Bayerischer Landtag

17. Wahlperiode

19.07.2016 17/11799

Schriftliche Anfrage

des Abgeordneten **Florian Ritter SPD**
vom 21.03.2016

Krypto-Trojaner in Bayern

Nach Presseberichten infiziert der Krypto-Trojaner Locky in Deutschland bis zu 5000 Geräte in der Stunde. Der Trojaner verschlüsselt die Dateien der infizierten Geräte und entschlüsselt diese erst nach der Bezahlung eines „Lösegelds". Zudem breitet sich der Trojaner auch über bestehende Netzwerke auf andere Rechner aus. Ebenfalls wurde letztens bekannt, dass der Krypto-Trojaner Teslacrypt die Systeme der bayerischen Gemeinde Dettelsbach verschlüsselte hatte und diese erst nach einer Zahlung von 1,3 Bitcoin (rund 500€) wieder zugänglich waren.

Ich frage die Staatsregierung:

1. a) Wie viele Rechner und Serversysteme von bayerischen Behörden, Gebietskörperschaften und öffentlichen Unternehmen waren in den letzten fünf Jahren durch Krypto-Trojaner betroffen (bitte aufgeschlüsselt in Jahr, Name des Trojaners, Art der betroffenen Stelle, Anzahl infizierter Systeme)?
   b) Gibt es standardisierte Verfahren oder Vorgaben bezüglich der Datensicherung sowie im Umgang mit Krypto-Trojanern für bayerische Behörden, Gebietskörperschaften und öffentliche Unternehmen?
   c) Wenn ja, welche Abläufe sind dabei vorgesehen?

2. a) In welchen Fällen wurde das geforderte „Lösegeld" von den zuständigen Stellen gezahlt?
   b) Wie hoch war das gezahlte „Lösegeld" in den jeweiligen Fällen (bitte aufgeschlüsselt nach Jahr, Nennung der Behörde – Gebietskörperschaft – öffentliches Unternehmen, Höhe des gezahlten Betrags)?
   c) Wie bewertet die Staatsregierung, auch unter juristischen Gesichtspunkten, die Zahlung des „Lösegelds" in den konkreten Fällen?

3. a) In welchen Fällen wurden durch Krypto-Trojaner Daten verschlüsselt, die nicht wieder hergestellt werden konnten?
   b) Wie viele Systeme waren davon betroffen?
   c) Wie viele Gigabyte umfasste die Datenmenge der nicht wiederherstellbaren Daten?

4. a) Wie werden Mitarbeiterinnen und Mitarbeiter in bayerischen Behörden, Gebietskörperschaften und öffentlichen Unternehmen über Krypto-Trojaner, ihre Wirkungsweise und das richtige Verhalten informiert?
   b) Wie werden Mitarbeiterinnen und Mitarbeiter geschult um verdächtige E-Mails zu erkennen?
   c) Welches Vorgehen wird dabei vermittelt?

5. a) Wie oft wird das beim Bayerischen Landesamt für Verfassungsschutz angesiedelte Cyber-Allianz-Zentrum (CAZ) seit Bestehen im Juli 2013 pro Jahr angefragt (aufschlüsseln nach Jahr, Typ des Anfragers, Grund der Anfrage)?
   b) In wie vielen Fällen wurde das CAZ von den in seiner Zielgruppenbeschreibung genannten Gruppen seit Bestehen im Juli 2013 wegen einer Gefährdung durch Krypto-Trojaner angefragt?
   c) In welcher Form hat das CAZ in dieser Zeit Unternehmen, Hochschulen und Betreiber kritischer Infrastruktur (KRITIS) von sich aus über die jeweils aktuellen Krypto-Trojaner informiert (bitte um Angabe der Anzahl)?

