14021/J XXIV. GP

Eingelangt am 18.02.2013

ANFRAGE

der Abgeordneten Bucher

Kolleginnen und Kollegen

an die Bundesministerin für Inneres

betreffend Cyberspionage gegen Österreich

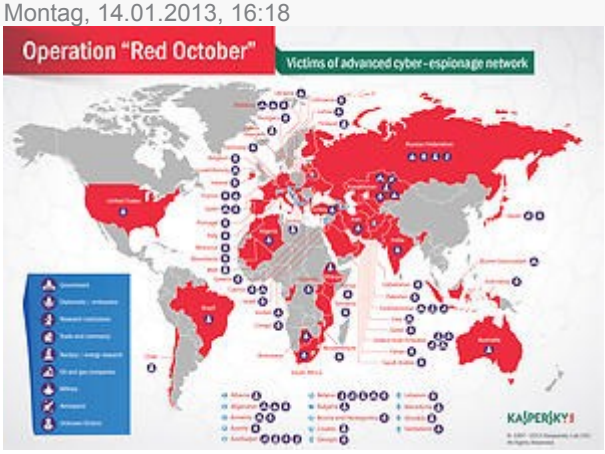
Laut nachstehendem Artikel des Nachrichtenmagazins „Focus“ wurde ein groß angelegter Spionage-Angriff über das Internet auf diplomatische Vertretungen, Regierungsorganisationen und Forschungsinstitute in verschiedenen Ländern entdeckt. Laut beigefügter Übersicht dürfte auch Österreich betroffen gewesen sein. Dies gilt es zu hinterfragen.

http://www.focus.de/digital/internet/operation-roter-oktober-einzigartige-und-hochflexibele-cyberspionage-aktion-enttarnt_aid_897766.html

„Operation Roter Oktober“

„Einzigartige und hochflexibele“ Cyberspionage-Aktion enttarnt

Montag, 14.01.2013, 16:18



Kaspersky
Experten sprechen von einer gigantischen Cyberspionage-Aktion und einem „einzigartigen und hochflexiblen Schadprogramm“. Es beschaffte sich vertrauliche geopolitische Informationen von Regierungen und diplomatischen Vertretungen.
Sicherheitsexperten haben einen groß angelegten Spionage-Angriff über das Internet auf diplomatische Vertretungen, Regierungsorganisationen und Forschungsinstitute in verschiedenen Ländern entdeckt. Betroffen waren vor allem Einrichtungen in Osteuropa sowie in Zentralasien. Seit mehreren Jahren seien Computer und Netzwerke der Organisationen systematisch nach hochsensiblen Dokumenten mit vertraulichen geopolitischen Inhalten durchsucht worden, teilte der russische Antivirus-Spezialist Kaspersky Lab am Montag mit.

Weiterhin wurden Zugänge zu gesicherten Computersystemen ausspioniert sowie Daten aus persönlichen mobilen Geräten und von Netzwerk-Komponenten gesammelt. An der Aufklärung der Aktion waren Experten der offiziellen Computer Emergency Response Teams (CERT) in Weißrussland, Rumänien und den USA beteiligt.

Aktion könnte schon seit 2007 laufen

Wer die Angreifer sind, konnte Kaspersky nicht ermitteln. Aber Kaspersky geht nach einer Analyse der Schadsoftware davon aus, dass die Angreifer eine russisch-sprachige Herkunft haben. „Das heißt aber nicht, dass staatliche Stellen in Russland die Spionage-Aktion in Auftrag gegeben haben, denn russisch-sprachige Programmierer gibt es in vielen Ländern“, sagte Kalkuhl.

Die Cyberspionage-Kampagne „Operation Roter Oktober“ sei im vergangenen Oktober entdeckt worden, sagte Kaspersky-Virenanalyst Magnus Kalkuhl der Nachrichtenagentur dpa. „Wir gehen jedoch davon aus, dass die Aktion schon im Jahr 2007 begonnen hat.“ Außer Botschaften und Regierungsorganisationen seien vor allem Forschungsinstitute, Energie- und Atomkonzerne, Handelsorganisationen und Einrichtungen der Luft- und Raumfahrt betroffen gewesen. Der Cyberspionage-Angriff laufe noch immer.

Angreifer schicken infizierte E-Mails

Die Angreifer nutzen nach Angaben von Kaspersky Schwachstellen in den Microsoft-Programmen Word und Excel aus. Für die gibt es zwar bereits Sicherheitsaktualisierungen, aber viele Anwender haben diese noch nicht installiert. Dabei schickten die Angreifer infizierte E-Mails an ihre Opfer, um die Schwachstellen der Programme auszunutzen.

Weitere Werkzeuge der Online-Spione seien bösartige Erweiterungen für den Acrobat Reader von Adobe sowie Microsoft Office, mit denen auf den befallenen Rechnern Programme ausgeführt werden können. Auf diesem Weg erhalten die Angreifer auch dann einen Zugriff auf das Zielsystem, wenn der eigentliche Kern der Schadsoftware bereits entdeckt und entfernt oder das System mit einem Sicherheitsupdate gesichert wurde.

Hacker haben es auf Regierungsdateien abgesehen

Die Online-Spione haben es vor allem auf Dateien mit der Endung „.acid“ abgesehen, die von der Software „Acid Cryptofiler“ erzeugt werden. Dieses Verschlüsselungsprogramm wird nach Angaben von Kaspersky von verschiedenen öffentlichen Einrichtungen genutzt, unter ihnen der Europäischen Union und der Nato.

Kontrolliert wurden die Angriffe von mehr als 60 Servern, die vor allem aus Deutschland und Russland stammten. Diese Infrastruktur in der ersten Reihe der „Command-and-Control-Server“ dient auch dazu, die Identität des eigentlichen Kontrollsystems zu verbergen.

Daher stellen unterfertigte Abgeordnete an die Frau Bundesministerien für Inneres folgende

ANFRAGE:

1.

Gab es seit 2007 Cyberangriffe auf Österreich?

2.

Wenn ja, welche konkreten Angriffe gab es seit 2007 bzw. wie genau sahen diese Angriffe aus und wer wurde insbesondere von wem angegriffen? (Bitte aufgegliedert nach einzelnen Angriffen samt Schilderung der „Sachverhalte“ - insbesondere Nennung der Angreifer und der „Opfer“, der konkreten Abläufe, Schäden bzw. „gestohlene“ Informationen, etc.)

3.

Wann haben Sie jeweils Kenntnis von den jeweiligen Angriffen erlangt?

4.

Welche Maßnahmen wurden in diesem Zusammenhang seitens Ihres Ministeriums gesetzt?