Fraktion BÜNDNIS 90/DIE GRÜNEN -
Rathausallee 62 - 22846 Norderstedt

Werkleitung
Stadtwerke Norderstedt
Anfrage Stadtwerkeausschuss 14.05.2014

Fraktion der
Stadtvertretung Norderstedt
Rathausallee 62
22846 Norderstedt
Telefon 040 53595 507
Telefax 040/53595 517
E-Mail: fraktion@gruene-norderstedt.de
www.gruene-norderstedt.de

Norderstedt, 09.05.2014

Anfrage – Sicherheit der Steuerung der Stadtwerke für Strom/Gas/Wasser

In einem Artikel „Blackout“ aus der Zeitschrift „Die Zeit“ vom 10.04.14 (siehe Anlage 1) 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 16.09.13 wurde auf Anfrage von B 90/DIE GRÜNEN u.a. erläutert:

„Die Steuerung der Energie- und Wassernetze der Stadtwerke Norderstedt geschieht über ein Fernwirksystem, das 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 u. Systemsicherheit, Punkt 2 b)

1. Stimmt die Werkleitung vor dem Hintergrund des Artikels der Schlussfolgerung zu, dass externe Manipulationen 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 09.04.14 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. 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 ‚*verschiedenen Sicherheitskategorien*‘ eingeführt.

7. Der Vortrag schließt auf Seite 21 mit offenen 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.

Michael Ramcke
f. d. Fraktion B90/DIE GRÜNEN

Anlage: „Blackout“, Die Zeit vom 10.04.14

IT-SICHERHEIT:

Blackout

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigte: Die Stromnetze in Deutschland sind nicht sicher. von Christiane Grefe

DIE ZEIT Nº 16/201417. April 2014 08:37 Uhr 31 Kommentare

Es ist Zeit für einen Anruf. "Noch ein paar Klicks, dann ist es dunkel", sagt Felix Lindner. Wenn er jetzt seine Finger bewegt, geht in der süddeutschen Stadt Ettlingen das Licht aus. 40.000 Einwohner haben dann keinen Strom mehr. 200.000 Wasserpumpen könnten jetzt still stehen, weil der Hacker Felix Lindner sein Ziel erreicht hat.
Am anderen Ende der Leitung sitzt der Wächter über den Strom in Ettlingen, Eberhard Oehler. Der Geschäftsführer der Stadtwerke erschrickt, als er die tiefe Stimme hört. Hat der tatsächlich die Leitwarte, die Zentrale seiner Stadtwerke, geknackt? Oehler hält den Atem an. In seinem Kopf läuft ein Film mit schnellen Schnitten ab: tote Telefone und Computer,funktionsuntüchtige Mobilfunkmasten, Supermarktkassen, Benzinzapfsäulen, Fahrstühle, Kochherde, Radios. Ettlingens Altstadt mit dem markgräflichen Schloss liegt lahm in diesem Film.

Dann lässt der Schock nach. Oehler weiß ja: Dieser Hacker wird die Lichter in Ettlingen nicht ausschalten. Er hat ihn selbst engagiert für diesen Angriff auf sein Stadtwerk.
Und der Hacker Felix Lindner ist einer der bekanntesten Experten für IT-Sicherheit in Deutschland. Während seines Angriffs sitzt er nur wenige Hundert Meter entfernt von Oehlers Büro im Gästehaus der Stadtwerke am Rechner. Viel Zeit hat er nicht gebraucht, um ins vermeintlich abgesicherte Herzstück der städtischen Stromversorgung einzudringen. "Als er anrief, war meine Resthoffnung dahin, dass man das vielleicht doch nicht schafft", sagt der Geschäftsführer der Stadtwerke.

Mit dem gezielten Penetrationstest unter Livebedingungen, der erstmals öffentlich gemacht wird, wollten Oehler und "FX", wie sich Lindner auch nennt, nicht nur Schwachstellen im Ettlinger Versorgungssystem aufdecken. Sie machen auch auf eine bislang unterschätzte Entwicklung aufmerksam: Mit der Energiewende, die innovativ auf dezentrale und computergesteuerte Stromversorgung setzt, werden die Netze zugleich anfälliger für Cyber-Angriffe, weil mit den neuen Technologien auch die Zahl der Angriffspunkte wächst. Wie viele andere Systeme wird auch Deutschlands Infrastruktur – Strom, Wasser, Verkehr – umso verwundbarer, je mehr sie von digitalen Systemen abhängig ist.
Die wirtschaftlichen Folgen eines Ausfalls der Stromversorgung könnten dramatisch sein. In einer Metropole wie Berlin würde ein einstündiger Blackout zur Mittagszeit knapp 23 Millionen Euro kosten, schätzt das Hamburger Weltwirtschaftsinstitut.

