Sitzung	Stadtwerkeausschuss 25.06.2014
Thema	Anfrage zur Sicherheit der Steuerung der Stadtwerke für Strom/Gas/Wasser
Anfrage	Herr Ramcke (Fraktion Bündnis 90/DIE GRÜNEN) – Anfrage im Stadtwerkeausschuss am 14.05.2014
Beantwortung	Werkleitung: Axel Gengelbach, Jens Seedorff & Theo Weirich

Frage:
„In einem Artikel „Blackout" aus der Zeitschrift „DIE ZEIT" vom 10.04.2014 (siehe Anlage 1 auf den Seiten 3-5) wird beschrieben, dass es für einen – in diesem Fall extra engagierten – Hacker nur zwei Tage brauchte, um in das vermeintlich so sichere Steuerungssystem der Stadtwerke Ettlingen einzudringen. Auch das System der STW Ettlingen ist „isoliert" vom Internet.

Im Stadtwerkeausschuss vom 16.09.2013 wurde auf Anfrage von B 90/DIE GRÜNEN u.a. erläutert:

> *„Die Steuerung der Energie- und Wassernetze der Stadtwerke Norderstedt geschieht über ein Fernwirksystem, dass über eine Netzleitwarte geführt wird. Dieses System ist isoliert vom allgemeinen Internet in einem demilitarisierten – also in einem privaten – Netzwerk eingebunden. Ein externer Zugriff ist nicht vorhanden und damit ist eine direkte Manipulation von außen ausgeschlossen. Remotezugriffe für Wartungen und Systemanpassungen werden nur temporär über den Abteilungsleiter für Wartungsarbeiten zugelassen und dokumentiert". (Fragen und Antworten – TOP Datensicherheit und Systemsicherheit, Punkt 2 b)*

1. *Stimmt die Werkleitung vor dem Hintergrund des Artikels der Schlussfolgerung zu, dass externe Manipulation der Steuerungssysteme nicht ausgeschlossen sind und ist es demzufolge nicht ausreichend ist, sich (nur) auf getrennte Netze zu verlassen?*

2. *Wird der „erfolgreiche" Hackerangriff auf die Stadtwerke Ettlingen auch bei den STW Norderstedt ein Umdenken hervorrufen?*

3. *Wie wird insbesondere dem im Artikel angesprochenen Sicherheitsrisiko „Mensch" begegnet?*

Im Stadtwerkeausschuss am 09.04.2014 wurde u.a. über Normen, Anforderungen und Zertifizierungen der IT-Sicherheit berichtet. Aufgrund des sich ständig ändernden

Umfeldes und des hohen Gefährdungspotentials hat die IT-sicherheit nach unserer Meinung eine hohe Priorität. Bedauerlicherweise hat der Vortrag zur IT-Sicherheit vom 09.04.2014 den Ausschussmitgliedern vorab nicht zur Verfügung gestanden, so dass nun eine Reihe von Nachfragen erforderlich wird:

4. *Auf Seite 9 steht „Ein angemessener Schutz des Betriebes eines Energieversorgungsnetzes wird vermutet, wenn der Katalog der Sicherheitsanforderungen eingehalten und dieses vom Betreiber dokumentiert worden ist". Auf den Seiten 11-17 wird über das „ISMS" System berichtet. Auf Seite 21 wird nach der „Zertifizierung" gefragt. Das klingt nach sehr viel Bürokratie.*
   Sind der „Katalog der Sicherheitsanforderungen", ein „ISMS System" bei den Stadtwerken eingeführt? Falls nein, ist es ein Ziel diese Systeme einzuführen, sowie eine „Zertifizierung" zu erreichen?

5. *Sind derartige Konzepte zielführend, um einem kreativen, variantenreichen und sich stetig verändernden Hackerumfeld zu begegnen?*
   Inwieweit würden solche Konzepte helfen, dem Unsicherheitsfaktor „Mensch" (siehe im oberen Teil) zu begegnen?

