



Herrn Stadtrat  
Karl Richter  
BIA

Rathaus

Datum  
29.09.2011

**Wie steht es um die Cyber-Sicherheit in München?**

Schriftliche Anfrage gemäß § 68 GeschO  
von Herrn Stadtrat Karl Richter  
vom 17.06.2011, eingegangen am 17.06.2011

Sehr geehrter Herr Stadtrat Richter,

auf Ihre Anfrage vom 17.06.2011 nehme ich Bezug. In dieser beziehen Sie sich auf die Inbetriebnahme des Abwehrzentrums der Bundesregierung gegen Angriffe aus dem Internet sowie die Zahlen der täglich auf das Informationsnetz der Bundesregierung registrierten Internetangriffe. Vor diesem Hintergrund erkundigen Sie sich nach dem Stand der Cyber-Sicherheit in München.

Vorab bedanke ich mich für die entsprechend meiner Zwischennachrichten vom 28.06.2011 und 27.09.2011 gewährten Terminverlängerungen.

Zu den im Einzelnen gestellten Fragen kann ich Ihnen folgendes mitteilen:

**Frage 1:**

*Welche Dienststelle der Stadt München ist für den Schutz der städtischen Kommunikationsinfrastruktur gegen Angriffe aus dem Internet zuständig? Wie viele Mitarbeiter umfasst diese Dienststelle? Welcher Mittelansatz ist für diese Dienststelle im städtischen Haushalt unter welcher Produktziffer eingestellt?*

**Antwort:**

Die Zuständigkeit für den Schutz der städtischen Kommunikationsinfrastruktur, genauer gesagt für den Schutz des Verwaltungsnetzes, gegen Angriffe aus dem Internet liegt beim Direktorium, HA-III Informationstechnologie (D-III).

Rathaus, Marienplatz 8  
80331 München  
Telefon:233 - 82100  
Telefax:233 - 82165

Bei D-III sind 286 aktive Mitarbeiterinnen und Mitarbeiter beschäftigt (Stand 14.07.2011).

Die Produktziffern lauten:

- 5130002 für ITD
- 5130004 für LiMux-Projekt
- 513010009 für ITS

Der Mittelansatz von D-III beträgt:

- 13.873.200 € im Personalbereich
- 38.963.863 € im Sachhaushalt

**Frage 2:**

*Wie hat sich die Sicherheits- und Bedrohungslage für das städtische Netzwerk in den letzten Jahren entwickelt? Inwieweit kann die Stadt die z.B. vom BSI registrierte Zunahme von Internet-Angriffen auf deutsche Behördenrechner für den Bereich der LHM bestätigen? Falls Informationen vorliegen: wie entwickelten sich die Zahlen registrierter Internet-Attacken gegen Münchner Behörden und Dienststellen in den letzten Jahren?*

**Antwort:**

Die Sicherheits- und Bedrohungslage für das städtische Netzwerk hat sich – nach dem Kenntnisstand von D-III – in den letzten Jahren nicht anders entwickelt als für alle anderen Behörden bzw. Teilnehmer am Internet.

Zahlenmaterial über Internetangriffe gegen die Stadt München liegt nicht vor.

**Frage 3:**

*Wie beurteilt die Stadt die Gefahr größerer Schäden bzw. Beeinträchtigungen an Einrichtungen der Münchner Infrastruktur durch gezielte Cyber-Attacken? Zu denken wäre z.B. an Angriffe gegen die Stadtwerke, auf die Stromversorgung etc. Inwieweit liegen dazu aktuelle Risikoschätzungen entweder von städtischer oder dritter Seite vor? Haben sich solche Vorfälle bereits ereignet?*

**Antwort:**

Die Methoden der Angreifer werden immer raffinierter, und die Abwehr von Angriffen erfordert einen immer höheren Aufwand.

Gegen „Standardattacken“ ist das Verwaltungsnetz gut gewappnet. Gegen professionelle Attacken von Experten mit entsprechenden Ressourcen kann sich die Landeshauptstadt München ebenso wenig absichern wie andere Organisationen.

Bislang hat es keine erfolgreichen Angriffsversuche auf städtische Fachanwendungen sowie die für die Infrastruktur erforderlichen IT-Komponenten gegeben.

Hinsichtlich der Stadtwerke München fällt die Angelegenheit in den operativen Geschäftsbereich der Stadtwerke München (SWM). Diese teilen mit:

Die IuK-Systeme werden in den Geschäftsprozessen eingesetzt und unterliegen einem kontinuierlichen Verbesserungsprozess. Dabei werden Veränderungen in der Bedrohungslage laufend erkannt, bewertet und entsprechende Maßnahmen eingeleitet.

