SILICON SAXONY
MY FAVORITE PLACE

PRESSEINFORMATION

Politik / Sicherheit / Technologie / Gesellschaft

Cybersicherheit ist zentrale Herausforderung für eine vernetzte Gesellschaft

- **Gemeinsame Aufgabe von Staat und Wirtschaft: Schutz von lebenswichtigen, öffentlichen Datennetzen gegen Cyberattacken**
- **Rasanter Anstieg von Cyberattacken gegen deutschen Mittelstand und Betreiber von „kritischen Infrastrukturen“ in Deutschland**
- **Sächsische Chip- und Softwarebranche liefert technologischen Beitrag für die Sicherheit von lebenswichtigen Datennetzen**

Dresden, 2. Mai 2013. Europas größter und wichtigster Chipstandort Silicon Saxony arbeitet an Technologien für eine sichere IT-Infrastruktur. Auf einer Fachveranstaltung, die heute in Dresden stattfindet, diskutierten Experten aus Industrie und Politik über Bedrohungsszenarien so genannter "Kritischer Infrastrukturen"* durch Hackerangriffe. Deutschlands Institutionen und ihre lebenswichtigen Datennetze sind zunehmend vernetzt – das macht sie für Cyberattacken anfällig und zu potentiellen Zielen: Transportwesen, Energie- und Wasserversorgung sowie der Eisenbahn- und Flugverkehr bilden potentielle Angriffsziele. Aber auch Banken und Krankenhäuser sowie Telekommunikations- und Medienunternehmen kommen infrage.

„Cyberattacken gehören neben dem internationalen Terrorismus, schweren Unfällen, Epidemien oder internationalen Konflikten zu den vier am höchsten eingestuften Bedrohungs-Kategorien", betonte Bundesinnenminister Dr. Hans-Peter Friedrich bei der Cyber-Fachveranstaltung im Dresdner Coselpalais. Weiter erklärte der Bundesminister: "Zusammen mit den Partnern aus der Wirtschaft muss die Verfügbarkeit widerstandsfähiger Cyber-Strukturen unbedingt sichergestellt werden. Darauf müssen wir unser sicherheitspolitisches Handeln konzentrieren. Deutschland hat seine Hausaufgaben gemacht. Mit der Nationalen Cybersicherheitsstrategie haben wir unsere Prioritäten auch nach außen hin verdeutlicht. Noch in dieser Legislaturperiode werden wir dem Kabinett einen Gesetzentwurf zum Schutz der IT-Sicherheit vorlegen."

Drastischer Anstieg: 42 Prozent mehr Attacken als noch im Vorjahr
Experten verzeichnen eine Zunahme solcher Aktivitäten: "Die Cyber-Spionage gegen kleine und mittelgroße Firmen nimmt weiter drastisch zu. So nahmen im Jahr 2012 im Vergleich zum Vorjahr gezielte Spionageangriffe um satte 42 Prozent zu. Die Angreifer richten sich in erster Linie gegen das produzierende Gewerbe sowie kleine und mittelständische Unternehmen (KMU) und wollen vor allem geistiges Eigentum stehlen", sagt Frank Giessen, Leiter Öffentliche Auftraggeber beim IT-Sicherheitsunternehmen Symantec. Das Softwareunternehmen veröffentlicht jährlich den „Internet Security Threat Report“. Dieser liefert eine Analyse der weltweiten Bedrohungsaktivitäten des vergangenen Jahres.

Aus Sicht des Branchennetzwerkes Silicon Saxony gibt es bei dem Thema "Cybersicherheit" mehrere Handlungsfelder: Für Investoren und Unternehmen sind zuverlässige öffentliche Infrastrukturen enorm wichtig, insbesondere bei hohen Investitionen. Eine weitere Rolle spielt der Schutz von geistigem Eigentum – in einer Hochtechnologieregion wie dem Silicon Saxony ein wichtiger Punkt. Zusätzlich sind viele der hier beheimateten Firmen und Forschungsinstitutionen direkt betroffen, da sie sich als Mittelständler und Zulieferer besonders im Visier von Cyberkriminellen befinden.

