heise online

04.10.2013 08:11

NSA/GCHQ-Skandal: Massiver Cyberangriff auf Belgacom mit "hochentwickelter Malware"

Experten gehen nach einer Untersuchung der **ausgefeilten Cyber-Attacke[1]** auf das belgische Telekommunikationsunternehmen **Belgacom[2]** davon aus, dass keine Kundendaten oder sonstigen personenbezogenen Informationen abgegriffen oder kompromittiert wurden. Diesen Fall könne man zwar nicht ganz ausschließen, erklärte Frank Robben aus dem Büro des belgischen Datenschutzbeauftragten am Donnerstag bei einer **Anhörung[3]** im **Untersuchungsausschuss[4]** des EU-Parlaments zum Geheimdienstskandal. Es habe aber offenbar keine "massive Weiterleitung" entsprechender Daten gegeben.

Behörde hat Robben zufolge vor allem geprüft, ob die getroffenen Sicherheitsmaßnahmen des Providers anhand der bekannten Risiken für eine derartige Firma ausreichten. Belgacom habe die Datenschützer dazu auch vertrauliche Dokumente einsehen lassen. Herausgekommen sei, dass die Absicherung gut gewesen und der halbstaatliche Provider nicht gegen Datenschutzvorschriften verstoßen habe. Robben bescheinigte Belgacom eine "professionelle Reaktion" auf den Vorfall, durch die "weiterer Schaden vermieden worden" sei.

Der Kontrolleur räumte aber ein, dass noch nicht alle Umstände des Angriffs aufgeklärt seien. Die von Belgacom im Juni entdeckte Schadsoftware habe eine anspruchsvolle Verschlüsselungstechnik für die Kommunikation nach außen verwendet. Um genau herauszufinden, welche Informationen übertragen wurden, und um der Attacke auf den Grund zu gehen, müssten diese Verfahren erst geknackt werden. "Dazu haben wir in Belgien keine ausreichende Sachkenntnis", meinte Robben. Für ein entsprechendes Unterfangen müssten EU-weite Zuständigkeiten geschaffen und Kräfte gebündelt werden. Noch stehe auch in den Sternen, ob andere europäische Provider Opfer ähnlicher Angriffe geworden sein könnten. Generell sei es wichtig, auf EU-Ebene eine schlüssigere Strategie zur Cyber-Sicherheit auszuarbeiten.

Der *Spiegel* hatte jüngst unter Berufung auf den Whistleblower Edward Snowden **gemeldet[5]**, dass das Government Communications Headquarters (GCHQ) hinter der schon seit 2010 laufenden Attacke gestanden habe. Es sei dem eng mit der US-amerikanischen NSA **kooperierenden[6]** britischen Geheimdienst darum gegangen, an die zentralen, internationalen Datenverkehr durchleitenden Router des Unternehmens zu gelangen. Die Kontrolle darüber sollte dann für Man-In-The-Middle-Angriffe auf Smartphone-Nutzer missbraucht werden. Auch der niederländische öffentlich-rechtliche Rundfunk will **Beweise dafür haben[7]**, dass die Briten verantwortlich sein sollen.

Belgacom-Generalsekretär Dirk Lybaert wies diese Berichte als reine Spekulation zurück. Er gab zwar zu, dass auch die Tochter **BICS[8]** (Belgacom International Carrier Services) betroffen gewesen sei, die einen Austauschknoten für Daten- und Kommunikationsdienste zwischen mehreren hundert Providern einschließlich der Zugangsanbieter von EU-Gremien betreibt. Da es Verbindungen mit dem internen Netz der Muttergesellschaft gebe, "haben wir auch dort die Malware festgestellt". Die Firma wisse aber nicht, wer oder was das eigentliche Ziel der Spähaktion gewesen sei und wer dahinterstecke. Klar sei nur, dass man es mit einem Angreifer zu tun gehabt habe, "der sehr große Ressourcen eingesetzt hat".

"Wir haben keine Hinweise, die uns zum Täter führen könnten oder welche Informationen er erhalten hat", führte der Belgacom-Manager Geert Standaert aus. Wo genau die ausgenutzte Schwachstelle sich befinde und wie die Attacke im Detail abgelaufen sei, habe bislang ebenfalls nicht herausgefunden werden können. Die "hochentwickelte Malware" sei von Sachverständigen im eigenen Haus "in Zusammenarbeit mit HP und Microsoft" entdeckt worden. Belgacom habe daraufhin den Angriff pflichtgemäß gemeldet und den **umstrittenen niederländischen Dienstleister Fox-IT[9]** als Experten herangezogen.