6. *Bedeuten die Formulierungen auf Seite 20, dass das Sicherheitskonzept derzeitig lückenhaft ist? Es wurden „verschiedene Sicherheitsrichtlinien" in „verschiedene Sicherheitskategorien" eingeführt.*

7. *Der Vortrag schließt auf Seite 21 mit offen Fragen unter der Überschrift „Quo Vadis? – wo wollen die Stadtwerke hin?" ab.*
   Auch uns ist nach dem Vortrag bzw. Durchsicht der Unterlagen nicht klar was die nächsten (wesentlichen) Schritte sind?

Wir bitten um schriftliche Beantwortung."

Erläuterungen der Werkleitung

Frage 1:

Stimmt die Werkleitung vor dem Hintergrund des Artikels der Schlussfolgerung zu, dass externe Manipulation der Steuerungssysteme nicht ausgeschlossen sind und ist es demzufolge nicht ausreichend ist, sich (nur) auf getrennte Netze zu verlassen?

Antwort:

Bei dem IT-Angriff auf das Netzwerk der Stadtwerke Ettlingen wie es in dem Artikel der „Zeit" und des Weiteren in dem Fernsehbeitrag von ARTE dargestellt wurde, handelt es sich um einen internen Angriff durch externe Mitarbeiter. Die externen Mitarbeiter haben sich Zugang über das im Fall ausgelagerte interne Netzwerk verschafft. Die Stadtwerke Norderstedt sehen das eigene autarke Glasfasernetz als einen ganz wichtigen Baustein zur IT Sicherheit gegen externe Angriffe.

Frage 2:

Wird der „erfolgreiche" Hackerangriff auf die Stadtwerke Ettlingen auch bei den STW Norderstedt ein Umdenken hervorrufen?

Antwort:

Die Stadtwerke Norderstedt arbeiten schon über mehrere Jahre bei dem BDEW-Lenkungsausschuss Informationstechnik aktiv mit. Dort ist das Thema kritische Infrastrukturen und IT Sicherheit ein immer wieder diskutiertes Thema. Unter anderem wurde das vom BDEW herausgegebene Whitepaper "Anforderungen an sichere Steuerung und Telekommunikationssysteme" (Ursprungsversion 2008) und das in Zusammenarbeit mit „Österreichs Energie", dem dortigen Branchenverband, aufgearbeiteten Ausführungs-hinweise zur Anwendung des BDEW- Whitepaper (Ursprungsversion 2012) intensiv bearbeitet und praktische Umsetzungshinweise für Unternehmen ausgetauscht.

Die Verbandsarbeit in den Facharbeitsgruppen hat dazu geführt, dass die Stadtwerke Norderstedt nicht umdenken mussten, sondern aktiv mit dem Thema IT-Sicherheit umgegangen sind. Bevor das Thema in den Medien aufgegriffen wurde, haben sich die Stadtwerke Norderstedt mit ihrem Leitsystem-Hersteller in Verbindung gesetzt und geprüft, welche Verbesserungen erforderlich sind.

Frage 3:

Wie wird insbesondere dem im Artikel angesprochenen Sicherheitsrisiko „Mensch" begegnet?

Antwort:

Das Sicherheitsrisiko „Mensch" kann durch organisatorische Maßnahmen minimiert werden. Das "Restrisiko" muss vor allem durch Personalführung und Überwachung minimal gehalten werden. Wesentlicher Punkt der Personalführung in diesem Bereich ist

die Erzeugung einer Identifikation mit dem Unternehmen, die Motivation der Mitarbeiter und der sensible Umgang mit diesem spezialisierten Personal. Durch den weiteren Ausbau der DV-Organisation und der Sensibilisierung aller Beschäftigten gegenüber diesem Problemkreis soll dort das Bewusstsein weiter gestärkt werden.

Frage 4:

Auf Seite 9 steht „Ein angemessener Schutz des Betriebes eines Energieversorgungsnetzes wird vermutet, wenn der Katalog der Sicherheitsanforderungen eingehalten und dieses vom Betreiber dokumentiert worden ist". Auf den Seiten 11-17 wird über das „ISMS" System berichtet. Auf Seite 21 wird nach der „Zertifizierung" gefragt. Das klingt nach sehr viel Bürokratie.
Sind der „Katalog der Sicherheitsanforderungen", ein „ISMS System" bei den Stadtwerken eingeführt? Falls nein, ist es ein Ziel diese Systeme einzuführen, sowie eine „Zertifizierung" zu erreichen?