Viel schwerwiegender als ein kurzer lokaler Ausfall wie in Ettlingen wäre ein gleichzeitiger Angriff auf mehrere miteinander verbundene Netze. Der Bestsellerautor Marc Elsberg hat vor zwei Jahren die Konsequenzen in seinem Roman *Blackout* drastisch ausgemalt: Nach einer listigen Cyber-Attacke durch Terroristen herrscht in seiner Geschichte zwischen Rom und Brüssel Chaos, weil Ampeln, Flugzeuge und Züge ausfallen, weil Nahrungsmittel und Medikamente ohne Kühlung knapp werden und Toilettenspülungen, Heizungen und Produktionsmaschinen tot sind. Der Dow-Jones-Index fällt im Sturzflug. Die Zivilisation steht auf der Kippe.
Stadtwerkechef Eberhard Oehler hat den Roman mit Spannung gelesen. Die technischen Details, die der Handlung zugrunde liegen, seien gut recherchiert, sagt er. Die Geschichte habe ihn wie viele Netzexperten und Katastrophenschützer beunruhigt.

Beim Lesen habe er bisweilen gedacht, "verdammt, das ist ja ein Fachbuch", sagt Oehler, auch wenn eine perfekt koordinierte Kettenreaktion, wie sie im Buch konstruiert wird, extrem unwahrscheinlich sei.
Oehlers Aufmerksamkeit für das Thema war geschärft, aber der Anstoß für den Realitätstest kam von außen. Die Hamburger Produktionsfirma filmtank fragte an, ob der Stadtwerkedirektor für eine Dokumentation über Netzkriege des Fernsehsenders Arte mit FX im Interesse von Sicherheit und Aufklärung zusammenarbeiten wolle. Nach einigem Nachdenken sagte er zu.

Welch ungleiches Paar: Zwar ist Oehler stets offen dafür, sich auf ungewöhnliches Terrain zu begeben. Das erkennt man am modernen Neubau der Stadtwerke ebenso wie daran, dass er seit Jahren nach Afghanistan reist, um beim Aufbau der Wasserversorgung zu helfen. Aber er sei doch "ein älteres Semester", sagt der 59-Jährige, und daher "erst mal nicht sehr IT-affin".

Auf der anderen Seite der Technik-Vorstand der Recurity Labs, deren Räume in einer Fabriketage in Berlin-Kreuzberg vom gleichen existenzialistischen Schwarz beherrscht werden wie des Hackers T-Shirt. Unaufhörlich hampelt FX, Mitte dreißig, auf seinem Stuhl herum, er beißt in diverse Schokoriegel, formuliert ironisch, provozierend. Dabei ist ihm die Sache ernst. Und offenbar reizt es den Kenner der "offensiven Seite der Computersicherheit", der große, auch internationale Unternehmen berät, auch nach Jahren, professionell in die Rolle eines *"agresseur du jour"* zu schlüpfen, wie er sagt. "Der wird in der Öffentlichkeit im Moment ja wohl am ehesten in einer russischen Hackertruppe gesehen."
"Ganz schön schräge Type", sagt Eberhard Oehler über FX. Aber nach einem ersten gemeinsamen Essen im noblen Wirtschaftstreff Berlin Capital Club verband die beiden rasch ein "sehr, sehr guter Draht". Das liegt vielleicht auch ein bisschen daran, dass Felix Lindner den Ettlinger Stromkunden rund 30.000 Euro Kosten erspart hat, die so ein Penetrationstest sonst kostet: "Dafür, dass die Stadtwerke im Film mitmachen, haben wir unsere Dienstleistung kostenlos erbracht", sagt der Hacker.
Ihn selbst habe an dem Filmprojekt interessiert, "mal ohne mystifizierende Strumpfmaske zu demonstrieren, wie wir Sicherheitsleute vorgehen und wie so ein Angriff funktionieren könnte".

Aber bringt er Bösewichte damit nicht erst auf miese Ideen? Denjenigen, die zu so etwas in der Lage seien, erzähle man da nichts Neues, winkt FX ab.