6. a) Werden durch das CAZ auch andere Einrichtungen als die in der Zielgruppenbeschreibung genannten, wie z. B. bayerische Behörden, Gebietskörperschaften oder öffentliche Unternehmen, vom CAZ beraten und informiert?
   b) Falls nein, warum nicht?
   c) Falls ja, in wie vielen Fällen hat das CAZ von sich aus Initiative ergriffen diese Gruppen zu informieren?

7. a) Welche konkreten Hilfsangebote bietet das CAZ im Falle einer Infizierung mit Krypto-Trojanern?
   b) Da laut der Eigenbeschreibung des CAZ auf der Homepage des Bayerischen Landesamts für Verfassungsschutz auch vorgesehen ist, elektronische Angriffe aus nachrichtendienstlicher Sicht zu bewerten, frage ich die Staatsregierung, welche Erkenntnisse dem CAZ aus dieser Perspektive über Krypto-Trojaner vorliegen?
   c) Auf welche anderen Angebote können Einrichtungen sowie Bürgerinnen und Bürger, die nicht zur definierten Zielgruppe des CAZ gehören, in Bayern zurückgreifen?

8. a) Welche Kriterien müssen erfüllt sein, damit das CAZ auf seiner Webseite vor einer Schadsoftware warnt?
   b) Wie erklärt die Staatsregierung, dass das CAZ – ausweislich seiner Homepage im Internetangebot des Bayerischen Landesamts für Verfassungsschutz – im Jahr 2015 lediglich 3 Warnmeldungen veröffentlicht hat?
   c) Wie beurteilt die Staatsregieruung die Gefährdung der Zielgruppen des CAZ durch die derzeit aktuellen Krypto-Trojaner-Varianten wie Locky und Teslacrypt?

Antwort

des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
vom 03.06.2016

Vorbemerkung zum Fragenkomplex 1 bis 4
Zur Beantwortung der Fragen 1 bis 4 wurde eine Ressortumfrage durchgeführt.
Die Vorgehensweisen zur Vorbeugung von Sicherheitsvorfällen und zur Reaktion darauf folgen gesetzlichen Vorgaben und koordinierten Prozessen. In der Folge gleichen sich die Antworten der Ressorts. Zur Vermeidung von Redundanzen wurden die Antworten daher zusammengefasst.

1. a) Wie viele Rechner und Serversysteme von bayerischen Behörden, Gebietskörperschaften und öffentlichen Unternehmen waren in den letzten fünf Jahren durch Krypto-Trojaner betroffen (bitte aufgeschlüsselt in Jahr, Name des Trojaners, Art der betroffenen Stelle, Anzahl infizierter Systeme)?
3. a) In welchen Fällen wurden durch Krypto-Trojaner Daten verschlüsselt, die nicht wieder hergestellt werden konnten?
b) Wie viele Systeme waren davon betroffen?
c) Wie viele Gigabyte umfasste die Datenmenge der nicht wiederherstellbaren Daten?

Die Bereiche Landtagsamt, Bayerischer Oberster Rechnungshof (ORH), Staatskanzlei (StK), Staatsministerium für Gesundheit und Pflege (StGP) und Staatsministerium für Arbeit und Soziales, Familie und Integration (StMAS) waren bislang nicht von Krypto-Trojanern betroffen. In den Bereichen des StMAS, des Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst (StMBW), Staatsministeriums für Ernährung, Landwirtschaft und Forsten (StMELF), Staatsministeriums der Finanzen, für Landesentwicklung und Heimat (StMFLH), Staatsministeriums der Justiz (StMJ) und Staatsministeriums für Umwelt und Verbraucherschutz (StMUV) wurden Trojaner laut folgender Tabelle entdeckt[1]:

