LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 6/2928**
6. Wahlperiode **30.04.2014**

ANTRAG

der Fraktionen der CDU und SPD

Bürgernahe Verwaltung - papierlose Kommunikation erfordert sichere IT-Strukturen

Der Landtag möge beschließen:

1. Der Landtag stellt fest,

   a) eine bürgernahe, moderne Verwaltung ist gekennzeichnet von einem einfachen elektronischen Zugang der Bürger zu den Behörden. Der papierlosen Antragsbearbeitung gehört die Zukunft. Sie ermöglicht eine rasche und transparente Erledigung der Anliegen.

   b) die stetig voranschreitende technologische Entwicklung erfordert eine kontinuierliche Betreuung der IT-Systeme in der Verwaltung sowohl des Landes als auch in den Kommunen. Daten und Kommunikation müssen effektiv gegen Manipulation, unberechtigten Zugriff und Datenverlust geschützt werden.

2. Die Landesregierung wird gebeten zu prüfen, ob unter Einbeziehung des Städte- und Gemeindetages Mecklenburg-Vorpommern und des Landkreistages Mecklenburg-Vorpommern aufeinander abgestimmte IT-Sicherheitskonzepte, aufbauend auf den Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ erarbeitet werden können, damit die IT-gestützten Geschäftsprozesse in den Kommunen unter besonderer Berücksichtigung der Bürgernähe, der Effektivität und Effizienz des Verwaltungshandels gestärkt werden können.

Vincent Kokert und Fraktion

Dr. Norbert Nieszery und Fraktion

Begründung:

Zu Ziffer 1 a)

Eine moderne Verwaltung bedeutet Bürgernähe, Bürokratieentlastung und Effizienz der Verwaltung. Hierzu gehört auch eine papierlose, elektronische Behörden-Bürger-Kommunikation.

Für Bürger und Unternehmen bedeutet eGovernement einen besseren Kontakt mit den Behörden. Ziel soll die Möglichkeit sein, online Anträge stellen zu können oder/und Bescheide abzurufen. Aus Sicht der Verwaltung bedeutet das eGovernement eine Nutzung von effektiveren und effizienteren Verwaltungsverfahren. Durch das elektronische Verfahren können Vorgänge schneller und - soweit notwendig und datenschutzrechtlich zulässig - transparent gestaltet werden.

Zu Ziffer 1 b)

Bei der Umsetzung des eGovernement müssen die Sicherheitsbelange aller Teilnehmer (Bürger, Unternehmen, Verwaltung) berücksichtigt werden.

Durch die NSA-Affäre ist die permanente Bedrohung der IT-Infrastrukturen durch „einfache“ Angriffe aus dem Blickpunkt der Öffentlichkeit verdrängt worden. Die IT-Systeme sind regelmäßig solchen Angriffen ausgesetzt - sei es zum Zwecke des Datendiebstahls oder um ein Bot-Netz für Angriffe auf weitere Netzwerke aufzubauen. Diese Angriffe erfolgen massenhaft und setzen auf Sicherheitslücken der IT-Strukturen. Allein die Systeme der DVZ-GmbH sind täglich mehreren Hunderttausend Angriffen ausgesetzt, davon 20.000 Port-Scans (Suche nach Sicherheitslücken im IT-Netzwerk) und 1.500 DoS-Attacken (Denial-of-Service Angriffen, d. h. der Versuch der Beeinträchtigung der Serververfügbarkeit durch Überlastung), wie der Landtagsdrucksache 6/2215 zu entnehmen ist.

Mit dem zunehmenden Grad der elektronischen Verwaltung steigen daher auch die Anforderungen an die Sicherheit der Daten. Die elektronische Datenverarbeitung muss stets den drei Grundsätzen Vertraulichkeit, Verfügbarkeit und Integrität genügen. Die Verwaltung muss hierauf rechtzeitig vorbereitet sein.

Einmalige Investitionen in die IT-Sicherheit können allenfalls temporär erfolgreich sein. Die Sicherheit der IT-Technik der Behörden muss permanent begleitet werden, da die Intensität der Angriffe mit dem technischen Fortschritt kontinuierlich steigt.

Zu Ziffer 2

Die Sicherheit von Kommunikationsstrukturen ist aber immer nur so stark, wie das schwächste Glied. Deshalb ist es notwendig, in den Behörden des Landes und der Kommunen einheitliche Mindeststandards zu erreichen und dauerhaft zu festigen.
Die Erarbeitung von abgestimmten IT-Sicherheitskonzepten der Landes- und Kommunalbehörden ist hierzu ein erster notwendiger Zwischenschritt. Ausgehend von der, vom IT-Planungsrat beschlossenen „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ soll ein Konzept zum Aufbau und Betrieb eines landesweiten Informationssicherheitsmanagements erarbeitet werden, mit welchem die Behörden des Landes in die Lage versetzt werden, bei IT-Angriffen, IT-Krisen und in Notfällen schnell, effizient und umfassend zu reagieren.
Damit auch die Kommunalbehörden vor Bedrohungen der IT-Infrastruktur geschützt werden können, ist zu prüfen, welche Empfehlungen und Möglichkeiten der Partizipation sich daraus ergeben können. Im Rahmen einer solchen Betrachtung werden folgende Punkte relevant: Bereitstellung von Experten für die Behandlung von Sicherheitsvorfällen, Mitnutzung eines Warn- und Informationsdienstes, der über mögliche Angriffe, Sicherheitslücken sowie neue Angriffswerkzeuge und entsprechende Gegenmaßnahmen informiert, Mitarbeit in der Kommission für Informationssicherheit der Landesverwaltung, Mitnutzung von Sensibilisierungs- und Schulungsmaßnahmen zur IT-Sicherheit, Unterstützung bei der Notfallvorsorge und der Durchführung von Sicherheitsaudits.