IQPC

28.02.2012 – 19:23 Uhr

Georgischen und US-amerikanischen Banken drohen Ordnungsstrafen für mangelnden Netzwerkschutz

London (ots/PRNewswire) -

Martin Howard, Leiter der Abteilung für Cyber-Politik im Government Communications Headquarter (GCHQ) des Vereinigten Königreichs, und weitere Führungskräfte aus Regierung und Militär werden im Mai auf der in Brüssel stattfindenden Konferenz International Cyber Security 2012 [http://www.cyber-securityevent.co m/redForms.aspx?id=677612&pdf_form=1] mit Leitern von Cyber-Informationsabteilungen massgeblicher infrastruktureller Unternehmen zusammentreffen , darunter BP, E.On Energie, CitiBank und GlaxoSmithKline.

Sowohl in Georgien als auch in den USA werden derzeit neue Rechtsvorschriften für die Cybersicherheit von Banken und anderen kritischen vernetzten Infrastrukturen (CNI) ausgearbeitet, welche einen Präzedenzfall für andere Länder schaffen könnten.

In einem Interview mit Defence IQ lieferte Georgiens stellvertretender Verteidigungsminister Andro Barnovi einen Abriss seiner Ansichten zur ungewöhnlichen Lage, in der sich ein Grossteil der Welt derzeit befindet - den Schutz von Objekten der nationalen Sicherheit Privatunternehmen übertragen zu müssen.

"Ich weiss, dass bestimmte Banken gegenwärtig sehr fortschrittliche Systeme für den Schutz vor Cyber-Kriminalität einführen. Es liegt jedoch nach wie vor in ihrem eigenen Ermessen. Die Regierung kann in dieser Richtung bestenfalls Ratschläge geben."

In Kürze könnten Gesetze verfasst werden, die sicherstellen, dass Unternehmen ihre Systeme schützen, so Barnovi. Er bezog sich dabei auf die nach wie vor laufende Entwicklung einer offiziellen staatlichen Cyber-Strategie, welche sich aufgrund der unvergleichlichen Komplexitäten des Cyber-Bereichs noch immer in der Entwurfsphase befindet.

"Ich denke, sobald wir das erreicht haben, werden mit Sicherheit Rechtsvorschriften folgen. Höchstwahrscheinlich wird es eine Reihe von Bestimmungen geben ... Bislang haben wir nur unsere gemeinsame Vorstellung von der Wichtigkeit dieser Gesetzgebungen und vom langen Prozess, den deren Verabschiedungen darstellt. Derzeit besteht noch keine gesetzliche Pflicht, aber wir können uns vorstellen, dass es diese in naher Zukunft geben wird."

Während Barnovi keinerlei detaillierten Angaben bezüglich theoretischer finanzieller Sanktionen machte, gaben die USA diesen Monat mehr preis. Der Senat gab neue, von beiden Parteien vertretene Legislativprogramme bekannt, welche Banken und Unternehmen mit Einfluss auf die amerikanische Wirtschaftsentwicklung unter Androhung empfindlicher Strafen dazu verpflichten würden, sich vor Infiltration zu schützen.

Gemäss dem "Cyber Security Act (S. 2105)", wäre das Department of Homeland Security (Heimatschutz-Ministerium) für die Identifizierung stark gefährdeter Unternehmen zuständig. Diese Unternehmen müssten daraufhin nachprüfen können, dass Cyber-Sicherheits-Standards eingehalten werden. Andernfalls drohte ihnen eine strafrechtliche Verfolgung.

Ziel der Konferenz für internationale Cyber-Sichereit "International Cyber Security" ist die Unterstützung privater und öffentlicher Bereiche mit Augenmerk auf die Netzwerk-Sicherheit in Schlüsselbereichen der nationalen Sicherheit. Hochrangige Vertreter von Regierung, Militär und Privatunternehmen, die einen wichtigen Beitrag zur nationalen Sicherheit leisten, werden ihre wesentlichen Bedenken bezüglich ihrer Netzwerke in den nächsten zwölf bis 18 Monaten äussern. Des Weiteren sind Massnahmen zum Schutz ihrer Systeme vor Cyber-Attacken ein Thema der Konferenz.

Weitere Informationen und Buchungsanfragen finden Sie unter http://www.Cyber-SecurityEvent.com.

Tel.: +44(0)20-7368-9300

E-Mail: enquire@iqpc.co.uk