SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 18/1941**
18. Wahlperiode 04.06.2014

Kleine Anfrage

des Abgeordneten Uli König (PIRATEN)

und

Antwort

der Landesregierung - Ministerpräsident

Stand der IT-Sicherheit in Schleswig-Holstein

1. *Ist das Land in der Lage Cyber-Angriffe auf die IT-Systeme von Behörden zu erkennen? Wenn ja, wie?*

   Antwort:
   Ja, über die Systemüberwachung und Auswertung von Protokolldateien.

2. *Sind Fälle von versuchten Cyber-Angriffen (beispielsweise Hacking) auf die IT-Systeme von Behörden des Landes Schleswig-Holstein bekannt?*
   a) Wenn Ja, diese bitte gesondert aufführen.

   Antwort:
   Gemäß der Definition des Nationalen Cybersicherheitsrates für Cyber-Angriffe[1] gab es im Jahr 2011 einen versuchten DDoS-Angriff auf die Webseite www.schleswig-holstein.de mit begleitendem Erpressungsversuch. Es handelte sich um einen wirtschaftskriminellen Hintergrund. Dieser konnte durch Dataport erfolgreich blockiert werden.

[1] Cyber-Sicherheitsstrategie für Deutschland; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

b) Ist das Land in der Lage auf Cyber-Angriffe zu reagieren? Wenn Ja, wie?

Antwort:
Es gibt ein über den CERT-Verbund mit dem BSI und anderen Bundesländern vernetztes IT-Sicherheitsvorfallmanagement. Dieses ist eingebunden in das Informationssicherheitsmanagement des Landes. In diesem Rahmen stehen Strukturen, Prozesse und abgestimmte Maßnahmen, z.B. Sperrprozesse für Firewallsysteme, zur Verfügung, die die Landesverwaltung in die Lage versetzen, auf Cyber-Angriffe angemessen zu reagieren.

3. *Gibt es IT-Dienste des Landes (E-Government, E-Mail, SMS, Informationsdienste etc.), die eine bestimmte Verfügbarkeit erfüllen müssen? Wenn ja, welche IT-Dienste sind dies und welche Verfügbarkeit müssen diese erfüllen?*

Antwort:
Die Anforderung an die Verfügbarkeit hängt von den mit den IT-Diensten verarbeiteten Daten ab. Darüber hinaus sind Mindestverfügbarkeitsanforderungen zentraler Basisinfrastrukturen definiert; diese sind für das Landesnetz Basis und LN V+ sowie die Basisinfrastrukturkomponenten E-Mail-Dienst, Anmeldedienst und Benutzerverwaltung sowie +1 Infrastruktur als „hoch“ gem. BSI-Grundschutz definiert, für den E-Faxdienst als „normal“.

Wie wird diese Verfügbarkeit im Angesicht von Cyber-Angriffen, wie beispielsweise DDoS, sichergestellt?

Antwort:
Es werden umfangreiche Maßnahmen nach gängigen Standards ergriffen, die die Verfügbarkeit anforderungsgerecht herstellen.

4. *Wie würde im Fall einer landesweiten IT-Krise, das heißt „wenn mittelbar oder unmittelbar IT-bedingt ein Ausfall oder eine Beeinträchtigung von Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen mit nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen eintritt beziehungsweise zu erwarten ist“[2] die Verteilung der Zuständigkeiten zur Krisenbewältigung aussehen und wer trägt die Verantwortung?*

Antwort:
Eine IT-Krise wäre eine „strukturelle Krise“. Diese würde im Rahmen vorhandener Strukturen für die Krisenbewältigung behandelt.

2 Definition des Bundesministerium des Inneren in Nationaler Plan zum Schutz der Informationsinfrastrukturen

Gibt es eine zentrale Instanz zur Koordination zwischen den verschiedenen Stellen?

