STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Der Staatsminister

Aktenzeichen
(bitte bei Antwort angeben)
34-0141.50/9879

Dresden, 27. Mai 2016

SÄCHSISCHES STAATSMINISTERIUM DES INNERN
01095 Dresden

Präsidenten des Sächsischen Landtages
Herrn Dr. Matthias Rößler
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Kleine Anfrage des Abgeordneten Valentin Lippmann,
Fraktion BÜNDNIS 90/DIE GRÜNEN
Drs.-Nr.: 6/5043
Thema: Hackerangriffe bei Sachsens Polizei und Verfassungsschutz

Sehr geehrter Herr Präsident,

den Fragen sind folgende Ausführungen vorangestellt:

„Vorbemerkung: Die MZ berichtete am 29.04.2016, dass Sachsen-Anhalts Verfassungsschutz Opfer eines Hackerangriffs geworden sei. So seien Computer mit sog. Erpressungs-Trojanern verschlüsselt worden. Bei der Säuberung habe man sog. Backdoor-Trojaner auf einem Server entdeckt. Dieses Schadprogramm kopiere unbemerkt Daten und versende diese über das Internet. Die IT-Spezialisten des Verfassungsschutz Sachsen-Anhalts haben weder den Verschlüsselungstrojaner entfernen, noch den Backdoor -Trojaner erkennen können. Es sei eine Spezialfirma beauftragt worden."

Namens und im Auftrag der Sächsischen Staatsregierung beantworte ich die Kleine Anfrage wie folgt:

Frage 1:
Wie viele und welche solcher Schadsoftware wurden in den vergangenen zwei Jahren auf wie vielen Rechner und Servern welcher Dienststellen der sächsischen Polizei bzw. des sächsischen Verfassungsschutzes festgestellt?

Weder im Datennetz der Polizei des Freistaates Sachsen noch im Datennetz des LfV Sachsen wurden derartige Schadprogramme bisher festgestellt.

Hausanschrift:
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Str. 2
01097 Dresden

Telefon +49 351 564-0
Telefax +49 351 564-3199
www.smi.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den Straßenbahnlinien 3, 6, 7, 8, 13

Besucherparkplätze:
Bitte beim Empfang Wilhelm-Buck-Str. 2 oder 4 melden.

Frage 2:
Inwieweit wurden aufgrund solcher Angriffe welche Daten kopiert und an wen bzw. welche Stelle abgeflossen sind?

Entfällt.

Frage 3:
Welche Maßnahmen wurden oder werden getroffen, um solche Angriffe zu verhindern?

Die Polizei des Freistaates Sachsen betreibt einen hohen Aufwand um die zu verarbeitenden Daten zu schützen. Auf jedem Server und auf jedem Client sind Schutzprogramme zur Erkennung und Abwehr von Schadprogrammen installiert. Zusätzlich wird der gesamte Datenverkehr in und aus dem Datennetz der Polizei des Freistaates Sachsen durch ein Sicherheitsgateway geschützt, in dem der ein- und ausgehende Datenverkehr geprüft und gefiltert wird (potentiell gefährliche Daten werden grundsätzlich geblockt).

Die Clients im Datennetz der Polizei des Freistaates Sachsen sind restriktiv aufgesetzt, so dass der Nutzer nur minimale Rechte auf dem System erhält und grundsätzlich keine selbständigen Installationen durchführen kann. Die Clients im Datennetz der Polizei des Freistaates Sachsen sind des Weiteren mit einer Software zur Schnittstellenkontrolle versehen.

Das LfV Sachsen arbeitet mit getrennten IT-Netzen. Die Verarbeitung von Verschlusssachen findet in einem stark geschützten Netz ohne Internetanbindung statt. Ein offenes Netz mit Internetanbindung wird für die Kommunikation innerhalb des Sächsischen Verwaltungsnetzes (SVN) und den Zugang zum Internet verwendet. Die beiden Netze sind strikt voneinander getrennt. Zum Schutz werden verschiedene Virenschutzprogramme, Firewalls und Datendioden eingesetzt.

Weitere Maßnahmen gegen Hacker-Angriffe durch Verschlüsselungs- oder Backdoor-Trojaner, die durch das Sächsische Staatsministerium des Innern (SMI) für das gesamte SVN initiiert bzw. koordiniert werden, liegen auf technischer Ebene bzw. auf Ebene der Mitarbeitersensibilisierung.

