13. August 2013

Peer Steinbrück und Kompetenzteam

Schutz für den Hochtechnologie-Standort Deutschland
6 Punkte-Aktionsplan gegen Wirtschaftsspionage

Der NSA-Skandal macht deutlich: Deutschland befindet sich im Fadenkreuz internationaler Spionage. Die neuen technologischen Ressourcen der Digitalisierung ermöglichen das Abschöpfen, Speichern und Verwerten von Daten aus Deutschland in einer nie dagewesenen Dimension. Private Emails und geheime Regierungsdokumente sind dabei genauso verwundbar wie Betriebsgeheimnisse. Fast alle Experten gehen davon aus, dass Wirtschaftsspionage hier eine große Rolle spielt, zumal die NSA mit einem unübersehbaren Geflecht von Privatfirmen kooperiert. Für den britischen Geheimdienst mit seinem gigantischen Datenerfassungsprogramm „Tempora“ zählt die „Sicherstellung des wirtschaftlichen Wohlergehens“ Großbritanniens sogar explizit zu den Aufgaben. Über welche Kapazitäten und Ziele die Dienste anderer Mächte wie China und Russland verfügen, kann nur spekuliert werden.

Für die deutsche Wirtschaft bedeutet diese Entwicklung eine massive Bedrohung. Denn wie kaum eine andere Wirtschaftsnation hängt unsere Wettbewerbsfähigkeit von dem technologischen Vorsprung ab, den sich viele deutsche Unternehmen gegenüber internationalen Wettbewerbern erworben haben. Forschung und Entwicklung sind für Deutschland als Hochtechnologie-Standort das entscheidende Kapital, um auch weiterhin erfolgreich auf den Weltmärkten zu agieren. Besonders Branchen wie Luft- und Raumfahrttechnik, Automobilindustrie oder Maschinenbau bangen um ihren Wissensvorsprung. Über Jahre hinweg teuer erworbene Entwicklungsvorsprünge gehen über Nacht verloren und können einzelne Unternehmen in ihrer ganzen Existenz gefährden.

2012 machten Hackerangriffe bereits rund 42% der Wirtschaftsspionage in Deutschland aus. Der Schaden der durch Wirtschaftsspionage jährlich in Deutschland entsteht, ist immens. Schätzungen gehen von bis zu 50 Milliarden Euro

jährlich aus. Am stärksten betroffen von dieser Bedrohung ist der deutsche Mittelstand: Viele kleine und mittlere Unternehmen verfügen nicht über die Ressourcen der Großkonzerne, um sich gegen die digitale Wirtschaftsspionage zu schützen. Hier hat höchstens jedes vierte Unternehmen bislang eine IT-Sicherheits-Strategie. Doch gerade der Mittelstand mit seinen vielen „hidden champions“ und hochspezialisierten Weltmarktführern steht besonders im Fokus der Ausspähung. Gerade Mittelständler sind darauf angewiesen, dass wie in allen sicherheitsrelevanten Bereichen der Staat seine Schutzpflicht wahrnimmt.

Schwarz-Gelb hat diese Pflicht in den letzten vier Jahren ignoriert. Obwohl Verfassungsschutz und Wirtschaftsverbände nachdrücklich vor der digitalen Wirtschaftsspionage warnen, ist die Bilanz der Regierung Merkel armselig. Im Koalitionsvertrag hatte Schwarz-Gelb noch versprochen: *„Wir werden die IT gegen innere und äußere Gefahren schützen, um die wirtschaftliche Leistungsfähigkeit und administrative Handlungsfähigkeit zu erhalten. Daher werden wir ein besonderes Augenmerk auf die Abwehr von IT-Angriffen richten.“*

Stattdessen regiert der Stillstand. Das vollmundig angekündigte Nationale Cyber-Abwehrzentrum verfügt über lediglich 10 Mitarbeiter, während vermutlich Zehntausende Geheimdienstler allein für die amerikanische NSA tätig sind. Das zentrale Vorhaben, das IT-Sicherheitsgesetz, das Frau Merkel bei der CeBIT versprochen hatte, ist über den Stand eines Referentenentwurfes nicht hinausgekommen, da sich die Koalition auch hier nicht einigen konnte. Nach wie vor existieren Doppelstrukturen und Kompetenz-Wirrwarr bei den zuständigen Behörden. Diese Bundesregierung gefährdet durch ihr Nichtstun die Substanz des Standorts Deutschland. Das werden wir ändern.

Mit mir als Bundeskanzler wird die Regierung das Thema Cyber-Sicherheit zur Chefsache machen:

Aktionsplan gegen Wirtschafts-Spionage

1. **Einführung von verpflichtenden, kostengünstig angebotenen IT-Sicherheitsmindeststandards:** Das Bundesamt für Sicherheit in der

Informationstechnik muss seine Standards zum IT-Grundschutz weiterentwickeln. Die Sicherheitsmindeststandards sollen für Institutionen mit niedriger, mittlerer und hoher Gefährdungslage abgestuft sein. Ab einer bestimmten Betriebsgröße werden Unternehmen verpflichtet, einen Mindeststandard an IT-Sicherheit zu erfüllen. Denn: Häufig werden Unternehmen angegriffen, um von dort aus IT-Angriffe auf Dritte zu starten. Deshalb sollen diese mindestens den Sicherheitsstandard der niedrigsten Stufe verpflichtend umsetzen. Daraus darf jedoch kein Wettbewerbsnachteil erwachsen. Gerade kleine und mittlere Unternehmen scheuen aufgrund der hohen Kosten häufig aufwändige IT-Sicherheitskonzepte. Als Voraussetzung für die verpflichtende Einführung der Sicherheitsstandards muss das Bundesamt für Sicherheit in der Informationstechnik daher Grundschutzkonzepte gemeinsam mit der deutschen Spitzenforschung und Unternehmen im Bereich IT-Sicherheit entwickeln und diese für KMUs kostengünstig zur Verfügung stellen.