Sachsens Innenminister Markus Ulbig betont: „Cybersicherheit ist der Standortfaktor der Zukunft! Der Staat muss auch im virtuellen Raum für Sicherheit sorgen. Im sächsischen Innenministerium haben wir dafür im Oktober 2012 den Arbeitskreis Cybersicherheit ins Leben gerufen. Im offenen Dialog mit der Industrie wollen wir dort vernetzte Lösungen für eine vernetzte Welt finden. Ziel ist, insbesondere den Kommunen als Rückgrat für ein digitales Sachsen technische und organisatorische Unterstützung zu geben. Im Mittelpunkt steht dabei der Schutz der kritischen Infrastruktur: Nicht auszudenken, wenn Angreifer bspw. die Strom- oder Wasserversorgung von Großstädten lahmlegen oder Verkehrsleitsysteme übernehmen. Auf solche Szenarien müssen wir vorbereitet sein."

Silicon Saxony: Kompetenznetzwerk für sichere Chiparchitekturen
Die europäische Mikro- und Nanoelektronikbranche im Silicon Saxony forscht bereits an sicheren Chiplösungen, ohne die eine verlässliche IT-Infrastruktur nicht funktionieren würde, insbesondere im Bereich des Designs von Chips. „Sie bilden die Basis für alle elektronischen Dienste. Bei der Mikro- und Nanoelektronik handelt es sich damit um die wichtigste und grundlegendste Schlüsseltechnologie in der heute vernetzten Welt", sagt Heinz Martin Esser, Präsident des Hightech-Branchennetzwerkes Silicon Saxony e.V. "Eine sichere Chiparchitektur ist die Basis für eine sichere IT. Die „höchsten" Firewalls und abgeschirmtesten Firmennetzwerke nützen nichts, wenn die Hardware nicht sicher ist – und dafür braucht es auch die dazu passenden Chips", sagt Esser weiter. Die Lösung liege in der Grundidee eines "security system on a chip", so Heinz Martin Esser: „Ohne solche sicheren Halbleiter mit bereits darauf verankerter sicherer Software gibt es in Zukunft keine zuverlässige IT-Infrastruktur", sagt Esser. Vor jeder Regulierung und Meldepflichten betroffener Unternehmen und Institutionen brauche man besonders sichere Technologien – neben der Software spiele die Hardware dabei die Schlüsselrolle.

„Deutschland verfügt im internationalen Vergleich über ausgezeichnete Infrastrukturen – sei es im Bereich Telekommunikation, Energie, Verkehr, Gesundheit oder staatliche Dienstleistungen. Jetzt stehen wir vor der großen Herausforderung, diese in einem Konzept von intelligenten Netzen zu bündeln. Wenn wir es schaffen, hierbei mit der Zuverlässigkeit und Sicherheit unserer Technologie und Systeme zu punkten, so wird die Digitalisierung für den Technologiestandort Deutschland zu einem nachhaltigen Erfolgsfaktor", sagt Michael Kretschmer, Mitglied des Deutschen Bundestages und Stv. Vorsitzender der CDU/CSU- Bundestagsfraktion für Bildung und Forschung, Kunst, Kultur und Medien, abschließend.

*__Hinweis für Journalisten__: Unter "Kritischer Infrastruktur" versteht man unter anderem das Transportwesen, Energie- und Wasserversorgung, der Eisenbahn- und Flugverkehr oder der öffentliche Dienst. Ebenso in Betracht kommen Telekommunikations- und Medienunternehmen, der Finanzsektor, Krankenhäuser sowie die Ernährungswirtschaft. Nach Definition des Bundesinnenministeriums handelt es sich "um 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." Diese Infrastrukturen sind stark vernetzt und voneinander abhängig. Das wiederum erhöht die Risiken und – im Fall einer Cyberattacke – die Wahrscheinlichkeit von "Lawineneffekten".
(Quelle: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf).

Für Rückfragen:
PR Piloten (Agentur), Robert Weichert / Susann Bewernick / Ulf Mehner, Telefon: 0351 50 14 02 00, E-Mail: info@pr-piloten.de

Über SILICON SAXONY e.V.: Der Silicon Saxony e.V. ist der größte Industrieverband für Mikro- und Nanoelektronik, Photovoltaik, Software, Smart Systems und Applikationen in Europa. Der Verein wurde im Dezember 2000 als Netzwerk der Halbleiter-, Elektronik- und Mikrosystemindustrie gegründet. Er verbindet Hersteller, Zulieferer, Dienstleister, Hochschulen, Forschungsinstitute und öffentliche Einrichtungen am Wirtschaftsstandort Sachsen. In den 300 Mitgliedsunternehmen, die einen Umsatz von mehr als 4,5 Milliarden Euro pro Jahr erzielen, sind derzeit rund 40.000 Mitarbeiter beschäftigt.