



### **Kleine Anfrage**

des Abgeordneten Uli König (PIRATEN)

**und**

**Antwort**

**der Landesregierung - Ministerpräsident**

### **Kenntnisse der Landesregierung über Infektionen von Computersystemen durch Ransomware Anfrage 2**

#### Vorbemerkung des Abgeordneten:

In ihrer Antwort auf meine Kleine Anfrage vom 31.03.2016 hat die Landesregierung erklärt, dass sie Kenntnisse über die Infektionen von sechs Computersystemen durch sogenannte Ransomware hat.

#### Vorbemerkung der Landesregierung:

Es wird vorab darauf hingewiesen, dass sich die betroffenen Systeme teilweise nicht in unmittelbarer Zuständigkeit der Landesregierung befinden und die Auskünfte der betreffenden Stellen auf freiwilliger Basis erfolgten.

1. Welche Einrichtungen waren genau durch die Infektionen betroffen? Bitte namentlich nennen.

#### Antwort:

Aus Sicherheitsgründen werden konkrete Informationen zu den Standorten und den Systemen nicht veröffentlicht, können aber vertraulich mitgeteilt werden.

2. Wie lange waren die fünf Systeme, bei denen ein Backup eingespielt werden musste, außer Betrieb?

Antwort:

Standort A	ca. einen Tag außer Betrieb
Standort B	einen Nachmittag außer Betrieb, der Client wurde während der Ausfallzeit nicht benötigt
Standort C	der Client war ca. 30 Minuten außer Betrieb, für das Einspielen der Sicherung auf dem Server wurde ein halber Tag benötigt
Standort D	der Fileserver war ca. vom 07.12.2015 11:00 Uhr bis 08.12.2015 13:20 Uhr außer Betrieb

3. Standen währenddessen Ersatzsysteme zur Verfügung, um den laufenden Betrieb weiterhin zu gewährleisten?

Antwort:

Standort A	es war kein Ersatz möglich, da durch die Verschlüsselung auf dem Fileserver der gesamte Standort betroffen war
Standort B	Ersatzsystem stand zur Verfügung, der Einsatz war nicht notwendig
Standort C	Ersatzsystem wurde sofort eingesetzt
Standort D	Ersatzsystem stand nicht zur Verfügung, es war lediglich ein Fileserver betroffen, IT-Fachverfahren standen durchgehend zur Verfügung

4. Hat die Landesregierung über entstandene Kosten, die durch den Ausfall der Systeme bzw. für die Beseitigung der Viren entstanden sind? Bitte aufschlüsseln nach System.

Antwort:

Der Schadsoftwarebefall konnte, soweit bekannt, mit eigenem IT-Personal bzw. im Rahmen der bestehenden Supportverträge mit dem Dienstleister Dataport ohne finanzielle Mehrbelastung für den Landeshaushalt behoben werden. Die Beschaffung neuer Hard- und / oder Software war nicht erforderlich.

5. Hat die Landesregierung Kenntnis über den Weg, über den die Schadsoftware in die Systeme eingedrungen ist? Bitte aufschlüsseln nach betroffenem System.

Antwort:

In einem identifizierten Fall erfolgte die Infizierung durch eine E-Mail-Anlage in einem privaten Webmail-Postfach.

6. Welche Betriebssysteme waren von den Infektionen betroffen? Bitte aufschlüsseln nach betroffenem System und Version des Betriebssystems.

Antwort:

In einem Fall handelt es sich um einen Windows 7 Client, zu weiteren Systemen werden aus Sicherheitsgründen konkrete Informationen nicht veröffentlicht.

7. Wie genau werden Mitarbeiter der Landesregierung bezüglich der Prävention durch Computervirenbefall geschult?

Antwort:

Es erfolgen per E-Mail aktuelle Warnmeldungen, die in der Regel Handlungsempfehlungen enthalten. Die Mitarbeiterinnen und Mitarbeiter werden in Fort- und Ausbildungsveranstaltungen sensibilisiert. Die entsprechenden Veranstaltungen werden im Intranet bekannt gegeben.

8. Werden auf allen Rechnern der Landesregierung Antivirenprogramme eingesetzt? Wenn nein, warum nicht?

Antwort:

Alle an die +1 Infrastruktur angebotenen Landesbehörden nutzen standardmäßig den zentralen Antivirensoftware Management Service aus +1 Infrastruktur.