Ministerium für Inneres und Kommunales
des Landes Nordrhein-Westfalen

Ministerium für Inneres und Kommunales NRW, 40190 Düsseldorf

Präsidentin des Landtags
Nordrhein-Westfalen
Platz des Landtags 1
40221 Düsseldorf

für die Mitglieder
des Innenausschusses

60-fach

18. Januar 2016
Seite 1 von 1

Aktenzeichen
(bei Antwort bitte angeben)

MR Jülke
Telefon 0211 871-
Telefax 0211 871-

Sitzung des Innenausschusses am 21.01.2016
Antrag der Fraktion der Piraten
TOP 6 „IT- Angriff auf die Landesverwaltung"

Sehr geehrte Frau Landtagspräsidentin,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich 60 Exemplare des schriftlichen Berichtes zum TOP 6 „IT-Angriff auf die Landesverwaltung".

Mit freundlichen Grüßen

Ralf Jäger MdL

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@mik.nrw.de
www.mik.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 703, 706, 712, 713, 725, 835, 836, NE 7, NE 8
Haltestelle: Kirchplatz

Schriftlicher Bericht des Ministers für Inneres und Kommunales zu TOP 5 „IT-Angriff auf die Landesverwaltung" der Innenausschusssitzung am 21.01.2016

Der Antrag der Piraten-Fraktion bezieht sich auf den mündlichen Bericht des Innenministers über den IT-Schadensfall in der Landesverwaltung am 09.12.2015 und die darauf folgende Presseberichterstattung über IT-Ausfälle in der Landesverwaltung und bittet darum, dem Innenausschuss über diesen Vorfall zu berichten.
Dabei soll auch auf die entstandenen Schäden wie den Arbeitsausfall, Datenverluste oder gezahlte Lösegelder eingegangen werden. Es sollen auch Erkenntnisse darüber mitgeteilt werden, welchen Zugang die Angreifer zu Verschlusssachen, vertraulichen Informationen und Datenbanken der Ministerien hatten.

Anlass für die mündliche Information im Innenausschuss am 10.12. 2015 war ein Sicherheitsvorfall im MIK, der zu einer kontrollierten Netzabschaltung führte und am Nachmittag des 09.12.2015 auch über die Presse kommuniziert wurde.

Im Folgenden wird deshalb
1. der Sicherheitsvorfall im MIK,
2. die Situation im Geschäftsbereich des MIK und
3. die Situation in anderen Ministerien, soweit hierzu zwischenzeitlich dem CIO berichtet wurde, beschrieben.

1. Sicherheitsvorfall im MIK

- Im MIK ist am Morgen des 09.12.2015, gegen 06:45 Uhr eine ungewöhnliche Aktivität im Datennetz des MIK festgestellt worden. Erkennbar war, dass Dateien aus dem Bestand des MIK verschlüsselt wurden. Außerdem wurden Textdateien gefunden, in denen mitgeteilt wurde, dass eine Verschlüsselung von Dateien stattfinde. Gegen die Zahlung eines Betrags in Bitcoines (Internetwährung) würde der Schlüssel zur Verfügung gestellt, der für die Entschlüsselung der Dateien erforderlich sei.

- Als Sofortmaßnahme hat das MIK daraufhin die Verbindung zum Landesverwaltungsnetz und damit zum Internet getrennt. Außerdem wurden umgehend die Server und Dateienspeicher heruntergefahren, um weitere Verschlüsselungen unmöglich zu machen.

- Das MIK arbeitet mit einem leistungsfähigen Virenscanner. Bei der Schadsoftware handelte es sich aber um eine neue Variante, für die der Hersteller der im MIK eingesetzten Antivirensoftware bis zum Sicherheitsvorfall noch keine Virensignatur bereitgestellt hatte.

- Die separaten Netze der Polizei und des Verfassungsschutzes im MIK waren nicht betroffen. Es gab auch keine Beeinträchtigung der Telefonie, weil das MIK seit seinem Umzug ins neue Dienstgebäude über eine vom Datennetz getrennte VoiP-Telefonie-Infrastruktur verfügt. Die Beschäftigten des MIK waren zu jeder Zeit intern und extern telefonisch erreichbar.

- Das MIK hat sofort eine Gruppe von Spezialisten zusammengestellt, dem u.a. Vertreter des Kompetenzzentrums Cyberkriminalität des LKA und des CERT NRW angehörten. Außerdem sind externe Spezialisten für die im MIK eingesetzte Antivirensoftware und für die Datenspeicherungs- und Sicherungssysteme hinzugezogen worden.

