Thüringer Landtag
7. Wahlperiode

Drucksache 7/9086
23.11.2023

K l e i n e A n f r a g e

des Abgeordneten Bilay (DIE LINKE)

und

A n t w o r t

des Thüringer Ministeriums für Inneres und Kommunales

Vorfälle mit Ransomware (Verschlüsselungstrojaner, Erpressungstrojaner) in Thüringen

Durch sogenannte Ransomware infizieren Kriminelle die Endgeräte von Betroffenen und führen eine Verschlüsselung der Geräte beziehungsweise gespeicherten Daten durch. Anschließend sehen sich Betroffene mit Lösegeldforderungen konfrontiert, bei denen ihnen nach erfolgter Zahlung eine Entschlüsselung versprochen wird. In der Vergangenheit waren damit auch Verwaltungen und Unternehmen konfrontiert.

Das **Thüringer Ministerium für Inneres und Kommunales** hat die **Kleine Anfrage 7/5109** vom 26. Juli 2023 namens der Landesregierung mit Schreiben vom 16. November 2023 beantwortet:

1. Welche Kenntnisse liegen der Landesregierung beziehungsweise den ihr nachgeordneten Behörden über die Anzahl bekannt gewordener Ransomware-Angriffe gegen Computer, Endgeräte oder Netzwerksysteme in Thüringen in den Jahren 2021 und 2022 jeweils vor?

   Antwort:
   In der Polizeilichen Kriminalstatistik (PKS) der Thüringer Polizei sind für 2021 sieben und für 2022 17 Fälle zu Straftaten mit Ransomware-Angriffen erfasst. In der PKS werden jedoch nur die bei der Polizei bearbeiteten Straftaten einschließlich der mit Strafe bedrohten Versuche und weitere Angaben zu den registrierten Fällen abgebildet (sogenannte Hellfeld). Die PKS ist stark von dem Anzeigeverhalten der Geschädigten abhängig. Straftaten, die nicht angezeigt beziehungsweise öffentlich registriert werden, verbleiben im sogenannte Dunkelfeld.

   Der Phänomenbereich Cybercrime, welchem die Ransomware-Angriffe zugerechnet werden, weist insgesamt ein weit überdurchschnittlich großes Dunkelfeld auf. Die angegebenen Zahlen geben deshalb nicht die tatsächliche Betroffenheit im Freistaat Thüringen wieder.

2. Welche Angaben kann die Landesregierung anonymisiert über die betroffenen Branchen und deren Häufigkeit vornehmen (zum Beispiel "Kommunalverwaltung", "Wissenschaftseinrichtung", "Medizinunternehmen", "Privatperson")?

   Antwort:
   In der PKS werden keine Informationen zu den Geschädigten von Straftaten erfasst. Eine Aussage zur Betroffenheit von konkreten Branchen kann daher nicht getroffen werden. Ebenso wenig können Angaben zur tatsächlichen Häufigkeit gemacht werden. Auf die Antwort zur Frage 1 wird Bezug genommen.

Druck: Thüringer Landtag, 1. Dezember 2023

Darüber hinaus liegen der Landesregierung keine eigenen Erkenntnisse vor.

3. Welche Kenntnisse hat die Landesregierung über die Spannbreite in der Höhe der geforderten Lösegeldsummen?

   Antwort:
   Die geforderten Lösegelder werden nicht in der PKS der Thüringer Polizei abgebildet. Die regelmäßig im § 253 StGB (Erpressung) erfassten Schadenshöhen geben keinen verlässlichen Anhaltspunkt zur Beantwortung der Fragestellung. Auf die Antwort zu Frage 4 wird Bezug genommen.
   In der Regel wird in der abgelegten Erpresserbotschaft auf dem angegriffenen System entgegen den Anfangszeiten dieses Phänomens mittlerweile keine konkrete Lösegeldsumme mehr genannt. Erst nach der Kontaktaufnahme des Geschädigten zum Täter wird eine Summe für die Übermittlung eines Codes zur Entschlüsselung der Daten festgelegt. Oftmals wird dabei noch zusätzlicher Druck durch eine Erhöhung der geforderten Lösegeldsumme nach Ablauf einer festgesetzten Zeitspanne aufgebaut. Die Höhe des Lösegelds richtet sich dabei häufig nach der Größe der vorher ausgekundschafteten IT-Landschaft.

4. Welche Schäden entstanden nach Kenntnissen der Landesregierung durch Ransomware in den Jahren 2021 und 2022 in Thüringen?