Wie also konnte er die digitalen Schutzmauern in Ettlingen durchdringen? Gleich auf zwei Wegen. Nachdem Oehler den Hacker mit dem Auftrag betraut hatte, schickte FX eine E-Mail an einen Stadtwerkemitarbeiter – mit einer Schadsoftware im Anhang.
Die müsse der Empfänger nur öffnen, und schon, sagt FX, habe er Zugang zu einem Rechner, der sein Brückenkopf ins interne Netz der Firma sei. Über den könne sich ein Angreifer dann in aller Ruhe im System umschauen.
Verlässlicher sei Weg Nummer zwei, sagt Lindner: direkt über die Hardware, indem der Angreifer sich physischen Zugang zu Netz und Rechner verschaffe. Kriminelle oder womöglich nationalstaatliche "Angreifer" bedienten sich dazu meist einer "Spezialistentruppe für Einbrüche", sagt Lindner. Er selbst fand einen bequemeren Zugang, als "über die Zäune zu hüpfen". Im Gästehaus der Stadtwerke konnte er ein Modul an eine Netzwerkdose anschließen, über die es eine Verbindung ins Stadtwerkenetz gab. Anschließend konnte er mit ein paar Hilfsgeräten vom eigenen Laptop aus Kontakt aufnehmen.

In diesem Stadium, sagt FX, fühle man sich in der fremden Netzumgebung ähnlich wie ein Dieb in einem Bürogebäude: "Der muss auch erst mal an allen Türen rütteln, um zu gucken, was es wo zu holen gibt." Sein Team durchforstete Datensätze daraufhin, ob sie eine Verbindung zur Leitwarte weisen könnten. Dass sie eine Menge Hinweise gefunden hätten, demonstriere eine Unzulänglichkeit, von der laut FX die meisten IT-Systeme geprägt seien: Alle internen Zugriffe gälten als vertrauenswürdig, nur die von außen als bedrohlich, frei nach einer amerikanischen Süßigkeiten-Werbung: "Außen knusprig,
innen weich".

Nachdem der Hacker erste Wegweiser zur Leitwarte gefunden hatte, half ihm auch noch der Zufall weiter, ein ziemlich verbreiteter freilich: die menschliche Unzulänglichkeit überlasteter Mitarbeiter in der IT-Abteilung. Die Leitwarte ist zwar mit einem eigenen, getrennten Netzwerk vor Zugriffen geschützt. "Auch das muss allerdings gepflegt und gewartet werden", sagt der Hacker. Um "ihren Job zu machen", hätten die IT-Experten die Schaltzentrale für den Transport von Updates und Back-ups dann doch mal ans Hausnetz angeschlossen, "und diesen Weg haben wir zurückverfolgt". Er führte die Hacker zu bestimmten Nutzern, die solche Dienste häufig anboten und über hohe Zugangsprivilegien verfügten. Diese mussten eine zentrale Funktion haben, schlussfolgerte das Hacker-Team.
Eine Adressliste mit Namen und Aufgaben der Mitarbeiter hatten die Hacker unterwegs schon "eingesammelt". Nun blieben nur mehr begrenzte Möglichkeiten, auf welchem Rechner ein Paket der Leitstellen-Software deponiert sein könnte, um sie bei einem möglichen technischen Ausfall rekonstruieren zu können. Die Einbrecher wussten, an welchen Türen es sich lohnen würde, zu rütteln.
Fehlte noch das Passwort. FX fand "mit der von Berufs wegen antrainierten Fähigkeit, auch in einem unbekannten Binärformat Muster zu erkennen", gleich mehrere heraus. Als er damit Zugang zur Leitstelle bekam und das System ihm anbot, die Kontrolle zu übernehmen, war die Schwelle erreicht, die er mit den Mitarbeitern der Stadtwerke vertrauensvoll verabredet hatte.
FX griff zum Hörer: "Noch ein paar Klicks ..."
"Unsere IT-Dienstleister erschraken noch mehr als wir selbst", erzählt Eberhard Oehler. Die Firma hat schließlich nicht nur die Stadtwerke Ettlingen zum Kunden. Nach dem Testangriff habe sie sich, froh über die Hinweise, schleunigst darangemacht, die erkannten Schwachstellen im System zu beheben.