Jahr	Frage 1a Anzahl Rechner	Frage 3a Daten verschlüsselt?	Frage 3b Anzahl verschlüsselter Systeme	Frage 3c Verschlüsselte Datenmenge
Ressort:	**StMAS**			
2015	23	ja	4	1,4
Ressort:	**StMBW**			
2012	4	nein	0	0
2015	9	ja	4	450
2016	10	ja	2	500
Ressort:	**StMELF**			
2015	19	nein	0	0
Ressort:	**StMFLH**			
2015	28	ja	6	200
2016	2	ja	2	<1
Ressort:	**Staatsministerium des Innern, für Bau und Verkehr (StMI)**			
2015	13	ja	6	1,3
2016	4	nein	0	0
2012	5	nein	0	0
2013	2	nein	0	0
2014	1	nein	0	0
2015	48	nein	0	0
Ressort:	**StMUV**			
2015	2	nein	0	0

[1] Die Namen der entdeckten Trojaner werden aus Sicherheitsgründen nicht genannt, können aber informell beim StMFLH nachgefragt werden.

b) Gibt es standardisierte Verfahren oder Vorgaben bezüglich der Datensicherung sowie im Umgang mit Krypto-Trojanern für bayerische Behörden, Gebietskörperschaften und öffentliche Unternehmen?

Die technischen Verfahren zur Datensicherung beruhen auf den einschlägigen Industriestandards. Der Umgang mit Krypto-Trojanern wird durch das Bayerische E-Government-gesetz sowie im Rahmen einer Richtlinie für die Sicherheit von IT-gestützten Endgeräten geregelt.

c) Wenn ja, welche Abläufe sind dabei vorgesehen?

IT-Sicherheitsvorfälle werden dem Bayern-CERT gemeldet. Die einzuleitenden Gegenmaßnahmen sind einzelfallabhängig.

2. a) In welchen Fällen wurde das geforderte „Lösegeld“ von den zuständigen Stellen gezahlt?
b) Wie hoch war das gezahlte „Lösegeld“ in den jeweiligen Fällen (bitte aufgeschlüsselt nach Jahr, Nennung der Behörde – Gebietskörperschaft – öffentliches Unternehmen, Höhe des gezahlten Betrags)?

In keinem einzigen Fall.

c) Wie bewertet die Staatsregierung, auch unter juristischen Gesichtspunkten, die Zahlung des „Lösegelds“ in den konkreten Fällen?

Die Zahlung von Lösegeld wird grundsätzlich abgelehnt, da jede erfolgreiche Erpressung den Angreifer motiviert, weiter zu machen.

4. a) Wie werden Mitarbeiterinnen und Mitarbeiter in bayerischen Behörden, Gebietskörperschaften und öffentlichen Unternehmen über Krypto-Trojaner, ihre Wirkungsweise und das richtige Verhalten informiert?

Die Mitarbeiter werden bereits beim Eintritt in die Behörde entsprechend informiert. Dabei werden die unterschiedlichen Erscheinungsformen und Wirkungsweisen von Schadsoftware dargestellt. Ferner werden angemessene Verhaltensweisen vorgegeben.
Weitere Informationen erfolgen anlassbezogen per E-Mail und/oder durch Bekanntgabe in den Intranets.
Darüber hinaus finden Informationsveranstaltungen und Schulungen statt. Zudem wird den Mitarbeitern über ein eLearning-Portal ein aktueller Kurs zum Thema IT-Sicherheit angeboten.

b) Wie werden Mitarbeiterinnen und Mitarbeiter geschult um verdächtige E-Mails zu erkennen?

Siehe hierzu auch Antwort zu Frage 4 a.
Die Mitarbeiter werden sensibilisiert, anhand der Gestaltung des Absenders, des Betreffs, von in den E-Mails enthaltenen Links, kritische Dateiformate und von E-Mail-Anhängen verdächtige Mails erkennen zu können. Ferner gilt der Grundsatz, dass E-Mails von unbekannten Absendern und mit unbekanntem Bezug nicht geöffnet werden sollen.
Die Mitarbeiter erhalten über die Beauftragten für IT-Sicherheit zeitnah aktuelle Warnungen des Bayern-CERT.

c) Welches Vorgehen wird dabei vermittelt?