   Antwort:
   In der PKS der Thüringer Polizei wird nur bei vollendeten Straftaten eine Schadensangabe erfasst, sofern der Geschädigte Angaben dazu macht. Ist kein Schaden bestimmbar, gilt ein symbolischer Schaden von einem Euro. Für das Jahr 2021 weist die PKS einen Vermögensschaden von einem Euro und für das Jahr 2022 von 1.061 Euro aus.

   Für eine Schätzung der wirtschaftlichen Schäden in Thüringen durch Ransomware liegen der Landesregierung deshalb keine statistischen Daten vor. Auf die Antwort zur Frage 1 wird Bezug genommen.

   Schäden für eine Organisation durch Ransomware können grundsätzlich in Eigenschäden, Fremdschäden und Reputationsschäden unterteilt werden. Je nach Auffassung werden auch Kosten von allgemeinen Präventionsmaßnahmen oder Folgekosten nach einem Angriff, zum Beispiel die Verbesserung der Organisations- oder IT-Struktur, mit dazu gezählt. Auf die Antwort der Landesregierung vom 19. Juli 2021 zur Frage 9 der Kleinen Anfrage 7/2126 des Abgeordneten Kemmerich (FDP) "Cybersicherheit im Handwerk in Thüringen" (Drucksache 7/3814) wird Bezug genommen.

5. Welche Kenntnisse hat die Landesregierung zahlenmäßig über solche Fälle, in denen Betroffene in den Jahren 2021 und 2022 auf die Forderungen der Erpresser eingingen?

   Antwort:
   Hierzu liegen der Landesregierung keine statistischen Daten vor. Eine Erfassung der Anzahl, in denen der Betroffene auf die Forderung der Erpresser eingeht, erfolgt in der PKS der Thüringer Polizei nicht.

6. Wer ist aus Sicht der Landesregierung potenziell durch Ransomware-Attacken gefährdet?

   Antwort:
   Grundsätzlich kann weder im unternehmerischen, behördlichen oder privaten Bereich eine Gefährdung durch Ransomware ausgeschlossen werden. Deshalb ist jede wirtschaftliche Einheit (Unternehmen, Selbstständige, Freiberufler et cetera) oder öffentliche Einrichtung (Behörden, Universitäten, Forschungseinrichtungen et cetera), die über Rechner mit Verbindung zum Internet verfügen oder auf deren Rechnern externe Datenträger ausgelesen werden, potenziell gefährdet.

   Besonders gefährdet sind Unternehmen und Organisationen, die über hohe finanzielle Ressourcen verfügen oder die in kritischen Sektoren tätig sind, wie zum Beispiel Gesundheitswesen, Energie oder Finanzdienstleistungen, aber auch die öffentliche Verwaltung.

7. Zu welchen präventiven Vorsichtsmaßnahmen rät die Landesregierung potenziell Gefährdeten von Ransomware-Attacken, insbesondere Unternehmen und Verwaltungen, insbesondere hinsichtlich regelmäßiger Datensicherungen und des Zugriffsschutzes?

Antwort:
Die Landesregierung orientiert sich bei präventiven Vorsichtsmaßnahmen gegen Ransomware-Angriffe an den Empfehlungen des BSI (beispielsweise Maßnahmenkatalog Ransomware). Dieser enthält unter anderem als präventive Maßnahmen regelmäßige Backups und die Vorbereitung auf eintretende Szenarien.

Innerhalb der Landesverwaltung gibt es verschiedene Vorgaben zur Informationssicherheit und nicht nur zum Schutz gegen Ransomware. Grundlage hierfür bildet die Informationssicherheitsleitlinie der Thüringer Landesverwaltung (ThISL). Zentral ist dabei ein ganzheitlicher Ansatz zur Informationssicherheit, neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium konkrete Anforderungen. Das umfasst auch Datensicherungen und den Zugriffsschutz. Die Auswahl und Ausgestaltung geeigneter Maßnahmen sowie Aufrechterhaltung und stetige Verbesserung der Informationssicherheit durch kontinuierliche Überprüfung und Anpassung der Vorkehrungen ist dabei wesentlich. Welche Maßnahmen im konkreten Einzelfall erforderlich sind, bestimmt sich nach den Maßstäben des "Standes der Technik". Die konkreten Empfehlungen des IT-Grundschutz-Kompendiums (als integrales Bestandteil der Methodik des BSI-Standards 200-2) bilden dabei den aktuellen Stand der Technik ab.