- Alle Ressorts wurden noch am Vormittag des 09.12.2015 mittels der etablierten Strukturen des CERT NRW über den Sicherheitsvorfall unterrichtet, um Maßnahmen der Eigensicherung vornehmen zu können.

- Die Schadsoftware im MIK wurde am frühen Mittwochnachmittag durch das LKA gefunden und identifiziert. Bei der Schadsoftware handelt es sich um einen Verschlüsselungstrojaner der so genannten TeslaCrypt-Version. Dies ist eine Schadsoftware mit erpresserischem Hintergrund (Ransomware).
  Die Software gelangt u.a. per E-Mail Anhang meistens des Typs „ZIP" oder der Dateiendung „js" auf die Rechner. Wird diese Datei geöffnet, bzw. installiert, verschlüsselt TeslaCrypt auf dem Computer und auf den angeschlossenen Laufwerken befindliche Dateien. Dazu wird im ersten Schritt eine VBS-Datei auf die Festplatte geschrieben und gestartet. Diese lädt die eigentliche Schadsoftware aus dem Internet nach und startet sie. Anschließend wird eine Meldung angezeigt, in der die Kriminellen eine Geldforderung stellen. Im Gegenzug soll dem Betroffenen der Schlüssel mitgeteilt werden, mit dem es möglich ist, die verschlüsselten Dateien, die mit der Endung „vvv" angelegt wurden, wieder zu entschlüsseln.

- IT.NRW hat in Reaktion auf den Sicherheitsvorfall im MIK auf seinen für die eMail-Kommunikation zuständigen Servern die Einstellungen vorübergehend so verschärft, dass ZIP-Dateien nicht weitergeleitet wurden.

- Inzwischen ist klar, dass die Schadsoftware fast zeitgleich über zwei Arbeitsplatzcomputer in das Netz des MIK gelangte. Sie hat sich von den Anwendern unbeabsichtigt und unbemerkt installiert.

- Es gibt keine Anzeichen dafür, dass das MIK gezielt Adressat des Trojaners war. Vielmehr spricht alles dafür, dass der Trojaner breit gestreut war und das MIK zufällig betroffen war. Die „Infektionswelle" dieses Typs von Schadsoftware und seinen zahlreichen Folgevarianten ist derzeit noch nicht beendet.

- Aus Sicherheitsgründen ist das Rechenzentrum des MIK erst am Freitag, 11.12.2015, gegen 10:15 Uhr wieder in Betrieb genommen worden. Dieser Zeitraum war erforderlich, um durch eine umfassende Durchsuchung des gesamten Datenbestandes sicher zu stellen, dass die Schadsoftware an keiner Stelle im System mehr vorhanden ist. Aufgrund der zu prüfenden Datenmengen war der Zeitraum nicht weiter zu verkürzen. Weitere „Infektionen" konnten dadurch auch ausgeschlossen werden.

Der Trojaner hat nicht versucht, Daten des MIK zu stehlen. Soweit Dateien durch die Schadsoftware bereits verschlüsselt wurden, konnten diese gegen Sicherungskopien vom Vortag ausgetauscht werden.
Die Arbeitsfähigkeit des MIK war technisch eingeschränkt: Keine eMail-Kommunikation, kein Zugriff auf webbasierte Anwendungen. Allerdings bestand jederzeit eine telefonische Erreichbarkeit. Die Beschäftigten konnten ihre Notebooks und Desktop-Rechner auch ohne Netzanbindung/ Internetzugang quasi offline nutzen, um notwendige Schreiben etc. vorzubereiten. Durch zusätzliche Faxgeräte - Installation wurde eine netzunabhängige Kommunikationsmöglichkeit geschaffen. Im Übrigen haben die Beschäftigten anstehende Besprechungstermine vorgezogen.
Ein Schaden im Sinne von Arbeitsausfall ist nicht konkret zu identifizieren, geschweige denn zu beziffern.
Insbesondere ist durch den Netzausfall kein Sicherheitsrisiko für Dritte entstanden, da wie bereits erwähnt, die speziellen Netze der Polizei und des Verfassungsschutzes nicht betroffen waren.

- Das MIK ist selbstverständlich nicht auf die Erpressungsforderung eingegangen. Im Übrigen ist zweifelhaft, ob eine Zahlung auch zu einer Bereitstellung des Schlüssels führt. Es ist davon auszugehen, dass einer erfolgreichen Erpressung weitere Forderungen folgen.