Dem großen Unterschied in den Angriffsmustern (Stichwort „Social Engineering“) kann nur begrenzt durch standardisierte Verhaltensweisen begegnet werden. Daher haben die meisten Dienststellen anlassbezogene Prozesse definiert, die eine flexible, dem jeweils aktuellen Bedrohungsszenario entsprechende Information und Reaktion ermöglichen.

Vorbemerkung zum Fragenkomplex 5 bis 8

Die Fragen 5 bis 8 wurden durch das für das Cyber-Allianz-Zentrum (CAZ) zuständige StMI beantwortet.
Das CAZ beim Bayerischen Landesamt für Verfassungsschutz ist zuständig für die Aufklärung, Abwehr und Prävention von elektronischen Angriffen mit nachrichtendienstlichem Hintergrund und solchen, die sich gegen die Sicherheit des Bundes oder eines Landes richten. Beim Themenbereich „Krypto-Trojaner“ handelt es sich um Cyberkriminalität, deren Bekämpfung Polizei und Justiz obliegt. „Krypto-Trojaner“ werden von kriminellen Tätern eingesetzt, um von ihren Opfern „Lösegeld“ für die Freigabe ihrer Daten zu erpressen. Im Bereich elektronischer Angriffe mit nachrichtendienstlichem Hintergrund, für die das CAZ zuständig ist, spielen „Krypto-Trojaner“ keine Rolle. Ziel der elektronischen Spionage ist die verdeckte Ausforschung und Ausleitung von Know-how wissenschaftlicher Einrichtungen oder Wirtschaftsunternehmen, nicht die bloße Geldbeschaffung mittels Erpressung.

5. a Wie oft wird das beim Bayerischen Landesamt für Verfassungsschutz angesiedelte Cyber-Allianz-Zentrum (CAZ) seit Bestehen im Juli 2013 pro Jahr angefragt (aufschlüsseln nach Jahr, Typ des Anfragers, Grund der Anfrage)?

Das Cyber-Allianz-Zentrum Bayern (CAZ) hatte seit seinem Bestehen (Gründung 01.07.2013) insgesamt 327 Kontakte mit bayerischen Wirtschaftsunternehmen, Hochschulen bzw. Forschungseinrichtungen und Behörden (Stand: 19.02.2016). Diese können nach Jahr, Typ des Anfragenden und Anfragegrund wie folgt aufgeschlüsselt werden:
2013/14:
160 Kontakte, davon 64 Fallbearbeitungen und 96 Maßnahmen im Rahmen des Sensibilisierungsprogrammes (Beratungen, Vorträge etc.).
Bei den Fallbearbeitungen stellte man in 49 Fällen (35 Unternehmen, 11 Behörden, 3 Hochschulen) nachrichtendienstliche Aktivitäten fest. Bei 15 Fällen (13 Unternehmen, 2 Behörden) lag ein cyberkrimineller Hintergrund vor.
2015:
126 Kontakte, davon 51 Fallbearbeitungen und 75 Maßnahmen im Rahmen des Sensibilisierungsprogrammes.
Bei den Fallbearbeitungen stellte man in 41 Fällen (18 Unternehmen, 20 Behörden, 3 Hochschulen) nachrichtendienstliche Aktivitäten fest. Bei 10 Fällen (8 Unternehmen, 2 Behörden) lag ein cyberkrimineller Hintergrund vor.
2016 (bis 19.02.2016):
41 Kontakte, davon 10 Fallbearbeitungen und 31 Maßnahmen im Rahmen des Sensibilisierungsprogrammes.
Bei den Fallbearbeitungen stellte man in 6 Fällen (6 Unternehmen) nachrichtendienstliche Aktivitäten fest. Bei 4 Fällen (4 Unternehmen) lag ein cyberkrimineller Hintergrund vor.

b) In wie vielen Fällen wurde das CAZ von den in seiner Zielgruppenbeschreibung genannten Gruppen seit Bestehen im Juli 2013 wegen einer Gefährdung durch Krypto-Trojaner angefragt?