Antwort:
Die „Zusammenarbeit der Ministerien im Krisenfall, in besonderen Lagen und bei sonstigen Gefahren“ ist in den 1999 von der Landesregierung beschlossenen Grundsätzen geregelt. Demnach sind Krisenfälle besondere Ereignisse, deren Bewältigung – unbeschadet der Zuständigkeiten der einzelnen Ministerinnen und Minister der Landesregierung – einer unverzüglichen Abstimmung unter den betroffenen Ministerien bedarf. In Krisenfällen bildet die Landesregierung einen Krisenstab. Besondere Lagen sind Ereignisse unterhalb des Krisenfalles, die insbesondere dann gegeben sind, wenn wegen einer bevorstehenden Gefahr oder einer eingetretenen Störung der öffentlichen Sicherheit (…) die ständige Beobachtung der Lage erforderlich ist und/oder laufend Maßnahmen getroffen werden müssen (...). In einer besonderen Lage wird ein interministerieller Leitungsstab gebildet, der vom federführenden Ministerium einberufen und geleitet wird.

Über welches Medium würde die Kommunikation erfolgen, sind alternative Kontaktdaten wie beispielsweise Mobiltelefonnummern der Verantwortlichen anderer Behörden hinterlegt? Wie wird sichergestellt, dass diese stets aktuell sind?

Antwort:
Die Kommunikationswege sind im Rahmen der o.a. Zuständigkeiten definiert und werden entsprechend aktualisiert.

5. *Wird bei der Übermittlung von sensiblen Daten, wie zum Beispiel personenbezogenen Daten, Dienst- oder Geschäftsgeheimnissen etc. an Dritte oder an andere Behörden durch die Landesregierung Verschlüsselung eingesetzt?*

   a) *Wird eine Verbindungsverschlüsselung wie z.B. SSL eingesetzt? Wenn ja, wo im einzelnen? Wenn nein, ist geplant, eine Verbindungsverschlüsselung wie z.B. SSL einzusetzen?*
   b) *Wird eine Ende-zu-Ende Verschlüsselung wie z.B. PGP/GPG eingesetzt? Wenn ja, wo im einzelnen? Wenn nein, ist geplant, eine Ende-zu Ende Verschlüsselung wie z.B. PGP/GPG einzusetzen?*

      Antwort zu a) und b):
      Der Einsatz von Verschlüsselung obliegt der Daten verarbeitenden Stelle, also der verantwortlichen Behörde. Verschlüsselung wird entsprechend des jeweiligen Schutzbedarfes der verarbeiteten Daten eingesetzt.
      Die Art der Verschlüsselung hängt dabei im Einzelfall von technischen und strukturellen Voraussetzungen ab.
      Die Landesregierung stellt darüber hinaus folgende Verschlüsselungsmechanismen bei Infrastrukturdiensten bereit:
      - Kommunikation mit Externen über das Government-Gateway (SSL)
      - Telearbeit (VPN-Einwahl über das Internet, IPSec)
      - In der internen und externen Mailkommunikation (Grundverschlüsselung, PGP).

   c) *Wird perfect forward secrecy oder Ähnliches verwendet? Wenn ja, wo im einzelnen? Wenn nein, ist geplant perfect forward secrecy oder Ähnliches zu verwenden?*

      Antwort:
      Perfect forward secrecy (PFS) ist eine Eigenschaft von Verschlüsselungsverfahren, die eine zurzeit technisch nicht mögliche, aber denkbare nachträgliche Entschlüsselung verschlüsselt gesendeter Inhalte zusätzlich erschwert. Auch hier gilt das Prinzip, dass Verschlüsselungsverfahren aufgrund von Anforderungen der Daten verarbeitenden Stellen eingesetzt werden.

d) Ist das verschlüsselte Netz des Landes LN V+ bereits fertiggestellt? Wenn nein, wie ist der aktuelle Stand und wann ist mit dessen Fertigstellung zu rechten.

Antwort:
Die Errichtungsphase für LNV+ ist abgeschlossen.
Bis zum heutigen Tage (Stand 26.05.2014) sind 305 Anschlüsse ausgerollt und aktiviert. Weitere 28 Landesdienststellen befinden sich derzeit im Rollout.
Grundsätzlich sind alle Landesdienststellen an das redundante LNV+ Netz angeschlossen. Sog. Kleinstdienststellen befinden sich noch in der Planungsphase.
Da durch Änderungen und Verbesserungen im laufenden Betrieb generell ein laufender Aufwand entsteht, ist nicht damit zu rechnen, dass ein Netz wie LN V+ prinzipiell als fertiggestellt bezeichnet werden kann.