Antwort:

1. Rechtliche Vorgaben zum Schutz „kritischer Infrastrukturen"; Definition eines „Information Security Management System" (ISMS)

Die Stadtwerke Norderstedt und die wilhelm.tel GmbH gehören mit ihren wesentlichen satzungsgemäßen Aufgabenfeldern der Bereitstellung von sogenannten „technischen Basisinfrastrukturen" nach den Kriterien des Bundesministeriums des Innern – BMI – und des Bundesamtes für Sicherheit in der Informationstechnik – BSI – zu den Betreibern sogenannter „kritischer Infrastrukturen". Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Unternehmen, die kritische Infrastrukturen betreiben, haben zur Sicherstellung eines umfassenden Schutzes ihrer Versorgungssysteme IT-Sicherheitskonzepte als unternehmensspezifisches Regelwerk nach allgemeinen Standards zu erstellen und umzusetzen. Eine derartige Aufstellung von Verfahren und Regeln, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern, wird als Information Security Management System (ISMS) bezeichnet.

Zum Schutz kritischer Infrastrukturen gibt es für alle Unternehmen sektorübergreifende Vorschriften, die sich aus dem Aktien- und Datenschutzrecht ableiten lassen. Das Aktiengesetz fordert über den durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) eingeführten § 91 Abs. 2 AktG allgemein ein Risikomanagement, welches auch grundsätzlich die Unternehmens-IT umfasst. Im Vergleich dazu zwingt das Datenschutzrecht die Unternehmen sehr viel detaillierter zur Sicherung von IT-Infrastrukturen, in denen personenbezogene Daten verarbeitet werden.

Zur Konkretisierung gesetzlicher Vorgaben zum Schutz vor IT-spezifischen Risiken wird parallel ein kooperativer Ansatz der Zusammenarbeit von staatlichen Behörden und Institutionen und Betreibern kritischer Infrastrukturen mit dem Ziel der Verankerung von wirksamen Selbstverpflichtungen und, soweit dieser nicht ausreicht, die Optimierung durch neue oder geänderte Rechtsetzung verfolgt. Zur Erfüllung des gesetzgeberischen Ansatzes hat das Bundesministerium des Inneren – BMI – am 5. März 2013 einen Entwurf für ein IT-Sicherheitsgesetz vorgelegt und den Branchenverbänden Gelegenheit zur Stellungnahme gegeben. Ziel des Entwurfs ist u.a. die Erarbeitung und Einhaltung von brancheninternen Mindestniveaus für die IT-Sicherheit für Betreiber kritischer Infrastrukturen. Betreiber kritischer Infrastrukturen sollen demnach gesetzlich zu angemessenen organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind, verpflichtet werden.

2. Schutz von Kommunikationsinfrastrukturen

Die Telekommunikationsanbieter und –netzbetreiber haben zum Schutz des Fernmeldegeheimnisses und der personenbezogen Daten die auf Art. 1 i.V.m. 2, Art. 10 und Art. 87f Abs. 1 GG (Recht auf informationelle Selbstbestimmung, Fernmelde-geheimnis, Infrastrukturgewährleistungsauftrag) basierende Verpflichtung, die erforderlichen technischen Vorkehrungen und sonstige Maßnahmen zu treffen (§ 109 Abs. 1 S. 1 TKG). Zur Konkretisierung dieser Pflichten und zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, sowie zur Beherrschung der Risiken für die Sicherheit von Telekommunikations-netzen und –diensten (§ 109 Abs. 2 TKG), hat die BNetzA einen „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)“ aufgestellt. Dieser ist mit der Veröffentlichung im Amtsblatt Nr. 8 am 08.05.2013 in Kraft getreten.

3. Schutz von Energieversorgungsinfrastrukturen

Ferner hat die BNetzA nach § 11 Absatz 1a EnWG im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen, erstellt (IT-Sicherheitskatalog), der aktuell konsultiert wird. Der IT-Sicherheitskatalog soll Betreibern von Energieversorgungsnetzen unter anderem als Grundlage für die Implementierung eines Informationssicherheits-Managementsystems (ISMS) dienen.