Auch die Stadtwerke-Leitung zog Konsequenzen. Es gab neue Dienstanweisungen, etwa: Den Computer vor dem Nachhausegehen herunterfahren, und Bürotüren abends abschließen. Alle nicht notwendigen Verbindungen zum internen Netzwerk wurden gekappt. Es fand sich sogar eine zu einem Gäste-PC.
Außerdem hat Eberhard Oehler seine IT-Abteilung personell aufgestockt. "Energieversorger denken noch immer nicht in den Kategorien der elektronischen Steuerung", sagt FX. "Deshalb sind diese Abteilungen häufig unterschätzt und unterbesetzt." In seinen Augen bezahlen Unternehmen zu oft viel Geld für eine weitere "magische" Sicherheitsanwendung, statt "die gleiche Summe für die leistungsfähigste adaptive Muster- und Anomalie-Erkennung auszugeben, die bisher bekannt ist: den Menschen". Echte Menschen, die Auffälligkeiten erkennen und beheben.
Der Angriff auf Ettlingen hat auch Ermutigendes zutage gefördert. Es sei zwar möglich, in das Stadtwerkenetz einzudringen und es zu kontrollieren, aber "die Kontrolle zu behalten eher nicht", so der Hacker. Angesichts der vielen mechanischen Anzeigen und Schutzelemente herkömmlicher Stromnetze wie dem von Ettlingen fallen Unregelmäßigkeiten rasch auf, "und notfalls springt eben ein Mann im Blaumann ins Auto und legt einen Schalter um".
Hätte FX tatsächlich einen Störfall ausgelöst, dann wäre in wenigen Sekunden ein Notaggregat für die Wasserpumpen angesprungen. Auch die Stromversorgung hätte man in Minuten, spätestens einer Stunde wieder hochgefahren, sagt Oehler.

Die Energiewende wird Ettlingen wie das ganze deutsche Stromnetz aber verwundbarer machen für Cyber-Angriffe. Die größten Sorgen machen Oehler und Lindner dabei sogenannte Smart Meter, die kleinere Erzeuger erneuerbarer Energien künftig nutzen müssen. Diese elektronischen Stromzähler lassen sich von außen über Computer ansteuern. Wenn die Smart Meter auch zur Regelung und Steuerung eingesetzt werden, dann haben ausgefuchste Hacker womöglich viele Tausend neue Zugänge zum Netz und seinen Schaltstellen, um die Stromversorgung aus dem Gleichgewicht zu bringen. Im Roman *Blackout* manipulieren die Verschwörer genau diese Geräte.
Dazu kommt, dass immer mehr Informationstechnologie erforderlich ist, um die Einspeisung schwankender Angebotsmengen von Wind- und Sonnenstrom mit dem Bedarf zu koordinieren. Der Aufbau solcher intelligenten Netze kann die Energiewende effizienter und kostengünstiger machen, weil dann weniger Stromleitungen gebaut werden müssen. Das ist ein großer Vorteil.

Doch auch dabei vervielfacht sich die Zahl der Vorder- und Hintertüren für böswillige Hacker.

Die Bundesnetzagentur und das Bundesamt für Sicherheit in der Informationstechnik haben bereits einen Sicherheitskatalog erstellt. Er sieht unter anderem vor, dass Infrastrukturunternehmen einen eigenen Beauftragten für IT-Sicherheit einstellen müssen. Eine Meldepflicht für Schadensfälle wird erwogen, damit auch andere die Ursachen, die man identifiziert hat, beheben können. Darüber hinaus legt die EU-Kommission eine Richtlinie mit Vorschlägen zur Cyber-Sicherheit vor. Das Thema wird im Verband der kommunalen Unternehmen und vielen Fachgremien diskutiert.
Ob das ausreicht? Kurt Rohrig, der am Fraunhofer IWES in Kassel seit vielen Jahren intelligente Energiesysteme erforscht, ist
zwar davon überzeugt, dass man die Smart Meter gegenüber Hacker-Angriffen absichern kann. Aber auch er sieht die Gefahr, dass "bei einem allzu rasanten Ausbau intelligenter Netze die Entwicklung der Sicherheitssysteme nicht parallel verläuft".
Nicht nur für die Politik, auch für die Energieindustrie ist die Herausforderung groß, vor allem weil sie einen regelrechten Kulturbruch bedeutet: Bei Infrastruktur-Investitionen rechnen die Konzerne in Jahrzehnten, doch in der Informationstechnologie vollziehen sich umwälzende Entwicklungen oftmals binnen Monaten.
Auch deshalb warnt der Hacker Felix Lindner davor, sich durch penible Vorschriften zu sehr in Sicherheit zu wiegen. Sein Rat klingt aus dem Munde eines Netzprofis erst mal erstaunlich. Man solle bei aller Vernetzungsbegeisterung auch darüber nachdenken, wo sie überflüssig sei und wo man entflechten könne: "Getrennt halten, was geht."