LANDTAG DES SAARLANDES
15. Wahlperiode

Drucksache 15/1867 (15/1720)
14.06.2016

A N T W O R T

zu der

Anfrage des Abgeordneten Andreas Augustin (PIRATEN)

betr.: Infizierung von Computersystemen des Landes durch die Schadsoftware „Locky“

Vorbemerkung des Fragestellers:

„Nach aktueller Presseberichterstattung hat die Schadsoftware „Locky“, die sich im weitesten Sinne als Trojanisches Pferd oder als Ransomware kategorisieren lässt, in Deutschland mit weitem Abstand mehr Computersysteme befallen als in anderen Ländern. Mit Stand vom 19.02.2016 geht man von 5.000 Neuinfektionen pro Stunde aus. „Locky“ verschlüsselt Dateien der Nutzer, benennt diese um und stellt anschließend eine „Lösegeldforderung“ an die Betroffenen. In dem „Erpresserschreiben“ wird darauf hingewiesen, dass die Dateien nur mit einer speziellen Software namens "Locky Decryptor" wieder entschlüsselt und dadurch gerettet werden können, für deren Bereitstellung der Erpresser vom Opfer die Zahlung eines bestimmten Betrags verlange.
Dies kann auch öffentliche Einrichtungen betreffen. So hat z.B. ein Krankenhaus in Los Angeles Lösegeld gezahlt, aber auch die Deutsche Stadt Dettelbach in Unterfranken hat erst letzten Monat in einem ähnlichen Fall Lösegeld gezahlt.
Vor dem Verlust der Daten kann man sich dadurch schützen, dass regelmäßig und somit insbesondere vor Befall der eigenen Daten ein Backup erstellt wird, das gegebenenfalls wiederhergestellt werden kann. Im beruflichen Umfeld bedeutet dies allerdings, dass Betroffene warten müssen, bis Backups zurückgespielt wurden, sodass das System währenddessen nicht genutzt werden kann und zusätzliche Kosten entstehen. Nicht zuletzt werden die Administratoren, die die Backups zurückspielen, damit auch von sonstiger Arbeit abgehalte.“

Ausgegeben: 14.06.2016 (08.03.2016)

Vorbemerkung der Landesregierung:

Die nachfolgenden Antworten der Landesregierung beziehen sich auf die Landesverwaltung. Darüber hinaus gehende Informationen liegen der Landesregierung nicht vor.

> Wurden bereits bzw. werden zur Zeit alle Systeme der Landesregierung, ihrer Ministerien und der nachgeordneten Behörden oder der technischen Infrastruktureinrichtungen (Bspw. Energieversorgung, Gasversorgung, Fernwärme, Kommunikation, Verkehrsinfrastruktur, Finanz- und Bankeninfrastruktur) und der sozialen Infrastruktureinrichtungen (wie z.B. Bildungs-, Hochschul- und Forschungssystem, Fürsorge-Dienstleistungen, Gesundheitssystem, Öffentliche Sicherheit und soziale Sicherung) auf eine mögliche Infizierung mit „Locky“ hin überprüft?
> a) Wenn ja, wie ist der aktuelle Prüf- und Bearbeitungsstand?
> b) Wenn nein, warum wird von der Durchführung einer solchen Überprüfung abgesehen?

Zu Frage 1:

Zur Abwehr von IT-Angriffen wird an zentraler Stelle (IT-Dienstleistungszentrum) als auch in den Ressorts Virenschutzsoftware eingesetzt. Diese wird mindestens täglich aktualisiert und über geeignete Mechanismen den Nutzern zur Verfügung gestellt. Zusätzlich werden die Mails von außen mit zwei Virenscannern untersucht. Diese Untersuchung wird auch bei den Mailrelays, über die der interne Mailverkehr läuft, durchgeführt.

> Wie viele Systeme der Landesregierung, ihrer Ministerien und nachgeordneten Behörden sowie solche der technischen und sozialen Infrastruktureinrichtungen wurden mit dieser Schadsoftware infiziert? Bitte die Systeme auch den entsprechenden Behörden zuordnen und diese benennen.

Zu Frage 2:

Mit der Schadsoftware "Locky" wurde in den Ministerien kein Arbeitsplatz infiziert. Lediglich in zwei nachgeordneten Behörden waren in Summe 5 Arbeitsplätze von der Schadsoftware befallen. Aus Sicherheitsgründen können diese nicht benannt werden.

Bei welchen Arten von Systemen (Server, Arbeitsplatzrechner, Laborcomputer etc.) der Landesregierung, der Ministerien und der nachgeordneten Behörden sowie der technischen und sozialen Infrastruktureinrichtungen werden regelmäßige Sicherungen („Backups“) erstellt, auf welche im Falle eines Datenverlustes zurückgegriffen werden kann und in welchem zeitlichen Abstand werden diese Datensicherungen erstellt?

Zu Frage 3:

Grundsätzlich werden die Daten der geschäftsrelevanten Server in den Ressorts mindestens täglich durch entsprechende organisatorische und technische Maßnahmen gesichert. Durch den weit verbreitenden Einsatz von Windows-Terminal-Server-Technologie findet die Datenspeicherung vorwiegend auf Daten- (Fileserver) oder Fachanwendungsservern statt. Lokale Arbeitsplatzrechner werden nach dienststellenspezifischen Regularien gesichert.

Welche Kosten sind durch eventuelle Wiederherstellung bestehender Sicherungen entstanden?

Zu Frage 4:

Da nur 5 Arbeitsplätze in den nachgeordneten Behörden durch die Schadsoftware "Locky" infiziert wurden, sind keine nennenswerten Kosten für die Wiederherstellung entstanden. Die Daten konnten durch eine Rücksicherung mit überschaubaren minimalem zeitlichen Aufwand wiederhergestellt werden.

Welche Kosten entstanden dadurch, dass Bedienstete der Landesregierung oder der ihr nachgeordneten Behörden sowie der technischen und sozialen Infrastruktureinrichtungen während der Durchführung der Datenwiederherstellung die Computersysteme nicht nutzen konnten und keinen Zugriff auf ihre Daten hatten?

Zu Frage 5:

Es sind keine konkretisierbaren Kosten entstanden.

Wurde im Falle einer Infektion mit Locky „Lösegeld“ gezahlt, um mit Hilfe von Locky Decryptor wieder Zugriff auf die gesperrten Daten zu erhalten?

Zu Frage 6:

Nein.