Innerhalb der Landesverwaltung werden folgende präventive Vorsichtsmaßnahmen getroffen:
- ein in der Thüringer Landesverwaltung etabliertes Informationssicherheitsmanagementsystem nach BSI-Standard 200-2,
- die Sensibilisierung der Mitarbeiter,
- eine Zertifizierung der IT-Infrastruktur nach BSI-Grundschutz,
- technische Maßnahmen (IPS/IDS, Firewalls, mehrstufige Antivirensoftware) und
- organisatorische Maßnahmen zur Erkennung von Schadsoftware (beispielsweise sicherer Umgang mit E-Mails).

Den Kommunalverwaltungen wird insbesondere die Umsetzung des Maßnahmenkataloges Ransomware des BSI für Behörden und Einrichtungen empfohlen.

Für eine weitergehende Beratung steht die speziell für Unternehmen sowie für öffentliche und nichtöffentliche Institutionen im Landeskriminalamt eingerichtete Zentrale Ansprechstelle Cybercrime (ZAC) als kompetente Ansprechpartner zur Verfügung.

Für Bürgerinnen und Bürger stehen ebenso öffentlich zugängliche Informationen zu Schadsoftware über die Webseite des BSI zur Verfügung.

8. Zu welchen Maßnahmen rät die Landesregierung Betroffenen von Ransomware-Angriffen, falls eine Verschlüsselung von Daten bereits stattgefunden hat?

Antwort:
Die erforderlichen Maßnahmen zur Bewältigung eines solchen Vorfalls bestimmen sich nach dem jeweiligen Einzelfall im Rahmen eines koordinierten Notfallmanagements beziehungsweise Business Continuity Managements. Auch hierzu gibt es mit dem BSI-Standard 200-4 beziehungsweise weiterführenden Arbeitshilfen des BSI geeignete Hilfestellungen.

Die Reaktion auf einen Ransomware-Angriff kann von Fall zu Fall variieren. In Fällen der Verschlüsselung ist es ratsam, Experten hinzuzuziehen, um eine angemessene und wirksame Reaktion zu gewährleisten. Nach einem Ransomware-Angriff ist schnelles und systematisches Handeln wichtig, um die Auswirkungen zu minimieren und die Wiederherstellung der Daten und Systeme zu ermöglichen. Unternehmen sowie öffentliche und nichtöffentliche Institutionen sollten sich an ihre Kammern und Verbände, an die im Landeskriminalamt eingerichtete Zentrale Ansprechstelle Cybercrime (ZAC) oder auch an das Amt für Verfassungsschutz wenden.

9. Welche Kenntnisse liegen der Landesregierung über etwaige Urheber von Ransomware-Attacken in Thüringen vor?

Antwort:
Zu den konkreten Urhebern von Cyberangriffen mit Ransomware im Freistaat Thüringen liegen der Landesregierung keine Kenntnisse vor. Im Jahr 2021 konnte lediglich ein Tatverdächtiger ermittelt werden. Gründe für die geringe Anzahl von aufgeklärten Straftaten sind unter anderem VPN-Anbieter, Proxy-Server, sogenannte Bullet-Proof-Hoster und Kryptowährungen, die es den Tätern ermöglichen, anonyme Angriffe im Internet durchzuführen und ihre Identität zu verbergen. VPN-Anbieter und Proxy-Server sind besonders problematisch für die Strafverfolgung, da sie oft außerhalb des Landes der sachbearbeitenden Ermittlungsbehörde betrieben werden und die Justizbehörden keinen Zugriff auf die Daten haben.

10. Inwiefern kann die Landesregierung Angaben zu den Motiven von Ransomware-Angreifern in Thüringen vornehmen? Stehen dabei ausschließlich der finanzielle Gewinn durch Private im Vordergrund oder auch Sabotagehandlungen beziehungsweise finanzieller Gewinn für andere Staaten (um gegebenenfalls durch somit beschaffte Devisen Sanktionen zu umgehen)?

Antwort:
In Bezug auf Thüringen kann eine konkrete Motivation von Ransomware-Angreifern nicht belegbar nachgewiesen werden. Jedoch wurde bei allen angezeigten Fällen eine Erpressernachricht auf dem angegriffenen System hinterlassen. Vordergründig ist deshalb der finanzielle Gewinn der Täter als Motivation zu bewerten. Es ist jedoch nicht feststellbar, inwieweit diese Täter aus eigenem Interesse oder im Auftrag anderer Staaten handelten.

Maier
Minister