und in einem zweiten Schritt kleinen und mittleren Unternehmen anbieten zu können.

Das Hessische Ministerium des Innern und für Sport ist seit Gründung im nationalen Cybersicherheitsrat als Ländersprecher neben Baden-Württemberg vertreten und führt den Vorsitz in der länderoffenen IMK-Arbeitsgruppe "Cybersicherheit".

Bereits im Jahr 2007 hat Hessen als erstes Bundesland mit der flächendeckenden Einrichtung von Internetfachkommissariaten und Internet-Präventionsberatern in allen Polizeipräsidien begonnen. Im Hessischen Landeskriminalamt wurden die "Kompetenzstelle für Cybercrime" und die "Virtuelle Streife" - die "Taskforce Internet" - zentral eingerichtet. Für diese Zwecke sind 57 zusätzliche Stellen im Polizeivollzug bereitgestellt worden. Außerdem konnten neun externe IT-Spezialisten eingestellt werden, die ihre Kompetenz gewinnbringend in die polizeilichen Ermittlungen und Auswertungen einbringen. Eine personelle Verstärkung um 14 Verwaltungsangestellte im Bereich der Datenträgerauswertung rundet das Personalkonzept ab. Die hessische Polizei ist somit personell gut und kompetent aufgestellt sowie technisch auf hohem Niveau ausgestattet.

Durch die Einrichtung der neuen Abteilung "Cybercrime und IuK-Einsatzunterstützung" im Hessischen Landeskriminalamt konnte Anfang 2012 ein weiterer wichtiger Schritt zur Optimierung der Bekämpfung von Cybercrime in Hessen getan werden. So konnten erstmals Ermittlungen, Auswertungen, Internetrecherchen, IT-Beweissicherung und Telekommunikationsüberwachung zentral und hoch kompetent in einer Abteilung gebündelt werden. Zur Bekämpfung der Cyberkriminalität stehen seit Januar 2012 mehr als 70 IT-Experten, Informatiker und Fachingenieure zur Unterstützung für die Ermittler im Land zur Verfügung. Insbesondere mit dieser Fachabteilung im Hessischen Landeskriminalamt kann der Schutz von Bürgerinnen und Bürgern, Unternehmen und empfindliche Infrastruktureinrichtungen deutlich erhöht werden.

Alle Kompetenzen im Bereich der Cybersicherheit werden in der Stabstelle "Kompetenzzentrum Cybersicherheit" im Hessischen Ministerium des Innern und für Sport zusammengeführt, um eine übergreifende Koordination, einen regelmäßigen Informationsaustausch und eine abgestimmte strategische Ausrichtung zu gewährleisten.

Mit der "Zentralstelle zur Bekämpfung der Internetkriminalität" (ZIT) verfügt Hessen seit Januar 2010 über die bundesweit erste Organisationseinheit einer Generalstaatsanwaltschaft, deren Aufgabe speziell die Bekämpfung der Internet- und Computerkriminalität ist.

Die ZIT hat ihre besondere Expertise seitdem in vielen Ermittlungsverfahren erfolgreich unter Beweis gestellt. Dabei handelt es sich regelmäßig um äußerst umfangreiche Ermittlungskomplexe aus den Deliktsbereichen "sexueller Missbrauch von Kindern und Kinderpornographie" und der sogenannten "Underground Economy". Hessen nimmt damit im Bereich der Bekämpfung der Internetkriminalität eine Vorreiterrolle in Deutschland ein.

Bundesweit einzigartig ist insbesondere das hessische Konzept einer Doppelfunktion, das die Erfahrung aus der eigenen operativen Ermittlungstätigkeit der ZIT mit Aufgaben der Weiterbildung und Grundlagenarbeit bündelt.

Der Modellcharakter der ZIT zeigt sich des Weiteren auch daran, dass auf der Tagung der Generalstaatsanwältinnen und Generalstaatsanwälte im Mai 2010 eine ständige Arbeitsgruppe zur Bekämpfung der Informations- und Kommunikationskriminalität (AG IuK) eingesetzt worden ist, die seitdem vom hessischen Generalstaatsanwalt in Frankfurt am Main geleitet wird.

Seit Juni 2011 kommt der ZIT darüber hinaus eine bundesweite Eilzuständigkeit für beweis-sichernde Erstmaßnahmen in Internet-Verfahren des Bundeskriminalamtes bei noch ungeklärter örtlicher Zuständigkeit zu.

Wiesbaden, 31. März 2014

Eva Kühne-Hörmann