- Das MIK hat Strafanzeige gegen unbekannt erstattet. Für die Ermittlungen zuständig ist die Staatsanwaltschaft Köln (ZAC).

- Nach Bereinigung der akuten Gefährdungssituation wurde in Kenntnis der fortdauernden Gefährdungslage als zusätzliche Vorsichtsmaßnahme der Internetzugang des MIK nicht freigegeben, sondern bis Mittwoch, 16.12.2015, gesperrt. Das IT-Referat des MIK hatte bereits 2015 eine Browser-Konzeption entwickelt, mit der eine verbesserte Sicherheit bei der Nutzung des Internets erreicht wird. Die Umsetzung der Maßnahme ist infolge des Sicherheitsvorfalls weiter forciert worden und konnte am 16.12.2015 in Betrieb genommen werden. Ziel und Grundkonzept des neuen Systems (2-Browser - Strategie) sind darauf gerichtet, dass Angriffe aus dem Internet nur eine virtuelle Maschine betreffen können und nicht mehr Beschäftigte mit ihrer lokalen Rechtestruktur.

- Die bisherigen Schutzmaßnahmen des MIK haben sich als sehr wirkungsvoll erwiesen. Ein Datenverlust- oder -abfluss konnte auch in diesem Fall verhindert werden. Der Vorfall wird aber noch weiter analysiert und zum Anlass genommen, die Informationssicherheit des MIK noch weiter zu verbessern.
  Einen hundertprozentigen Schutz gibt es nicht, aber die entsprechende Alarm- und Kommunikationsinfrastruktur muss so beschaffen sein, dass sie allen Behörden helfen kann. Der aktuelle Vorfall hat gezeigt, dass schnelles und überlegtes Handeln eine Ausbreitung begrenzt und eine verlustfreie Wiederherstellung von Daten ermöglicht hat.
  Das MIK wird die aus der Analyse des Vorfalls resultierenden Erkenntnisse allen Ressorts zur Verfügung stellen, um damit die Informationssicherheit in der gesamten Landesverwaltung zu stärken.

- Grundsätzlich gehen Sicherheitsstrategien von zwei Hauptansatzpunkten aus:
  1. Prävention: Das Eindringen von Schadsoftware soll möglichst verhindert werden. Hier aber sind die Möglichkeiten begrenzt. Unbekannte Schadsoftware neuen Typs wird von einem Virenscanner nur in seltenen Fällen durch ihr auffälliges Verhalten erkannt. Schutzmechanismen können i.d.R. nur aus der Analyse von Sicherheitsvorfällen entwickelt werden. Eine funktionierende, regelmäßige Datensicherung ist zwingend durchzuführen.
  2. Schnelle Reaktion: Sicherheitsexperten sind sich einig, dass das Eindringen von Schadsoftware nicht völlig verhindert werden kann. Deshalb ist es wichtig, Infektionen möglichst früh zu erkennen, um Schäden in Form von Datendiebstahl oder Datenzerstörung möglichst gering zu halten.

2. Situation im Geschäftsbereich des MIK

Die Behörden im Geschäftsbereich des MIK haben die CERT-Meldung vom 09.12.2015 erhalten und sind den Empfehlungen von CERT-NRW gefolgt. Bei vier Behörden konnte verschiedene Schadsoftware (u.a. auch die Schadsoftware TeslaCrypt, die aber nicht aktiv geworden ist und insbesondere keine Dateiverschlüsselungen ausgelöst hat) festgestellt werden. Mit einem vollständigen Scan von Servern und Rechnern und der Aktualisierung von Virensignaturen nach Mitteilung des sog. Hashwertes (Ergebnis der Ermittlungen beim MIK) sind notwendige Schutzmaßnahmen ergriffen worden. Datenverluste/ -beschädigungen wurden nicht gemeldet.

3. Situation in anderen Ressorts

Allen Ressorts ist die Meldung des CERT NRW vom 09.12.2015 zugeleitet worden.

Bei vier Ressorts konnte verschiedene Schadsoftware (u.a. auch die Schadsoftware TeslaCrypt) bei insgesamt 14 Behörden und Einrichtungen festgestellt werden. In allen Fällen konnten die Daten verlustfrei wieder hergestellt werden. Auch ein Datenabfluss wurde nicht festgestellt.