PRESSEMITTEILUNG

TeleTrusT – Bundesverband IT-Sicherheit e.V.:

IT-Sicherheitswirtschaft fordert nationale 'Security-Roadmap'

Klare Strategie für IT-Sicherheit und Datenschutz von Behörden, Unternehmen, Wissenschaft und Bürgern ist Grundlage für nationale Souveränität

Berlin, 28.10.2013 – Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) fordert die neue Bundesregierung auf, 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

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Engineer for System Security" (T.E.S.S.) sowie des Qualitätszeichens "IT Security made in Germany". Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

TeleTrusT – Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 /40054310, holger.muehlbauer@teletrust.de
www.teletrust.de