CDU-Fraktion 24.03.2015

Antrag	Vorlage-Nr: VO/2015/5388 Öffentlichkeitsstatus: öffentlich

Digitale Sicherheit im Konzern Stadt Osnabrück

Beratungsfolge:

Gremium	Datum	Sitzungs-art	Zuständigkeit	TOP-Nr.
Verwaltungsausschuss	21.04.2015	N	Vorberatung	
Rat der Stadt Osnabrück	21.04.2015	Ö	Entscheidung	

Beschluss:
Die Verwaltung wird beauftragt, den derzeitigen Stand des "digitalen Schutzes" im Organisations-, Personal- und Gleichstellungsausschuss darzustellen und nach Beschluss des IT-Sicherheitsgesetzes im Deutschen Bundestag aufzuzeigen, welche Maßnahmen getroffen werden müssen und wie eine stetige Überprüfung der Sicherheitsmaßnahmen stattfinden wird.
In den entsprechenden Aufsichtsräten der städtischen Gesellschaften und gegebenenfalls deren Beteiligungen etc. sind die Mitglieder ebenso zu informieren.

Begründung
Der Bundestag wird in diesem Jahr das IT-Sicherheitsgesetz verabschieden, das u.a. vorsieht, dass kritische IT-Infrastruktur einem gewissen Sicherheitsniveau entsprechen muss (Stichwort "BSI-Grundschutz"). Im Konzern Stadt betrifft das wahrscheinlich z.B. Stadtwerke, Klinikum, Feuerwehr. Das ist sinnvoll, denn Angriffe auf IT-Infrastrukturen sind realistisch. Cyber-Kriminalität ist heute schon allgegenwärtig. Im aktuellen Lagebericht zur IT-Sicherheit der Bundesregierung ist auch von einer steigenden Zahl von IT-Angriffen zu lesen.
Die Digitalisierung schreitet weiter voran - auch bei der Stadt Osnabrück - es sei nur DMS genannt oder E-Personalausweis, DE-Mail, digitale Vergabe usw.
Dies betrifft nicht nur die Verwaltung intern sondern auch die Zusammenarbeit mit "Draußen". Um hier einen reibungslosen Ablauf sicherzustellen und Schäden zu vermeiden, ist es wichtig, Gefährdungen früh zu erkennen und höchste Sicherheitsanforderungen zu verfolgen.

Die Digitale Sicherheit betrifft mehrere Ebenen, die nicht losgelöst voneinander betrachtet werden könnten:

Beispielhaft seien genannt:
- Schutz von Infrastruktur gegen physikalische Einflüsse - wie z.B. Feuer
- Schutz gegen unbefugten Zugriff auf Daten und Kommunikation bzw. Unbrauchbarmachen von außen und innen - z.B. "Hacken"
- Schutz gegen "Einspielen" von Schadsoftware - z.B. "verseuchte" USB-Sticks
- Ständige Aktualisierung von Software und Hardware durch Aufspielen von Updates
- Schulung von Mitarbeiterinnen und Mitarbeitern
- Einhaltung des Datenschutzes - auch bei Aussonderungen
- Nutzung von Infrastruktur für illegale Aktivitäten

Diese Anforderungen gelten natürlich auch für externe Dienstleister, wie z.B. der Firma ITEBO, mit denen zusammengearbeitet wird.

Ein weiterer Aspekt in diesem Zusammenhang ist natürlich auch das Thema "Datenschutz" und die Nutzung neuer Medien (Stichwort "Social Media Guidelines").

Der Inhalt der Vorlage unterstützt folgende/s strategische/n Stadtziel/e:
nicht zutreffend

gez. Dr. E. h. Fritz Brickwedde
CDU-Fraktionsvorsitzender