



STELLUNGNAHME zur Anfrage Stadtrat Friedemann Kalmbach (GfK) Stadtrat Eduardo Mossuto (GfK)	Vorlage Nr.:	2017/0730
	Verantwortlich:	Dez. 2
IT-Sicherheit der Stadt		

Gremium	Termin	TOP	ö	nö
Gemeinderat	12.12.2017	37	x	

1. Kam es in der Vergangenheit schon zu Angriffen auf das Netzwerk der Stadt Karlsruhe?

Die Stadt Karlsruhe ist - wie jede größere Organisation - täglich Angriffen aus dem World Wide Web ausgesetzt.

a. Wenn ja, wie viele Angriffe wurden ausgeübt?

Von den ca. 465.000 Mails, die die Stadt pro Monat empfängt, werden ca. 81 % als Spam oder gefährliche Mail erkannt und in einem mehrstufigen Verfahren automatisch ausgesondert. Darunter befinden sich ca. 500 Angriffe/Monat mit so genannten Trojanern. Direkte Angriffe auf Windows-Serversysteme erfolgten im Jahr 2017 bislang ca. 2.430.

b. Welche Arten von Angriffen wurde die Stadt Karlsruhe ausgesetzt?

In der jüngeren Vergangenheit hat die Bedrohung durch Verschlüsselungstrojaner (so genannte Ransomware) zugenommen. Insbesondere durch schadhafte Dateianhänge gelangen Datenpakete in das betroffene Datennetz und führen zur Verschlüsselung ganzer Rechnersysteme. Dabei werden oftmals aktuelle Sicherheitslücken von Softwareprodukten ausgenutzt, die dann seitens der Hersteller geschlossen werden.

c. Welcher Schaden könnte entstehen?

Angriffe auf Computernetze und Systeme sind grundsätzlich potentielle Gefahren für die darauf verarbeiteten Daten. Ein Kompletterverlust könnte zu sehr hohen Aufwänden für die Wiedergewinnung der Daten führen (falls überhaupt möglich).

Auch die Wiederherstellung einer komplexen Systemkonfiguration zentraler Netzwerke ist mit hohen personellen Aufwänden verbunden.

d. Ist in der Vergangenheit schon Schaden entstanden und wenn ja, in welcher Form?

Es ist - seit Amtsgründung IT - kein nennenswerter Schaden entstanden. Von Ransomware attackierte Rechner konnten ausnahmslos per Backup wiederhergestellt werden.

2. Welche Maßnahmen hat die Stadtverwaltung zum Schutze der IT umgesetzt?

Die Stadt Karlsruhe hat 2011 als eine der ersten Städte in Baden-Württemberg einen IT-Sicherheitsbeauftragten bestimmt, der nun organisatorisch dem Amt für Informationstechnik und Digitalisierung zugeordnet ist. Von dieser Stelle wurden zahlreiche Maßnahmen koordiniert, orientiert an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik.

Beispiele für Sicherheitsmaßnahmen:

- Erlass einer Informationssicherheitsleitlinie
- Durchführung einer IT-Sicherheits-Awarenesskampagne
- Aufbau redundanter Serverzentren
- Einsatz verschlüsselter USB-Devices
- Ausbau des Datennetzes (Ringtopologie) bei wichtigen Lokationen
- Nutzungsvereinbarungen für mobile Endgeräte
- Einsatz von Virtualisierungstechnologien für ein schnelles Patchmanagement
- Neubau einer modernen Rechenzentrumszelle im Rathaus (inkl. Brand- und Einbruchschutz)
- Auslagerung wichtiger Daten und Systeme zum kommunalen Rechenzentrum KIV BF

3. Welche weiteren Maßnahmen sind in Planung?

Für die nächsten Monate stehen derzeit folgende Maßnahmen auf der Agenda:

- Konzeption und Aufbau der neuen Web-Application-Firewall
- Segmentierung und Virtualisierung der bisherigen Internetplattform
- Konzeption einer Neuauflage der Awarenesskampagne
- Prüfung einer eventuellen Cyberversicherung
- Ausbau der Backup-Infrastruktur
- Neue technische Plattform für die Seite „karlsruhe.de“

4. Reicht der bisherige Schutz der Netzwerk-Infrastruktur und der Server der Stadt Karlsruhe aus?

Das Amt für Informationstechnik und Digitalisierung unternimmt derzeit die nach Stand der Technik und gemäß BSI-Grundschutz empfohlenen Maßnahmen, um ein hohes Maß an IT-Sicherheit zu erzielen. Gleichwohl kann nicht ausgeschlossen werden, dass neuere Angriffsszenarien zu schwerwiegenden Angriffen auf den Dienstbetrieb der Stadtverwaltung führen.

a. Wenn nein, welche Maßnahmen sollten nach Einschätzung der Verwaltung getroffen werden um das Maß an Sicherheit zu heben?

Ein besonderer Schwerpunkt sollte auf der weiteren Sensibilisierung der Mitarbeiterinnen und Mitarbeiter liegen. IT wird hierzu eine neue IT-Sicherheitskampagne auflegen. Zudem muss dauerhaft in die Aktualisierung der eingesetzten Sicherheitssysteme investiert werden.

b. Werden Sicherheitsexperten oder Unternehmen von der Stadt beauftragt, die Infrastruktur der Stadt auf ihre Sicherheit zu testen, bspw. durch Angriffsversuche?

Ja. In Zusammenarbeit mit der Karlsruher IT-Sicherheitsinitiative wurden solche Tests (Penetrationstests) durchgeführt. Die dabei gewonnenen Erkenntnisse sind in die oben beschriebenen und umgesetzten Maßnahmen und Planungen eingeflossen.