

An die  
Präsidentin des Nationalrats  
Doris BURES  
Parlament  
1017 Wien

GZ: BKA-353.110/0114-I/4/2016

Wien, am 15. Februar 2017

Sehr geehrte Frau Präsidentin,

die Abgeordneten zum Nationalrat Brückl, Kolleginnen und Kollegen haben am 15. Dezember 2016 unter der **Nr. 11140/J** an mich eine schriftliche parlamentarische Anfrage betreffend gezielte Trojaner-Attacken gegen die öffentliche Verwaltung gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu den Fragen 1 und 2:

- *Wie viele Rechner der öffentlichen Verwaltung sind in den letzten 5 Jahren von derartigen Trojanern befallen worden?*
- *In wie vielen Fällen wurde dabei in welcher Höhe Lösegeld geleistet?*

Das Government Computer Emergency Response Team (GovCERT), zuständig für die Öffentliche Verwaltung, war im genannten Zeitraum bezüglich Ransomware bei keiner Einrichtung der öffentlichen Verwaltung in einem Vor-Ort Einsatz tätig.

Zu Frage 3:

- *Wie hat sich die Anzahl der sicherheitsrelevanten Vorfälle durch gezielte Trojaner-Attacken in den letzten 5 Jahren generell entwickelt?*

Das „Geschäftsmodell Ransomware“ ist nicht neu, wurde aber in den letzten Jahren von Tätergruppen als gewinnbringend erkannt und entsprechend eingesetzt.

Hersteller von Anti-Viren-Software haben hierzu entsprechend der Spezialisierung eine deutlich umfassendere Telemetrie als das GovCERT, siehe auch [https://cert.at/reports/report\\_2015\\_chap04/content.html](https://cert.at/reports/report_2015_chap04/content.html)

Generell ist zu sagen, dass die meisten Ransomware-Infektionen keine gezielten Angriffe sind. Die Schadsoftware wird breitflächig über Spam-E-mails und Exploit-Packs auf Webseiten verteilt.

Zu Frage 4:

- *Welche Schutzmaßnahmen werden nach Bekanntwerden von gezielten Trojaner-Attacken getroffen?*

Das GovCERT hat gemeinsam mit CERT.at im März 2016 ein Whitepaper zu Ransomware publiziert, das die Bedrohung erklärt und entsprechende Gegenmaßnahmen empfiehlt. Diese Inhalte wurden auch im Dialog mit anderen Mitgliedern des CERT-Verbundes erarbeitet und enthalten daher auch Ideen und Erfahrungswerte von einigen großen Betreibern von Netzen der öffentlichen Verwaltung. Siehe dazu <https://cert.at/warnings/specials/20160325.html>.

Mit freundlichen Grüßen

Mag. KERN