2. **Aufstockung der Personal- und Sachmittel für Cyber-Sicherheit:** Eine effektive Cyber-Sicherheitsstrategie braucht eine entsprechende finanzielle Unterfütterung. Schwarz-Gelb hat auch bei diesem Thema Etikettenschwindel betrieben. Im 2011 neu geschaffenen Cyber-Abwehrzentrum (CAZ) arbeiten nur 10 Leute. Mittelfristig wollen wir die Mitarbeiterzahl auf über 100 Mitarbeiter erhöhen. Außerdem wird der Etat des Bundesamts für Sicherheit in der Informationstechnik in der nächsten Legislaturperiode von momentan 88 Millionen Euro auf mindestens 150 Millionen Euro erhöht, um die neuen Herausforderungen effektiv bewältigen zu können. Um klare Zuständigkeiten zu schaffen, werden wir eine Kommission einsetzen, die eine Bestandsaufnahme der bestehenden staatlichen wie privaten Initiativen, existierender Gesetze und Organisationen im Bereich Cyber-Sicherheit vornimmt. Sie hat die Aufgabe, Vorschläge zur Bündelung von Kompetenzen und Zuständigkeiten auszuarbeiten.

3. **Einführung des Marktortprinzips:** Die USA und Europa haben unterschiedliche Rechtstraditionen und Wertvorstellungen. Als Bundeskanzler werde ich mich deshalb dafür einsetzen, dass das sogenannte Marktortprinzip auch und gerade für Internetunternehmen gilt und auf europäischer Ebene durchgesetzt wird. Nach

diesem Prinzip müssen sich Unternehmen, die ihren Hauptsitz nicht in Deutschland oder der EU haben, an deutsches bzw. europäisches Recht halten, wenn sie ihre Dienste in Deutschland anbieten. Damit gelten deutsche Datenschutzrichtlinien und Grundsätze der IT-Sicherheit. Gleichzeitig treten Unternehmen auf diese Weise unter gleichen Bedingungen in den Wettbewerb des Marktes ein, so dass die hohen Standards für deutsche Unternehmen nicht zum Wettbewerbsnachteil werden.

4. **Qualifizierungsoffensive „IT-Sicherheit“**: Die zunehmende Bedeutung der IT-Sicherheit erfordert gut ausgebildete Fachkräfte. Sowohl staatliche Stellen als auch die Wirtschaft werden in den kommenden Jahren mehr Personal in der IT-Sicherheit benötigen. Momentan herrschen große Engpässe in diesem Bereich. Wir wollen daher Schulen, Universitäten, Arbeitgeber und Verbände an einen Tisch bringen, um eine Qualifizierungsoffensive „IT-Sicherheit“ zu starten. Darüber hinaus wollen wir Unternehmen für IT Sicherheit sensibilisieren. Das Bundesamt für Sicherheit in der Informationstechnik soll gemeinsam mit dem Bundesamt und den Landesämtern für Verfassungsschutz ein Trainingsprogramm Cyber-Sicherheit für Unternehmen, insbesondere für KMUs, entwickeln und anbieten. Schwerpunkt soll die Sensibilisierung der Unternehmen für das Thema „Innentäter“ bilden. Denn die meisten digitalen Angriffe sind nur erfolgreich, weil Mitarbeiter des betroffenen Unternehmens, teils unwissentlich über Social Engineering, mit dem Angreifer kooperieren.

5. **Stärkung der deutschen Spitzenforschung zum Thema „Cyber-Sicherheit“:** Als forschungsstarker Standort hat Deutschland die Chance, Spitzenreiter bei IT-Sicherheitslösungen zu werden. Einige der weltweit führenden Verschlüsselungstechnologien werden bereits jetzt in Deutschland entwickelt. Deswegen wollen wir die anwendungsorientierte Forschung und die Umsetzung von Forschungsergebnissen in marktreife Produkte fördern. Wir wollen gemeinsam mit der Forschung nachhaltige Prinzipien entwickeln. Im Zeitraum bis 2020 sollen durch Haushaltsaufstockung insgesamt 250 Millionen Euro für Vorhaben in der Cyber-Sicherheit zur Verfügung gestellt werden. Unser Ziel ist ein Deutsches Gütesiegel zur Cyber-Sicherheit.

6. **Innovationsstrategie zu Datenschutz und IT-Sicherheit „Made in Germany“:** Gemeinsam mit deutschen IT-Unternehmen und Forschungseinrichtungen wollen wir eine Innovationsstrategie entwickeln, die die Themen IT-Sicherheit und Datenschutz ins Zentrum stellt. Ein Gütesiegel zur IT-Sicherheit und zur Wahrung hoher Datenschutzstandards, nutzerfreundliche Lösungen für die Ende-zu-Ende Verschlüsselung der digitalen Kommunikation und Paketlösungen von Hardware und Software zu Sicherheit und Datenschutz für Verbraucher und Unternehmen können zu einem Exportgut der deutschen Spitzentechnologien werden. Dafür starten wir eine gemeinsame Initiative, die die Bedarfe, Rahmenbedingungen und technologischen Möglichkeiten zusammenbringt.