Die Schadsoftware hatte sich Standaert zufolge im internen System Belgacoms eingenistet, das vom öffentlichen Netz, speziellen Kundenleitungen oder Cloud-Lösungen getrennt sei. Von rund 20.000 angeschlossenen Rechnern seien rund 120 Windows-Server und -Clients nebst Microsoft-Office-Anwendungen befallen gewesen, die mittlerweile alle davon gesäubert worden seien. Wann der Trojaner in das System hineingekommen sei, "wissen wir nicht". Anomalien im Zusammenhang mit Netzwerkdaten seien nicht festgestellt worden.

Allgemein geht Standaert von einer ernsthaften, organisierten Bedrohung der Integrität Belgacoms aus, die aber "beschränkte Folgen" nach sich gezogen habe. Die Entwickler der Malware hätten "bedeutende Möglichkeiten und sehr gute technische Sachkenntnis" gehabt. Der Konzern selbst halte internationale Normen zur IT-Sicherheit ein, seine Datenzentren führten alle ein ISO-Zertifikat. Die Ergebnisse der intern weiter laufenden Prüfungen flößen in noch bessere Aktionspläne ein.

Die bekannten Wege zum Einspielen von Trojanern seien alle blockiert, jetzt überwache Belgacom den Netzverkehr noch intensiver, ergänzte Lybaert. Keiner könne aber eine Garantie dafür abgeben, einen derartigen Angriff abzuwehren. Dafür brauche es ein globales Vorgehen und entsprechende Rechtsgrundlagen. In der EU reichten die Mittel für eine effiziente Bekämpfung von Cybercrime nicht aus, monierte der Konzernchef. Der Staat müsse mehr Geld für die Strafverfolgung zur Verfügung stellen und den Austausch über Bedrohungen der IT-Sicherheit zwischen allen Seiten verbessern.

Die Ausführungen ließen die EU-Abgeordneten konsterniert zurück. Es sei unglaubwürdig, dass von einem massiven, offenbar von staatlicher Seite aus koordinierten Angriff nur Belgacoms interne Systeme betroffen gewesen seien, konstatierte die Sitzungsleiterin Sophie in't Veld. Die Liberale zeigte sich "frustriert", dass die gegebenen Antworten nur mehr Fragen aufgeworfen hätten. Der Innenexperte der Grünen, Jan Philipp Albrecht, forderte die EU-Kommission und den Rat auf, die Attacke als schwere Straftat und prinzipiellen Rechtsverstoß scharf zu verurteilen.

Mehrere Parlamentarier bezeichneten es als zynisch und inakzeptabel, dass der geladene GCHQ-Direktor Iain Lobban seine Teilnahme absagte und auch kein britischer Diplomat Stellung bezog. Parallel mehren sich Plädoyers der Volksvertreter, zur Aufklärung der Affäre Snowden per Videokonferenz als Zeugen zuzuschalten und so möglicherweise auch mehr Material für laufende Ermittlungen durch Strafverfolgungsbehörden der Mitgliedsstaaten zu erhalten. (*Stefan Krempl*) / (**jk[10]**)

URL dieses Artikels:

http://www.heise.de/newsticker/meldung/NSA-GCHQ-Skandal-Massiver-Cyberangriff-auf-Belgacom-mit-hochentwickelter-Malware-1972194.html

Links in diesem Artikel:

[1] http://www.heise.de/newsticker/meldung/Spaehangriff-auf-Belgacom-1958505.html
[2] http://www.belgacom.be/
[3] http://www.europarl.europa.eu/document/activities/cont/201309/20130930ATT72076/20130930ATT72076EN.pdf
[4] http://www.heise.de/newsticker/meldung/PRISM-und-Tempora-EU-Parlament-setzt-Untersuchungsausschuss-ein-1911312.html
[5] http://www.heise.de/newsticker/meldung/Britischer-Geheimdienst-GCHQ-steckt-offenbar-hinter-Cyber-Angriff-auf-Belgacom-1962497.html
[6] http://www.heise.de/newsticker/meldung/Bericht-Briten-schnueffeln-Internet-noch-massiver-aus-als-die-USA-1894852.html
[7] http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html
[8] http://www.bics.com/
[9] http://www.heise.de/newsticker/meldung/Streit-um-Polizeipraesenz-bei-Hacker-Festival-OHM-1849019.html
[10] mailto:jk@ct.de