Botschafterkonferenz im Auswärtigen Amt, Berlin

30. August 2011

Impulsvortrag von Peter Hellmonds, Nokia Siemens Networks

Thema:	Verfügbarkeit und Sicherheit mit IKT
Ort und Zeit:	Workshop 8, Raum 3-015, 14:30h
Teilnehmer:	Botschafter Ammon (Washington, DC) – Cyber-Sicherheitsrat
	Botschafter Bock (Kairo) – Arabische Revolutionen
	H. Hellmonds (NSN) – Innovative Technologien aus Deutschland
	H. Sterzinger (G&D) – Sicherheit
	H. Panev (Siemens) – eGovernment
	H. Rüdiger (Bundesdruckerei) – dt. Personalausweis

Sehr geehrte Exzellenzen, Herr Botschafter Ammon, Herr Botschafter Bock, sehr verehrte Damen und Herren, lieber Herr Brommer,

Vielen Dank für die Einladung, in diesem Rahmen heute zum Thema der Verfügbarkeit und Sicherheit der IKT Netze im internationalen Rahmen mit Ihnen diskutieren zu dürfen.

Bitte erlauben Sie mir, mit ein paar Worten kurz unser Unternehmen vorzustellen, denn Details über unser Unternehmen sind in der Regel nicht jedem so präsent.

Wir sind vor 4 ½ Jahren im April 2007 als Gemeinschaftsunternehmen von Nokia und Siemens gegründet worden und vereinbaren die Netzwerkaktiviäten, die vorher bei Nokia Networks und bei Siemens Communications angesiedelt waren. Wir stützen uns also auf die über 160jährige Tradition von Siemens und Nokia in diesem Bereich. Wir sind nach der kürzlich erfolgten Übernahme der Motorola Netzwerksparte mittlerweile ein Unternehmen von über 72,000 Mitarbeitern, verteilt auf Standorte in über 100 Ländern. Unsere ca 600 Kunden sind die großen und kleinen Telekommunikationsfirmen dieser Welt, verteilt auf über 150 Länder. Nicht weniger als 75 der Top-100 Telekom Firmen dieser Welt sind unsere Kunden. Wir sind also ein großes internationales Unternehmen der Telekommunikationsbranche, vergleichbar mit Ericsson aus Schweden, Alcatel-Lucent aus Frankreich und Huawei aus China. Dies sind unsere drei stärksten Mitbewerber in diesem heiß umkämpften Markt.

Aber wir sind nicht nur ein internationales, sondern auch ein sehr deutsch geprägtes Unternehmen. Nicht nur, dass wir mehr deutsche Vorstände unseres Unternehmens als finnische haben, sondern wir sind auch mit etwa 10,000 Mitarbeitern am Standort Deutschland präsent, die hier forschen und designen, produzieren und instandhalten, und Produkte aus Deutschland in über 100 Exportmärkte weltweit verkaufen.

Hier in Berlin beispielsweise haben wir eine Fabrik, in der hochperformante Netzwerkkomponenten für optische Netze gebaut werden. Dies ist High-Tech vom Feinsten - made in Germany. Optische Netze, das sind die Schnellbahnen im Netz. Diese werden gebraucht, um die immensen Datenströme in Echtzeit über kurze und natürlich auch über lange Wege schnell zu transportieren – mit Lichtgeschwindigkeit!

Seit jeder einen Laptop und ein Smart Phone hat und sich streaming Videos von YouTube und Filme via Netflix ansieht, ist die Datenmenge um ein Vielfaches gestiegen. Gleichzeitig sollen natürlich über die Netze auch noch Telefonate geführt werden, ohne dass man mit Unterbrechungen und Störungen zu rechnen hat. Die Anforderungen an die Netze sind also gewaltig. Und die Technologie, die das möglich macht, kommt hier aus Berlin. Aus Siemensstadt.

Wir haben dies im letzten Jahr auch dem Staatssekretär Fritsche aus dem Innenministerium gezeigt und ich lade Sie gerne ein, einmal unser Werk in Berlin zu besuchen, um sich selbst einen Eindruck davon machen zu können.

(Ok, nicht alle gleichzeitig und nicht jeden Tag einer, denn wir wollen ja auch noch etwas arbeiten.)

Aber, warum erwähne ich das. Es geht eben genau um die Verfügbarkeit und um die Sicherheit unserer IKT Infrastruktur. Und Herr Botschafter Ammon hat ja bereits geschildert, mit welchen Themen sich der Cyber-Sicherheitsrat der Bundesregierung befassen darf. Denn die IKT Netze werden ja auch zunehmend die Kommunikations-Grundlage für andere Infrastrukturen. Und somit steigen auch unsere Anforderungen an die Verfügbarkeit und die Sicherheit der Netze. Denn sie werden Bestandteil der sogenannten kritischen Infrastrukturen, ähnlich wie Energie, Wasser, Gasversorgung oder die Verkehrsinfrastruktur.

