LANDTAG DES SAARLANDES
15. Wahlperiode **Drucksache 15/404 (15/340)**
18.03.2013

A N T W O R T

zu der

Anfrage des Abgeordneten Hubert Ulrich (B90/Grüne)

betr.: Cyber-Strategie und Cyber-Angriffe auf die IT-Infrastruktur der Landesregierung

Vorbemerkung Fragesteller:

„Die „Cyber-Sicherheitsstrategie für Deutschland“ der Bundesregierung betrachtet den Schutz des Cyber-Raums als existentielle Frage des 21. Jahrhunderts. Vor dem Hintergrund der von der Bundesregierung skizzierten Bedrohungslage und angesichts der Aufrüstungsdynamik im Cyber-Raum muss auch die Landesregierung anhand einer Cyber-Strategie Abwehrmechanismen zum Schutz vor Angriffen erarbeiten.“

Wurde die Landesregierung in der Vergangenheit Ziel von Cyberangriffen? Wenn ja: bitte aufschlüsseln nach Jahr und Art des Angriffs.

Zu Frage 1:

2012 fand ein Angriff auf Webseiten statt, die mit Joomla, Typo3 oder WordPress erstellt wurden. Hierbei handelte es sich um den so genannten Pharma-Hack.

Die Server wurden anschließend vom Netz genommen, ausgetauscht und neu aufgesetzt. Die ZDV-Saar hat auch von einer Spezialfirma einen Penetrationstest durchführen lassen, ohne dass es gelungen ist, in das Rechnersystem einzudringen. Ein weiterer Penetrationstest ist in Vorbereitung.

Welche Maßnahmen, Fähigkeiten und Mittel stellt die Landesregierung bisher konkret zur Prävention und zum Schutz vor Cyber-Angriffen sowie zur Wiederherstellung und zur Reaktion auf derartige Angriffe bereit?

Zu Frage 2:

Als Schutz werden derzeit Firewalls und Virenschutzsoftware eingesetzt. Im Zuge der ständigen Aktualisierung der Schutzmaßnamen ist zusätzlich in Planung, Web-Application-Firewalls und Intrusion-Detection-Systeme einzusetzen. Die Virenschutzsoftware wird nach Ablauf der Vertragslaufzeit neu ausgeschrieben, die Ausschreibung wird um weitere Sicherheitslösungen erweitert.

Ausgegeben: 20.03.2013 (04.02.2013)

Welche Maßnahmen hat die Landesregierung ergriffen, um die Bund-Länder-Kooperation im Bereich Cyber-Sicherheit zu verbessern und ein effektives Krisenmanagement im Fall eines Angriffs zu gewährleisten?

Zu Frage 3:

Im Jahr 2010 hat der IT-Planungsrat als zentrales Steuerungsgremium für die föderale Zusammenarbeit in der Informationstechnik seine Arbeit aufgenommen.

Das Saarland ist sowohl im IT-Planungsrat als auch in verschiedenen Arbeitsgruppen vertreten. Hierbei findet ein regelmäßiger Informationsaustausch zwischen Bund und Ländern statt und es werden einheitliche Standards zur Informationssicherheit zwischen Bund und Ländern vereinbart.

In der Kooperationsgruppe „Leitlinie Informationssicherheit“ des IT-Planungsrates wird eine für Bund und Länder verbindliche Informationssicherheitsleitlinie erarbeitet, in der als gemeinsame Strategie die Etablierung eines einheitlichen und einvernehmlichen Mindestsicherheitsniveaus festgelegt wird. Das Saarland wirkt gleichzeitig in der länderoffenen Arbeitsgruppe „Cybersicherheit“ mit, die von der Innenministerkonferenz zur Begleitung der Arbeit des nationalen Cybersicherheitsrates einrichtet wurde.

Zur Stärkung der Informationssicherheit innerhalb der Landesverwaltung wird die Landesregierung das ressortübergreifende Kompetenzteam „Informationssicherheit“ einsetzen. Dieses setzt sich aus Vertretern der Ressorts sowie des Landes-Rechenzentrums (ZDV-Saar) zusammen und wird vom IT-Innovationszentrum geleitet. Eine vorbereitende Facharbeitsgruppe hat bereits 2012 ihre Tätigkeit aufgenommen. Der Leiter des Kompetenzteams ist zusätzlich zentraler Ansprechpartner gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der angebotenen Sicherheitsberatung.

Welche Maßnahmen ergreift die Landesregierung zur Erhöhung des Selbstschutzes gegen Cyber-Angriffe?
a) Welche Maßnahmen plant sie zur Verbesserung des Meldesystems für den Informationsaustausch?
b) Welche Maßnahmen plant sie hinsichtlich der Dezentralisierung und Diversifikation der IT-Systeme (IT = Information Technology)?

Zu Frage 4a:

Im Rahmen der Umsetzung der „Leitlinie Informationssicherheit“ des IT-Planungsrates, die derzeit in der Bund/Länderabstimmung ist, wird die Landesregierung verschiedene Maßnahmen umsetzen. Hierzu zählt beispielsweise der Aufbau eines Managementsystems für Informationssicherheit (ISMS). Ein ISMS ist ein Rahmenwerk zur Etablierung und Fortführung eines kontinuierlichen Prozesses zur Planung, Lenkung und Kontrolle der Konzepte und Aufgaben, die auf die Wahrung der Ziele der Informationssicherheit in einer Institution gerichtet sind.

Eine weitere wichtige Forderung zur Verbesserung des Meldesystems bei Sicherheitsvorfällen ist der Aufbau eines Computer Emergency Response Teams (CERT). Dies ist eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen (z. B. Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebssystemen, neuartige Virenverbreitung oder bei Spam versendenden PCs) als Koordinator mitwirkt, Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet. Diese Aufgabe wird derzeit für das Saarland vom IT-Referat des Ministeriums für Inneres und Sport wahrgenommen. Aktuell prüfen wir bei der Weiterentwicklung des CERT eine Kooperation mit Rheinland-Pfalz. Die geforderten Maßnahmen zur Verbesserung der Informationssicherheit und damit zur Erhöhung des Selbstschutzes gegen Cyber-Angriffe werden dann auf Basis einer verbindlichen Landesleitlinie für die Informationssicherheit umgesetzt werden.

Zu Frage 4b:

Die Landesregierung hat mit Ministerratsbeschluss von 13.03.2012 eine Neuausrichtung der IT-Strukturen des Landes auf den Weg gebracht, deren Ziel es ist, den technischen Betrieb in einem IT-Dienstleistungszentrum zu zentralisieren. Dabei ist neben der Wirtschaftlichkeit und der Servicequalität auch die Gewährleistung der IT-Sicherheit ein zentrales Ziel. Das zukünftige IT-Landessystem- und Betriebskonzept sieht vor, dass Sicherheitslösungen zentral vorgehalten werden, um das gesamte Landesdatennetz auf hohem Niveau zu schützen. Die darin vernetzen Behörden und deren Arbeitsplatzcomputer können so von einem hohen Schutzniveau profitieren.