Das CAZ ist für den Phänomenbereich „Krypto-Trojaner“ nicht zuständig (vgl. Vorbemerkung). Diesbezügliche Anfragen werden mit Zustimmung der Betroffenen an die zuständigen Polizeidienststellen weitergeleitet. Im Jahr 2016 gingen fünf Anfragen zum Thema „Krypto-Trojaner“ beim CAZ ein (Stand 31.03.2016).

c) In welcher Form hat das CAZ in dieser Zeit Unternehmen, Hochschulen und Betreiber kritischer Infrastruktur (KRITIS) von sich aus über die jeweils aktuellen Krypto-Trojaner informiert (bitte um Angabe der Anzahl)?

Auf die Vorbemerkung wird verwiesen. Warnmeldungen zu aktuellen „Krypto-Trojanern“ hat das CAZ nicht herausgegeben. Im Rahmen seiner Präventionsarbeit informiert das CAZ generell über mögliche Gefährdungen durch Schadprogramme (darunter auch „Krypto-Trojaner“). Dabei wird beraten, welche Schutz- und Gegenmaßnahmen allgemein ergriffen werden können.

6. a) Werden durch das CAZ auch andere Einrichtungen, als die in der Zielgruppenbeschreibung genannten, wie z. B. bayerische Behörden, Gebietskörperschaften oder öffentliche Unternehmen, vom CAZ beraten und informiert?

Das CAZ ist bei Bedrohungen durch Spionage und Sabotage nicht nur für Wirtschaft, Wissenschaft und Betreiber Kritischer Infrastrukturen (KRITIS) Ansprechpartner, sondern auch für den Staat. So werden Warnmeldungen dem Bayern-CERT zur Verfügung gestellt, das für die Absicherung der bayerischen Behörden und Behördennetze zuständig ist. Sofern öffentliche Unternehmen Kritische Infrastrukturen betreiben, erhalten diese im Einzelfall ebenfalls Warnmeldungen.

b) Falls nein, warum nicht?

Entfällt.

c) Falls ja, in wie vielen Fällen hat das CAZ von sich aus Initiative ergriffen, diese Gruppen zu informieren?

Seit seinem Bestehen hat das CAZ rund 100 Warnmeldungen herausgegeben. Die Warnmeldungen richten sich an betroffene und gefährdete Unternehmen und Einrichtungen. Im CAZ werden keine statistischen Auswertungen geführt, wie viele Warnmeldungen an einzelne Adressaten gerichtet wurden. Eine nachträgliche Erhebung wäre mit unverhältnismäßigem Aufwand verbunden, weil hierfür in jedem einzelnen Fall die gesamte Korrespondenz mit allen Adressaten überprüft werden müsste.

7. a) Welche konkreten Hilfsangebote bietet das CAZ im Falle einer Infizierung mit Krypto-Trojanern?

Auf die Vorbemerkung und die Antwort zu Frage 5b wird verwiesen. Wendet sich ein betroffenes Unternehmen gleichwohl an das CAZ, wird auf Wunsch der Kontakt mit den zuständigen Polizeidienststellen hergestellt. Im Übrigen können allgemeine Beratungsangebote zum Bereich Wirtschaftsschutz in Anspruch genommen werden. Grundlage dafür sind z.B. die Leitfäden des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Thema IT-Sicherheit und Vorfallsbearbeitung und das Themenpapier „Ransomeware: Bedrohungslage, Prävention & Reaktion“.

b) Da laut der Eigenbeschreibung des CAZ auf der Homepage des Bayerischen Landesamts für Verfassungsschutz auch vorgesehen ist, elektronische Angriffe aus nachrichtendienstlicher Sicht zu bewerten, frage ich die Staatsregierung, welche Erkenntnisse dem CAZ aus dieser Perspektive über Krypto-Trojaner vorliegen?

