19. Wahlperiode

Drucksache **19/4578**

HESSISCHER LANDTAG

18. 04. 2017

Kleine Anfrage

des Abg. Holschuh (SPD) vom 23.02.2017

betreffend Krypto-Trojaner

und

Antwort

des Ministers des Innern und für Sport

Vorbemerkung des Ministers des Innern und für Sport:
IT-Sicherheitsvorfälle sind in der Hessischen Landesverwaltung meldepflichtig. Mit der Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016)[1] wurde die Meldepflicht dahin gehend präzisiert, dass alle Sicherheitsvorfälle zu erfassen und an die zuständige Stelle im Ressort zu melden sind. Sicherheitsvorfälle, die andere Dienststellen beeinträchtigen können, sind darüber hinaus an das CERT-Hessen[2] zu melden. Das CERT-Hessen bewertet die Meldungen, initiiert und überwacht die Umsetzung notwendiger Gegenmaßnahmen. Sofern ein Sicherheitsvorfall bedeutende Störungen von IT-Diensten verursacht oder in der weiteren Entwicklung verursachen könnte, wird der CISO[3] informiert. Sind die Informationen zum Sicherheitsvorfall geeignet zum besseren Schutz der Informationstechnik des Bundes und der anderen Länder beizutragen, erstellt das CERT-Hessen eine Meldung für den Verwaltungs-CERT-Verbund.

Die Infektion mit Schadsoftware vom Typ Krypto-Trojaner bzw. Ransom-Ware gehört zur Kategorie der sofort an das CERT-Hessen zu meldenden Sicherheitsvorfälle.

Die Beantwortung erfolgt auf Basis der nach diesen Prozessen von den betroffenen Dienststellen der Landesverwaltung gemeldeten Sicherheitsvorfälle.

Krypto-Trojaner gehören seit Ende 2015 zu den großen Herausforderungen für IT-Verantwortliche. Mit der Erpressung von Lösegeld haben die Angreifer einen Weg gefunden, ihr Wissen über Lücken und Schwachstellen in IT-Systemen zu monetarisieren. Das kriminelle Geschäftsmodell ist so erfolgreich, dass ständig neue Angreifer-Gruppierungen auftreten und die Angriffsmethoden in kürzester Zeit an neue Sicherheitsmaßnahmen angepasst werden.

Den meisten Angriffen mit Krypto-Trojanern ist gemein, dass der Angreifer den Benutzer durch geschickte Manipulation dazu bewegt, die Schadsoftware selbst auszuführen. Diese Methoden zur Manipulation (social engineering) wurden in den letzten 18 Monaten deutlich verbessert und sind mitunter auch für aufmerksame und vorsichtige Benutzer kaum zu erkennen. Bestes Beispiel ist die letzte Angriffswelle aus dem Dezember 2016, bei der die Schadsoftware in vermeintlichen, per E-Mails zugesandten Bewerbungsunterlagen versteckt war; dabei bezogen sich die Zusendungen auf konkrete, aktuelle Ausschreibungsverfahren.

Diese Vorbemerkung vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

---

[1] (11. Juli 2016, StAnz. 31/2016, S.802)
[2] Computer-Emergency Response Team, im Jahr 2014 im HMdIS eingerichtet
[3] Chief Information Security Officer, der zentrale Informationssicherheitsbeauftragte der Landesverwaltung

Eingegangen am 18. April 2017 · Bearbeitet am 18. April 2017 · Ausgegeben am 20. April 2017
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Frage 1. Welche Hessischen Dienststellen wurden durch den sogenannten Krypto-Trojaner infiziert und welche Auswirkungen auf den Betrieb sind entstanden?

Datum des Vorfalls	Dienststelle	Auswirkung
01.12.2015	Amtsgericht Fürth	In einem Ordner einer Abteilungsablage (Datei-Server im Netzwerk) wurden 727 Dateien verschlüsselt; das AG Fürth wurde zur Analyse und Wiederherstellung für ca. 1 Werktag vom Landesnetz getrennt; Wiederherstellung der Daten aus der Datensicherung
08.02.2016	Hessische Zentrale für Datenverarbeitung	Verschlüsselung einzelner Dateien auf einer zentralen für verschiedene Kunden bereitgestellten Dateiablage in der HZD; ca. 1 Tag Ausfall der Dateiablage (Sperrung bzw. nur lesende Zugriffe); Wiederherstellung aus der Datensicherung
09.02.2016	Hessen Competence Center (OFD)	keine Auswirkungen auf den Betrieb gemeldet
09. - 10.02.2016	Hessen Mobil	8 infizierte PCs, ca. 1 Mio. verschlüsselte Dateien auf 8 Datei-Servern; der Aufwand zur Wiederherstellung wurde von Hessen Mobil auf ca. 8 Personentage geschätzt
10.02.2016	Finanzamt Friedberg	1 infizierter PC, keine verschlüsselten Dateien, keine Auswirkungen auf den Betrieb
14.04.2016	Hessisches Competence Center (OFD)	1 infizierter PC, keine verschlüsselten Dateien, keine Auswirkungen auf den Betrieb
06.12.2016	Amtsgerichte Wiesbaden und Darmstadt	Keine Angaben zur Anzahl der infizierten PCs, Krypto-Schadsoftware aus der Golden Eye-Kampagne; vollständige Verschlüsselung der Dateien zweier Amtsgerichte
07.12.2016	Oberfinanzdirektion	34 infizierte PCs (Golden Eye), aber keine Verschlüsselung von Daten; keine Auswirkungen auf den Betrieb
07.12.2016	Amtsanwaltschaft Frankfurt	keine weiteren Angaben und keine Auswirkungen auf den Betrieb gemeldet
07.12.2016	Statistisches Landesamt	1 infizierter PC; keine Auswirkungen auf den Betrieb gemeldet
24.01.2017	Regierungspräsidium Kassel	Verdachtsfall in einem Fachverfahren zur Abfallwirtschaft, der sich nach sorgfältiger Prüfung als unbegründet erwiesen hat; ca. 1 Personentag für Analyse

In engem zeitlichem Zusammenhang mit den hier aufgelisteten Vorfällen in Dienststellen des Landes wurden dem CERT-Hessen jeweils auch Vorfälle von hessischen Kommunen gemeldet, bei denen der Schadensverlauf vergleichbare Auswirkungen hatte.

Frage 2. Wie hoch war der finanzielle Aufwand für die Beseitigung der Schäden, die der sogenannte Krypto-Trojaner in hessischen Dienststellen verursacht hat?

Der finanzielle Aufwand für die Beseitigung von Schäden, die durch IT-Sicherheitsvorfälle verursacht wurden, wird nicht systematisch erfasst. Daher kann diese Frage über die punktuellen Angaben aus der Beantwortung der Frage 1 hinaus nicht beantwortet werden.

Wiesbaden, 3. April 2017

Peter Beuth