4. Sektorenübergreifende IT-Sicherheitsstandards

Nach dem zur Erfüllung der Verpflichtungen nach § 109 TKG aufgestellten Sicherheitskatalog der BNetzA kann die Planung und Umsetzung der zu diesem Zweck erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen auch auf der Basis anderer geeigneter Standards, Normen u. ä. (z.B. BSI-Standards, BSI-Grundschutzkataloge, DIN ISO/IEC-Normen) erfolgen.

In der Einleitung zu ihrem Entwurf eines Sicherheitskataloges gemäß § 11 Absatz 1a EnWG – Version 1, Stand: 12.12.2013 – stellt die BNetzA fest, dass die Funktionsfähigkeit der Energieversorgung von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig sei. Dies gelte insbesondere für den Bereich der Netzsteuerung, der auf valide Netzzustandsdaten für einen sicheren Systembetrieb angewiesen sei. Der Schutz der IKT für die Betreiber von Energieversorgungsnetzen soll durch die Umsetzung der Anforderungen des vorgelegten IT-Sicherheitskataloges gewährleistet werden. Im Kern fordert die BNetzA auch hier die Einführung eines Informationssicherheits-Managementsystems gemäß DIN ISO/IEC 27001 inkl. Verweisen auf die Normen DIN ISO/IEC 27002 und DIN SPEC 27009 (sowie dessen Zertifizierung durch eine unabhängige dafür zugelassene Stelle).

Die Anforderungen des Sicherheitskataloges sind unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit sie die relevanten Systeme (teilweise) selbst betreiben. Auch hier haben die Netzbetreiber insbesondere den allgemein anerkannten „Stand der Technik" in Bezug auf die Absicherung der jeweils eingesetzten leittechnischen Systeme zu beachten, sowie die allgemeine IKT-Bedrohungslage und die spezifische Risikostruktur für die eingesetzten leittechnischen Systeme (Netzsteuerung) zu berücksichtigen. Die Netzsteuerungs-dienlichkeit gilt insofern als besonderes branchenspezifisch zu schützendes IT-System. „Netzsteuerung" im Sinne des Sicherheitskataloges ist die unmittelbare Einflussnahme auf die Fahrweise von Transport- und Verteilnetzen im Strom- und Gasbereich. Zu den dafür notwendig zu betreibenden Systemen zählen neben den Netzleit- und Netzführungsystemen auch dienende Komponenten wie z.B. Messeinrichtungen an Trafo- oder Netzkoppelstationen.

5. IT-Sicherheitsmanagement in der Unternehmensgruppe der Stadtwerke Norderstedt

Aus Sicht der Stadtwerke Norderstedt und der wilhelm.tel GmbH als Betreiber mehrerer kritischer Infrastrukturen (Energie-, Telekommunikations- und Wasserversorgung, Verkehr) ist aus den vorstehend skizzierten jeweiligen branchenspezifischen Vorgaben für die IT-Sicherheit und ein einzurichtendes ISMS ein gemeinsamer Standard abzuleiten. Dieser Standard muss, um die rechtlichen Vorgaben für den branchenübergreifenden gemeinsamen Einsatz zentraler Infrastrukturkomponenten für den Betrieb der IKT wie z.B.

Gebäude, Serverräume, Server (virtualisiert), Datenbanken etc. zu erfüllen, den „kleinsten gemeinsamen Nenner“ der speziellen Anforderungen abdecken. Hierfür empfiehlt sich die Orientierung an der ISO Norm 27001 und den BSI-Grundschutzkatalogen, zumal die nach § 21d EnWG einzusetzenden kundenseitigen elektronischen Messgeräte und Messsysteme („Smart Meter“) und deren Kommunikationseinheit („Smart Meter Gateway“) unabhängig von den Vorgaben des Sicherheitskataloges gem. § 11Abs. 1a EnWG durch die Vorgaben der BSI-Schutzprofile (BSI-CC-PP-0073/BSI-CC-PP-0077) und die zugehörige Technische Richtlinie (BSI TR-03109) geschützt sind.

Das ISMS-System nach der Norm DIN ISO 27001 ist ein Managementsystem, das in seiner Systematik an die 9000 Reihe angeglichen ist. Damit ähnelt es dem Energiemanagementsystem DIN ISO 50001, welches die Stadtwerke bereits eingeführt haben.