Es ist nicht bekannt, dass Nachrichtendienste „Krypto-Trojaner“ zur Spionage oder Sabotage nutzen. Im Übrigen wird auf die Vorbemerkung verwiesen.

c) Auf welche anderen Angebote können Einrichtungen sowie Bürgerinnen und Bürger, die nicht zur definierten Zielgruppe des CAZ gehören, in Bayern zurückgreifen?

Die Zentrale Ansprechstelle Cybercrime (ZAC) beim Bayerischen Landeskriminalamt ist der zentrale polizeiliche Ansprechpartner für Unternehmen, Verbände, Behörden und weitere Institutionen. Sie ist „Ersthelfer“ und Berater für von Cyberkriminalität betroffene Institutionen. Als kompetenter Partner im Kampf gegen Cyberkriminalität berät sie diese auch im Vorfeld, z.B. auch im Rahmen von Vorträgen.
Auf Bundesebene betreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Bürger-CERT-Portal als Informationsplattform für Bürger (www.buerger-cert.de/). Das Portal informiert und warnt Bürger und kleine Unternehmen vor Viren, Würmern und Sicherheitslücken in Computeranwendungen.

8. a) Welche Kriterien müssen erfüllt sein, damit das CAZ auf seiner Webseite vor einer Schadsoftware warnt?

Das CAZ veröffentlicht auf seiner Webseite grundsätzlich keine detaillierten Warnmeldungen. Eine öffentlich bekanntgegebene Warnmeldung mit Indikatoren könnte nämlich dazu führen, dass deren Schutzwirkung aufgehoben wird, weil der Angreifer Kenntnis vom aktuellen Stand der Analyse des CAZ erhält. Die Warnmeldungen des CAZ werden deshalb unmittelbar an die jeweils betroffenen und gefährdeten Unternehmen und Einrichtungen adressiert. Die Entscheidung, zu welchen Gefahren Warnhinweise erstellt werden, erfolgt im jeweiligen Einzelfall auf Basis der forensischen Untersuchung der eingesetzten Schadprogramme.

b) Wie erklärt die Staatsregierung, dass das CAZ – ausweislich seiner Homepage im Internetangebot des Bayerischen Landesamts für Verfassungsschutz – im Jahr 2015 lediglich 3 Warnmeldungen veröffentlicht hat?

Auf die Antwort zu Frage 8a wird verwiesen. Bei den im Internetangebot des Bayerischen Landesamts für Verfassungsschutz veröffentlichten Meldungen aus dem Jahr 2015 handelt es sich nicht um detaillierte Warnmeldungen, sondern um Hinweise auf Warnmeldungen, die das CAZ an potenziell betroffene Unternehmen und Institutionen herausgegeben hat. Der damit verfolgte Hauptzweck war nicht die öffentliche Warnung; vielmehr sollten hierdurch bayerische Unternehmen auf das Angebot des CAZ aufmerksam gemacht werden. Hierdurch kann die Bereitschaft von Unternehmen verstärkt werden, das CAZ zu kontaktieren und elektronische Angriffe vertraulich mitzuteilen.

c) Wie beurteilt die Staatsregieruung die Gefährdung der Zielgruppen des CAZ durch die derzeit aktuellen Krypto-Trojaner-Varianten wie Locky und Teslacrypt?

Seit Ende 2015 ist eine starke Verbreitung von „Krypto-Trojanern“ zu beobachten. Da gezielte Angriffe bislang eher die Ausnahme darstellen, ist jeder Nutzer, der auf das Internet zugreift, potentiell gefährdet. Betroffen sind demnach insbesondere Privatleute, Behörden, wissenschaftliche Einrichtungen, Krankenhäuser und Unternehmen. Die konkrete Gefährdung der einzelnen IT-Nutzer ist individuell abhängig vom jeweiligen Sicherheitsstandard ihrer IT-Systeme und der Sensibilität im Umgang mit Cyberbedrohungen.