15.09.2011 – 18:48 Uhr

Privatsektor gefährdet laut Befund eines britischen Berichts die nationale Cybersicherheit

London (ots/PRNewswire) -

Britische Netzwerksicherheitsspezialisten haben Klagen über den Privatsektor geäussert. Doktrinen, Forschungen und Gespräche deuten auf die Notwendigkeit eines definitiven, umfassenden Plans für widerstandsfähige Cybersysteme hin.

Kritische nationale Infrastrukturen (KNI) Grossbritanniens sind einem enormen Angriffsrisiko ausgesetzt. Laut dem Bericht einer führenden Denkfabrik müssen Eigentümerunternehmen erhöhte Verantwortung für Sicherheit und Schutz ihrer Systeme übernehmen.

Chatham House bestätigte gemeinsam mit BAE Systems Detica diesen Befund, nachdem Interviews mit zahlreichen mit dem Schutz von Versorgungsbetrieben, Kommunikationsnetzwerken, Gesundheitsdiensten, Nahrungsmitteldiensten, Banken und Stromnetzen befassten Personen durchgeführt wurden.

Obwohl KNI als ein Hauptziel für Bedrohungen gelten, sei die dortige Umsetzung von Sicherheitsmassnahmen "planlos und willkürlich", und es bestehe "die Notwendigkeit, bei der Identifizierung potentieller Gefahren weiter vorauszublicken und vorgreifend Gegenmassnahmen gegen potentielle Cyberrisiken zu entwickeln."

In der Studie wird gefolgert, dass "es deutlich an einheitlichen und konsequenten Strategien und Praktiken fehlt, und zwar in dem Umfang, dass man in Grossbritannien nicht einmal annähernd von gesellschaftsübergreifenden Schutzmassnahmen gegen Cyberschwachstellen und -bedrohungen ausgehen kann."

Die Ergebnisse wurden diese Woche anlässlich einer Verteidigungsausstellung in London bekanntgegeben, bei der führende Denker zum Austausch über aktuelle Themen zusammentrafen. Allgemein herrschte Einigkeit darüber, dass KNI das wahrscheinlichste Ziel seien, wenn im Krisenfall entweder staatliche oder Einzelakteure die Cybersicherheit auf nationaler Ebene bedrohen. Die Teilnehmer stimmten auch dahingehend überein, dass ein gründliches Verständnis des "Cyberwortschatzes" notwendig sei, bevor wirklich nützliche Gespräche beginnen können.

Allerdings unterschieden sich die Expertenmeinungen und -prognosen hinsichtlich mehrerer kritischer Angelegenheiten wesentlich. Beispielsweise war strittig, ob Online-Banking nutzungssicher, ob "absolute" Cybersicherheit auf technologischer Ebene möglich und ob eine "digitale Katastrophe" mit einem Terrorangriff vergleichbaren Ausmasses wahrscheinlich sei.

Neben der am Privatsektor geäusserten Kritik erkannten die meisten Beteiligten an, dass die gegenwärtige Regierung die Bedrohung ernst genommen und entsprechende Fortschritte demonstriert habe. In der letztjährigen Strategic Defence and Security Review (SDSR) wurde die Bedeutung von Cybersicherheit auf Gefahrenstufe Eins (Tier One) erhöht und ein Budget von 650 Millionen Pfund Sterling für verbesserte Sicherheit eingeräumt. Erwartungsgemäss werden auch Initiativen wie die "Get-Safe-Online"-Kampagne, mit der die Öffentlichkeit über grundlegende digitale Sicherheit aufgeklärt werden soll, das öffentliche Bewusstsein stärken.

Dennoch wird im Bericht festgehalten, dass Minister Informationen bereitwilliger mit KNI-Unternehmen teilen müssen, um positive Änderungen möglich zu machen. Eine überarbeitete offizielle Cyber-Strategie soll im Oktober veröffentlicht werden.

Vor Herausgabe des Berichts hatte das Institute for Security & Resilience Studies am University College London eine "Cyber-Doktrin" veröffentlicht. Damit sollte ein "kohärenter Entwicklungsrahmen zum Lernen von Widerstandsfähigkeit" eingeführt und der Erkenntnis Rechnung getragen werden, dass der Cyberbereich sich schneller ändert, als dies in akademischen Publikationen reflektiert werden kann.

Die Ergebnisse und potentiellen praktischen Entwicklungen sollen von leitenden Vertretern internationaler staatlicher, militärischer und Industrieorganisationen auf der von Defence IQ im Januar in London organisierten Konferenz Cyber Defence and Network Security(CDANS) erörtert werden. Die jährliche Grossveranstaltung ist als eines der führenden europäischen Foren für Cyberfragen anerkannt. Geplant sind unter anderem Gespräche

zwischen Vertretern des britischen Verteidigungsministeriums, des US-Verteidigungsministeriums, internationalen Führungskräften des CERT (Computer Emergency Response Team) und anderen Entscheidungsträgern.

Weitere Informationen finden Sie auf http://www.CDANS.org. E-Mail: enquire@DefenceIQ.co.uk Telefon: +44(0)207-328-9300

Kontakt:

.