18.10.2016 – 14:52 Uhr

Internet in Europa durch DoD Gateways gefährdet

Hamburg (ots) -

Experten haben auf der IKT-Sicherheitskonferenz 2016 davor gewarnt, dass die Einbeziehung der globalen DoD Gateways in Cyberaktivitäten zu einer signifikanten Störung der Verfügbarkeit des Internets in Europa führen kann.

Backbone Gateways sind die Hauptschlagadern des Internets. Wenn durch Störungen oder Angriffe einige Gateways beschädigt werden bzw. ausfallen, wird der Datenstrom über die verbliebenden Backbone Gateways geleitet, um so die Verfügbarkeit des Internets weiterhin zu gewährleisten.

Aber welche Konsequenzen resultieren aus der Tatsache, dass die vorhandenen Backbone Gateways in Europa - die eine primäre Rolle für die Sicherstellung der Konnektivität des gesamten Internets in Europa einnehmen - als Bestandteil einer Cyberdoktrin anderer Staaten 'missbraucht' werden können?

Dieser Fragestellung gingen die Sicherheitsexperten der PAN AMP AG aus Hamburg nach, die anhand von Vermessungen der globalen Internet Gateways erstmals Cyberkonflikte zwischen den USA und Russland sowie den USA und China simulierten. Unter der Prämisse, dass in den Cyberkonflikten Waffen zur IP- und Datenpaket-Transformation zur Anwendung kommen, und die sich außerhalb des US-Territoriums befindlichen DoD Gateways in Deutschland und Japan zum Angriff / zur Verteidigung eingesetzt werden, führte die Simulation zu einer Überlastung der vernetzten Backbone Gateways in Europa und Asien.

Cyberdefence Experten zeigten sich überrascht, dass durch die Überlastung einzelner Backbone Gateways und die hieraus folgenden Umleitungen von Datenpaketen, zu Kettenreaktionen führten, die ihrerseits weitere Backbone Gateways überlasteten. So stieg die kriegsbedingte Netzlast in Europa auf bis zu 92,8 % bei einem Cyberwar zwischen den USA und Russland bzw. auf bis zu 98,1 % bei einem Cyberwar zwischen den USA und China.

"Auch wenn allgemein angenommen wird, dass Cyberkonflikte in Netzwerken mit einem verteilten Ressourcenmanagement, wie dem Internet, global wenig Schaden anrichten können, weisen die Ergebnisse der Cyberwar Simulation darauf hin, dass die topologischen Schwächen der gegenwärtigen Backbone Gateways, sich schwerwiegend bei einem gezielten Missbrauch auswirken können. Dies könnte von jenen Staaten ausgenutzt werden, die diese Systeme gezielt in ihre Cyberdoktrin einbinden", so Bert Weingarten, Vorstand der PAN AMP AG.

Eine Restkapazität von lediglich 1,9 bis 7,2 % der Backbone Gateways für nicht 'kriegsbedingten' Datenverkehr, wäre nicht mehr ausreichend, um in Europa Datenverbindungen aus Mobilfunknetzen oder Leit- und Steuerungssystemen für kritische Infrastrukturen aufrecht zu erhalten. Ein möglicher Kausalschaden wäre der großflächige Stromausfall in Deutschland, Österreich und der Schweiz.

Würden Staaten sich die Kenntnisse über die bestehenden Sicherheitsrisiken der Backbone Gateways zu eigen machen, so die Sicherheitsforscher, könnten sie die Backbone Gateways auch als Schutzschild im Cyberwar missbrauchen und somit großen Schaden anrichten. Denn Fakt ist, unsere moderne Gesellschaft ist mittlerweile vollumfänglich von der stetigen, reibungslosen Verfügbarkeit der Netzinfrastruktur, und somit auch der Backbone Gateways, abhängig.

Kontakt:

PAN AMP AG, Hamburger Straße 11, 22083 Hamburg, Deutschland
Der Vorstand
Internet: panamp.de
Telefon: +49 [0]40 553002-0