Aktuelle technische Projekte für mehr Informationssicherheit werden im Jahresbericht des Beauftragten für Informationssicherheit des Landes 2014/2015 unter 3.3. beschrieben. Zur Vermeidung von Angriffen durch Trojanersoftware dienen dabei insbesondere die Projekte HoneySens (3.3.1.) und der Ausbau der APT-Erkennung (3.3.3.) im SVN. Das SVN verfügt sowohl intern als auch an seinem Übergang zum Internet über erprobte und sich ständig aktualisierende technische Schutzmechanismen wie u. a. Virenscanner und „Blacklists“ von gesperrten, weil Schadcode aussendenden Internetseiten oder E-Mail-Adressen, um oben genannte unerlaubte Zugriffe auf Daten im SVN zu verhindern. Detaillierte Zahlen sind dem Jahresbericht des Beauftragten für Informationssicherheit des Landes unter 2.5. zum SVN zu entnehmen, die belegen, dass im Berichtszeitraum keine Einbrüche mit einem damit verbundenen gezielten Datenabfluss und/oder Manipulationen festgestellt worden sind.

Darüber hinaus werden durch das SMI, alljährlich Sensibilisierungsveranstaltungen zur Computer- und Internetsicherheit für die Bediensteten der Landesverwaltung angeboten, um die Gefahren u. a. durch Trojanersoftware aufzuzeigen und den Computernutzern wirksame Gegenmaßnahmen zu erläutern. An diesen Sensibilisierungsmaßnahmen, zu denen auch die Bediensteten der Polizei und des LfV Sachsen eingeladen sind, nahmen allein im Jahr 2015 rund 1.800 Personen teil. Diese Maßnahme wird auch im Jahr 2016 fortgeführt. Des Weiteren organisiert die Landtagsverwaltung unter Mithilfe des SMI, gesonderte Sensibilisierungsveranstaltungen für die Verwaltung und die Abgeordneten und ihre Mitarbeiter, die ebenfalls in diesem Jahr stattfinden werden.

Frage 4:
Inwieweit verfügt die sächsische Polizei bzw. der sächsische Verfassungsschutz über IT-Spezialisten zum Entfernen und Erkennen solcher Schadsoftware bzw. welche Spezialisten wurden wann und wo eingesetzt?

Diese Aufgabe übernehmen im Polizeibereich die in den Dienststellen und Einrichtungen beschäftigten System- und Anwenderbetreuer in Zusammenarbeit mit den jeweiligen Beauftragten für Informationssicherheit. Über interne Prozesse ist die Behandlung von Sicherheitsvorfällen im Zusammenhang mit dem Auftreten von Schadprogrammen geregelt. Dem Nutzer steht mit der IuK-Leitstelle in der Polizei des Freistaates Sachsen eine rund um die Uhr besetzte Stelle zur Verfügung, über die auch außerhalb der Regeldienstzeit entsprechende Maßnahmen eingeleitet werden können.

Im LfV Sachsen werden Mitarbeiter eingesetzt, welche die nötige Qualifikation besitzen, um Schadsoftware erkennen und entfernen können. Es findet zudem eine Zusammenarbeit mit dem Computer Emergency Response Team (CERT) des Staatsbetriebes Sächsische Informatikdienste (SID) und externen IT-Spezialisten statt, die im Bedarfsfall hinzugezogen werden können.

Frage 5:
Inwieweit wurden oder werden üblicherweise welche parlamentarischen Gremien von einem solchen Angriff in Kenntnis gesetzt?

Durch das LfV Sachsen würden die Parlamentarische Kontrollkommission oder die G 10-Kommission in einem solchen Fall im Rahmen ihrer jeweiligen Zuständigkeiten unterrichtet.

Eine Verpflichtung seitens der Polizei zur Information über derartige Vorfälle an parlamentarische Gremien ist weder üblich noch bekannt.

Im Rahmen der Arbeitsgruppe Informationssicherheit als das koordinierende Gremium für alle ressortübergreifenden Aspekte der Informationssicherheit in der Sächsischen Landesverwaltung berichtet das SAX.CERT monatlich über die Sicherheitslage des SVN. Mitglied in diesem Gremium ist dabei auch ein Vertreter der Landtagsverwaltung.

Darüber hinaus sieht das ressortübergreifende Meldeverfahren vor, dass ab einer bestimmten Eskalationsstufe der CIO des Freistaates über Sicherheitsgefährdungen informiert wird, was in der Folge eine Befassung auch parlamentarischer Gremien nach sich ziehen kann.

Mit freundlichen Grüßen

Markus Ulbig