Durch verschiedene Maßnahmen wird dafür Sorge getragen, dass das bestehende Sicherheitsniveau bestehen und wenn nötig und möglich laufend verbessert wird.

**Frage 4:**

*Inwieweit ist – falls vorhanden – der Cyber-Schutz der Stadt München in überregionale Architekturen der Netzsicherheit eingebunden, z.B. auf Landesebene? In welchen Abständen finden in diesem Rahmen Übungen statt? Wie ist das Zusammenwirken der städtischen „Cyber-Abwehr“ mit den zuständigen Dienststellen der Polizei geregelt?*

**Antwort:**

Im Rahmen der zunehmenden Online-Zusammenarbeit der Behörden sowie der Zentralisierung von Registern sowohl auf Bundes- als auch auf Landesebene ist das Netz der LHM an verschiedene überregionale Netze angebunden.

Übungen zur Cyber-Sicherheit finden nicht statt. Es erfolgt jedoch ein Informationsaustausch mit den Betreibern der überregionalen Netze.

Die Kontaktaufnahme mit dem Landeskriminalamt Bayern bzw. dem Polizeipräsidium München erfolgt im Einzelfall bei Vorliegen eines Verdachts auf strafbare Handlungen.

**Frage 5:**

*Welche Informationen liegen der Stadt darüber vor, in welchem Umfang in München ansässige Firmen Ziel von Angriffen aus dem Internet geworden sind? Falls vorhanden, bitte Fallzahlen der letzten fünf Jahre aufführen!*

**Antwort:**

Der Stadt liegen keine Informationen darüber vor.

**Frage 6:**

*Wie verteilen sich Cyber-Attacken gegen Münchner Unternehmen auf*

- *Versuche der Ausspähung,*
- *Versuche, Firmeneinrichtungen (z.B. Rechner, Produktionsanlagen) gezielt zu schädigen?*

*Falls vorliegend, bitte Zahlen der letzten fünf Jahre aufführen!*

**Antwort:**

Siehe Antwort zu Frage 5.

**Frage 7:**

*Inwieweit sieht sich die Stadt veranlasst, bei ihrer Cyber-Sicherheit nachzurüsten, etwa in Gestalt weiterer Stellenzuweisungen? Oder hält die Stadt ihre Kommunikationsarchitektur für ausreichend gegen Angriffe aus dem Netz gesichert?*

**Antwort:**

Die mit der Nutzung des Internets verbundenen Risiken wachsen ständig. Hinzu kommt, dass sich die Intensität und der Charakter der Angriffe verändert. Zu der quantitativ hohen Zahl an

Angriffen kommt eine neue Qualität zielgerichteter Angriffe hinzu. Daher ist die vorhandene Infrastruktur laufend zu optimieren bzw. auf die geänderte Gefährdungssituation anzupassen. Die Notwendigkeit einer Anpassung der personellen Ausstattung in den nächsten Jahren kann nicht ausgeschlossen werden.

**Frage 8:**

*Warum enthält der jährliche „Sicherheitsreport“ der Münchner Polizei keine Informationen zum Themenfeld „Cyber-Sicherheit der städtischen Behörden“ - laut Bundesinnenminister Friedrich immerhin eine „existenzielle Frage des 21. Jahrhunderts“? (Hierzu bitte ggf. eine Stellungnahme des Münchner Polizeipräsidioms einholen!)*

**Antwort:**

Hierzu wurde eine Stellungnahme des Polizeipräsidioms München eingeholt, die im Folgenden wiedergegeben wird:

„Der Begriff Cyber-Sicherheit ist laut Definition des Bundesministeriums des Inneren der anzustrebende Zustand der IT-Sicherheitslage (Quelle: Cyber-Sicherheitsstrategie für Deutschland, veröffentlicht im Februar 2011). Eine Aussage, welche Straftaten aus Sicht des BMI diese Sicherheitslage „gefährden“, wurde jedoch nicht getroffen.

Unserer Ansicht nach ist dies jede Straftat, die Einfluss auf ein IT-System nimmt oder nehmen kann. Wir haben deshalb folgende Straftaten untersucht:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage
- § 316b StGB Störung öffentlicher Betriebe

2010 wurden in der Polizeilichen Kriminalstatistik insgesamt 51 derartige Straftaten festgehalten. In 32 Fällen waren Privatpersonen betroffen.

Angriffe auf städtische Rechner sind uns nicht bekannt.“

Ich bitte Sie, von den vorstehenden Ausführungen Kenntnis zu nehmen, und gehe davon aus, dass die Angelegenheit damit abgeschlossen ist.

Mit freundlichen Grüßen

gez.

Christian Ude