IT-Sicherheitswirtschaft fordert nationale ‚Security-Roadmap'

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hat am 28.10.2013 die neue Bundesregierung aufgefordert, die Erarbeitung und Umsetzung einer nationalen ‚Security-Roadmap' in ihr Arbeitsprogramm aufzunehmen.

Das immer offenkundiger werdende Ausmaß der Abhöraktionen zeigt die Herausforderungen durch Cyber-Spionage. Dem muss durch eine entsprechende Priorisierung im kommenden Regierungsprogramm Rechnung getragen werden. Eine nachhaltige IT-Sicherheitsstrategie, in die die maßgeblichen Beteiligten aus Politik, Anwendern, Wissenschaft und IT-Sicherheitsindustrie eingebunden sind, ist für die Sicherstellung der Handlungs-Souveränität von Staat und Wirtschaft dringend erforderlich.

Mit dem im September 2013 eingerichteten „Runden Tisch zur IT-Sicherheitstechnik" hat die Bundesregierung bereits eine wichtige Grundlage geschaffen. Nun gilt es, dieses Gremium, in dem alle Vertreter an einem Tisch sitzen, mit der Erarbeitung einer konkreten nationalen ‚Security-Roadmap' zu beauftragen. Ziel ist es, die bereits identifizierten Handlungserfordernisse zu konkretisieren, mit den erforderlichen Finanzmitteln zu versehen und einen detaillierten Zeitplan zur Umsetzung vorzugeben.

„Voraussetzung für sichere IT ist die Beschaffung und der Einsatz von hochwertiger und vertrauenswürdiger Sicherheitstechnologie. Und diese gibt es weder zum Nulltarif noch kommt sie von alleine zum Einsatz. Das hat die Abhöraktion von Merkels ungeschütztem Partei-Handy noch einmal gezeigt", so TeleTrusT-Vorstand und Sirrix-CEO Ammar Alkassar. „Der Schutz von Daten und Kommunikation ist die Verkehrssicherheit einer digitalisierten Gesellschaft des 21. Jahrhunderts: Niemand stellt heute ernsthaft die Gurtpflicht trotz Komforteinbußen in Frage. Bei der IT-Sicherheit müssen wir dort noch hin."

Deutschland hat bereits eine ausgeprägte und international erstklassige IT-Sicherheitsindustrie und durch enge Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik auch eine bedarfsgerechte Lösungspalette zur Absicherung von IT-Systemen. Diese muss nun aktiv in eine langfristige und abgestimmte IT-Sicherheitsstrategie und -Roadmap integriert werden.

„Dabei muss das Ziel sein, einen Paradigmenwechsel in der IT-Sicherheit voranzutreiben, um nachhaltig und effizient unsere Informationen und Daten zu schützen. IT-Systeme müssen pro-aktiv vor intelligenten Angriffen geschützt werden, statt wie bisher nur reaktive Maßnahmen zu ergreifen. In diesem innovativen IT-Sicherheitsbereich ist Deutschland bereits Vorreiter, eine verstärkte Umsetzung ist allerdings erforderlich", meint Prof. Norbert Pohlmann, TeleTrusT-Vorsitzender und Leiter des Instituts für Internet-Sicherheit der Westfälischen Hochschule.

Zu den weiteren bereits identifizierten Handlungsempfehlungen gehören:

1. Angemessenes hohes IT-Sicherheitsniveau anstreben und IT-Sicherheitsmarkt stärken:

- Verpflichtung zur Einhaltung branchenspezifischer IT-Sicherheitsstandards in kritischen Infrastrukturen
- Nationales Routing der nationalen Kommunikationsverkehre (z.B. IP, E-Mail, Voice)
- Definition messbarer Sicherheitsziele für Deutschland (z.B. Domänenzertifizierung, E-Mail-Verschlüsselung)

2. Stärkung der Evaluierungskapazitäten von IT-Sicherheitsprodukten:

- Überprüfung der Produkthaftung für IT-Sicherheitsmängel
- Aufbau von zertifizierten IT-Sicherheitsdienstleistern zur Bewertung von IT-Sicherheitsprodukten
- Ausbau des Bundesamts für Sicherheit in der Informationstechnik zur kompetenten Begleitung der Digitalisierung der Gesellschaft durch verstärkte Beratungs- und Zertifizierungskapazitäten
- Deutsche IT-Sicherheitswirtschaft aktiv ausbauen

3. Flankierung bei der Bereitstellung von Risikokapital für IT-Sicherheitsunternehmen:

- stärkere Berücksichtigung nationaler IT-Sicherheitsinteressen bei öffentlichen Vergaben

G&D liefert Common Access Cards an DMDC des US-Verteidigungsministeriums

Giesecke & Devrient (G&D), einer der weltweit führendenden Anbieter sicherer Authentisierungs-lösungen, hat am 15.10.2013 den Zuschlag zur Bereitstellung von Karten zur physischen und logischen Zugangskontrolle für das hochsichere Rechenzentrum DMDC (Defense Manpower Data Center) des US-amerikanischen Verteidigungsministeriums erhalten. Diese Karten sollen der personenbezogenen Identitätsprüfung von Regierungsmitarbeitern und Vertragspartnern dienen und entsprechen dem hierfür von der US-Regierung festgelegten Standard FIPS 201.

Das DMDC stellt seit vielen Jahren Chipkartentechnologie zur Zugangskontrolle sowie personenbezogenen Identitätsprüfung (Common Access Card/Personal Identity Verification, CAC/PIV) im US-amerikanischen Verteidigungsministerium bereit. Die CAC ist die den Bestimmungen der „Homeland Security Presidential Directive 12" entsprechende Standard-ID-Karte zur personenbezogenen Identitätsprüfung für aktive Mitglieder der uniformierten Dienste, ausgewählten Reserve (SELRES), für zivile Ministeriumsmitarbeiter sowie berechtigte Vertreter von Vertragspartnern. Darüber hinaus dienen die CAC-/PIV-Karten vornehmlich zur physischen Zugangskontrolle in Gebäuden und zugangsbeschränkten Bereichen sowie zur logischen Zugangskontrolle für die Computernetzwerke und -systeme des Ministeriums.

Angesichts der langjährigen Erfahrungen von G&D bei der Entwicklung von Sicherheitstechnologien – mit weltweit Millionen zu Identifizierungs- und Authentisierungszwecken eingesetzten Chipkarten – beauftragte DMDC das Unternehmen mit der sofortigen Bereitstellung von Karten für sein CAC-/PIV-Programm.

TABULA RASA: EU-gefördertes Projekt schließt Sicherheitslücken bei biometrischen Anwendungen

Software zur Gesichts-, Sprach- und Fingerabdruckerkennung hat es inzwischen auf Smartphones und Tablets geschafft. Doch auch diese äußerst effizienten biometrischen Sicherheitssysteme haben Schwachstellen, die ausgenutzt werden, um Zugang zu fremden Ressourcen oder Daten zu gewinnen.