Die Werkleitung der Stadtwerke Norderstedt hat unabhängig vom gesetzgeberischen Status für das IT-Sicherheitsgesetz und im Rahmen dieses Verfahrens den Betreibern kritischer Infrastrukturen einzuräumender Umsetzungsfristen entschieden, frühzeitig ein ISMS einzuführen. Die Implementierung der entsprechenden IT-technischen, räumlichen und organisatorischen Komponenten bis hin zu einer Zertifizierbarkeit des ISMS wird einen Zeitraum von 1-3 Jahren beanspruchen. Ein ISMS-Zertifikat stellt ein notwendiges und entscheidendes Gütesiegel für die Dienstleistungsqualität von Betreibern kritischer Infrastrukturen dar.

Frage 5:

Sind derartige Konzepte zielführend, um einem kreativen, variantenreichen und sich stetig verändernden Hackerumfeld zu begegnen?
Inwieweit würden solche Konzepte helfen, dem Unsicherheitsfaktor „Mensch“ (siehe im oberen Teil) zu begegnen?

Antwort:

Ein ISMS senkt das Risikopotenzial derartiger Angriffe signifikant und unterliegt wiederum selbst auch einem ständigen Anpassungsprozess. Dadurch kann auch die Wirkung des Unsicherheitsfaktors "Mensch "reduziert werden.

Frage 6:

Bedeuten die Formulierungen auf Seite 20, dass das Sicherheitskonzept derzeitig lückenhaft ist? Es wurden „verschiedene Sicherheitsrichtlinien“ in „verschiedene Sicherheitskategorien“ eingeführt.

Antwort:

Nein, die Ausführungen des Datenschutzbeauftragten auf Folie 20 stellen im Gegenteil heraus, dass in der IT-Schutzorganisation der Unternehmensgruppe bereits Teilschritte auf

dem Weg zu einem ISMS umgesetzt worden sind. Dazu gehören die Analyse und Definition von sicherheitsrelevanten Parametern und deren Priorisierung (Sicherheitskategorien) und organisatorische Vorkehrungen zur Erhöhung der Datensicherheit (Sicherheitsrichtlinien). Auch räumliche Vorkehrungen (Unterbringung kritischer IT-Komponenten in den eigenen Rechenzentren) sind in hoher Qualität bereits getroffen worden.

Frage 7:

Der Vortrag schließt auf Seite 21 mit offen Fragen unter der Überschrift „Quo Vadis? – wo wollen die Stadtwerke hin?" ab.
Auch uns ist nach dem Vortrag bzw. Durchsicht der Unterlagen nicht klar was die nächsten (wesentlichen) Schritte sind?

Antwort:

Wie unter Frage 4. dargestellt, werden die Unternehmen im Bereich der Stadtwerke Norderstedt in einem Zeitraum von 1-3 Jahren die notwendigen Maßnahmen durchführen, um ein ISMS-Zertifikat erhalten zu können. Dafür wurde in der Stellenübersicht der wilhelm.tel GmbH für 2014 intern eine Stelle für „IT-Integration und Projektmanagement" eingerichtet und besetzt, auf welche die Verantwortung zur strategischen Konsolidierung der Softwaresysteme und die Steuerung von Realisierungsprojekten übertragen worden ist. Für entsprechende Projekte zur mittelfristigen Konsolidierung und Vernetzung der IT-Organisation der Stadtwerke und von wilhelm.tel – hier im ersten Schritt Software zur automatischen Provisionierung (Ablauforganisation) von technischen Prozessen sowie Kundenservice- und -managementprozesse –- sind im Jahr 2014 Investitionen von 0,6 Mio. € geplant (vgl. Wirtschaftsplan 2014 der Stadtwerke Norderstedt, Vorbericht). Im Bereich der Serverinfrastruktur wurde in den vergangenen zwei Jahren ein Projekt zur Storage-Erneuerung in Verbindung mit einer Servervirtualisierung realisiert. Weitere Schritte sind vor allem auch die Dokumentation und Verankerung der innerbetrieblichen Prozesse im Zusammenhang mit der Sicherheit kritischer IT-Systeme.

Norderstedt, den 25. Juni 2014

Werkleitung