Ein Beispiel: Wir wollen ja beispielsweise den Umbau unserer Energieversorgung hin zu einer grünen Energie. Dieser Umbau weg von Kohle- und Atomenergie und hin zu erneuerbaren Energiequellen ist sicher sinnvoll und auch politisch gewollt und von breitem sozialem Konsens getragen. Der Umbau der Netze von einem einfachen Verteilnetz hin zu einem intelligenten Smart Grid jedoch erfordert eine umfangreiche IKT Unterstützung. Also, wer A sagt, sollte auch ja zu B sagen. Wenn wir den Umbau der Energieversorgung wollen, dann brauchen wir Smarte Grids, und die brauchen die IKT Netze.

Genauso brauchen wir die IKT Netze, um insgesamt weniger CO_2 zu produzieren. IKT Netze erlauben uns beispielsweise, statt eine Dienstreise zu unternehmen, an einer Telefonkonferenz oder einer Videokonferenz teilzunehmen. Nicht nur spart das Zeit und Kosten und schont unsere Umwelt, es trägt auch zu einer besseren Work-Life-Balance bei, wenn ich nicht jeden Tag ins Büro fahren muss, sondern meine e-Mails bequem im Garten meines Hauses beantworten kann, nachdem ich mein Kind ins Bett gebracht habe.

Jedenfalls müssen wir uns Gedanken machen nicht nur über die technische Verfügbarkeit der Netze, sondern auch über die Sicherheit. Und hier sind wir aktiv in einer Forschungsinitiative, genannt Asmonia, das steht kurz für die Entwicklung einer Angriffsanalyse und von Schutzkonzepten für Mobilfunk-basierte Netzinfrastrukturen – unterstützt durch kooperativen Informationsaustausch. In diesem vom BMBF geförderten Projekt forschen wir gemeinsam mit anderen daran, wie wir die Netze sicherer machen können, denn die Gefährdung ist heute größer denn je.

Ein Beispiel: Stuxnet hat deutlich gemacht, dass die Bedrohung für unsere Infrastrukturen längst nicht mehr vom Hobby-Hacker ausgeht, der mal eben in seiner Freizeit neben dem Studium einen Trojaner bastelt. Stuxnet war ein vermutlich staatlich geförderter, groß angelegter Versuch, mittels eines kompliziert programmierten Trojaners ein ganz bestimmtes Ziel auszuschalten. Man geht davon aus, dass dieses Projekt Stuxnet mehre Millionen gekostet hat.

Ein anderes Beispiel sind Botnetze, die in der Lage sind, durch distributed Denial-of-Service Attacken die Zielrechner und Server lahmzulegen. Wir sehen hier in der letzten Zeit zunehmende "Professionalisierung" der Cyber-Crime Industrie. Man kann auf dem Markt für diese Art von Malware mittlerweile alles kaufen oder in Auftrag geben. Eine richtige Cyber-Mafia hat sich hier entwickelt, mit Umsätzen in Millionen oder Milliardenhöhe. Kreditkarten-Daten, Bankdaten, oder eine DDOS Attacke – alles ist käuflich. Und die Auftraggeber sind auch manchmal Unternehmen oder Geheimdienste anderer Staaten.

Unsere Forschung nach Backdoors (also Hintertürchen, Schlupflöchern) hat ergeben, dass es nahezu unmöglich ist, solche nachträglich in dem Code von Routern oder Switchen oder anderen Infrastrukturkomponenten zu finden. Wir versuchen zwar, entsprechende heuristische Verfahren zu entwicklen, mittels derer man die Stellen identifizieren kann, wo Schadcode sich verstecken könnte, aber wenn man sich z.B. den Stuxnet Code ansieht, erkennt man, dass man da, wo in Maschinensprache programmiert wird, nur mit unverhältnismäßigem Aufwand hinter die Geheimnisse kommen kann.

Insofern ist umso wichtiger, dass man ein Vertrauen darin hat, wie die Netze aufgebaut sind, wie die Software programmiert ist, von wem das Equipment kommt, wer es betreibt. Daher möchte ich also gerne die Einladung erneuern: schauen Sie sich einmal unser Werk in Berlin an, wo die hochperformanten Netzkomponenten gefertigt werden, die an den Schaltstellen unserer kritischen Infrastrukturen wirken.

Meine sehr geehrten Damen und Herren, Exzellenzen, ich danke Ihnen für Ihre Aufmerksamkeit.