Bundesministerium
des Innern

Innenausschuss
A-Drs. 17(4)390

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

An den
Sekretär des 4. Ausschusses
des Deutschen Bundestages (Innenausschuss)
Herrn Ministerialrat Dr. Heynckes
Platz der Republik 1
11011 Berlin

Leiter des
Kabinett- und Parlamentreferates
HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin
TEL +49 (0)30 18 681 - 1069
FAX +49 (0)30 18 681 - 1019
E-MAIL KabParl@bmi.bund.de
INTERNET www.bmi.bund.de

DATUM Berlin, 24. November 2011

BETREFF Bericht für den Innenausschuss des Deutschen Bundestages zum Hackerangriff auf die PATRAS-Systeme von Zoll und Bundespolizei
ANLAGEN - 1 -

Sehr geehrter Herr Dr. Heynckes,

anbei übersende ich Ihnen den in der 57. Sitzung des Innenausschusses am 9. November 2011 von den Ausschussmitgliedern erbetenen Bericht zum Hackerangriff auf die PATRAS-Systeme von Zoll und Bundespolizei.

Ich bitte diesen Bericht den Mitgliedern des Innenausschusses zur Verfügung zu stellen.

Mit freundlichen Grüßen
Im Auftrag

Dr. Klos

Innenausschuss
Eingang mit Anl. am 29.11.2011/2475
1. Vors. m.d.B. um
Kenntnisnahme/Rücksprache
2. Mehrfertigungen mit/ohne Anlagen
an Abg. SE, Obl., Sekr.
...
3. Wv
4. z.d.A.

Bundesministerium
des Innern

Bericht für den Innenausschuss des Deutschen Bundestages

zum Thema:

Hackerangriff auf die PATRAS-Systeme von Zoll und Bundespolizei

Eine Gruppe von Hackern mit dem Namen „No-Name Crew" (NNC) hat am 08.07.2011 Daten des Zolls und der Bundespolizei im Internet veröffentlicht. Hierbei handelt es sich um Geo-Daten sowie Steuerungsdaten für die Ortungstechnik aus einem Zielverfolgungssystem des Zollkriminalamtes (ZKA) sowie um Softwarepakete und Servicemitteilungen zur Installation von PATRAS-Servern (PATRAS = **PA**ip **TRA**cking **S**ystem; (PAIP = Police Applications Intercommunication Protocol)) der Bundespolizei. Die darüber hinaus von der NNC veröffentlichten Dokumente der Bundespolizei (lokal begrenzte Dienststelleninformationen wie Organisationpläne, Dienstanweisungen, Formulare), die nicht aus dem Angriff auf die PATRAS-Server stammen, gehen auf individuelles Fehlverhalten eines Polizisten beim Umgang mit dienstlicher E-Mail zurück, die er weisungswidrig auf seinen privaten Rechner weiter geleitet hatte, der dann erfolgreich angegriffen wurde.
PATRAS ist eine durch die Bundespolizei entwickelte und gepflegte Software zur Verarbeitung, Aufbereitung und Visualisierung von Geo-Lokations-Daten (z.B. auf einer elektronischen Landkarte). Diese werden mittels GPS-Trackern (Geräten zur Nachverfolgung einer zurückgelegten Wegstrecke) im Zuge operativer Maßnahmen gewonnen – in aller Regel von in Ermittlungsverfahren Beschuldigten oder Tatverdächtigen.

Weitere Angriffe auf eingesetzte PATRAS-Systeme bei der Landespolizei sind aus Sachsen, Berlin, Mecklenburg-Vorpommern und Nordrhein-Westfalen bekannt. Zu diesen Angriffen liegen der Bundesregierung keine detaillierten Angaben vor.

Das BfV hat bei seinen Untersuchungen keine Hinweise darauf gefunden, dass seine PATRAS-Systeme kompromittiert wurden. Das BKA betreibt keine PATRAS-Systeme, sondern eine andere Technik mit vergleichbarem Funktionsumfang.

Direkte Folgen des Hackerangriffs:

- Alle eingesetzten PATRAS-Zielverfolgungssysteme wurden nach Bekanntwerden des Vorfalls vorsorglich abgeschaltet und die vorhandenen Daten gesichert. Diese Abschaltung der Systeme dauert bis auf weiteres an.
- Das Einsatzmittel der GPS-Ortung steht auch nach Abschaltung der Server zur Verfügung, da zum einen neben PATRAS auch andere Softwarelösungen existierten und zum anderen mittels der Direkteinwahl auch unmittelbar auf die GPS-Module zugegriffen werden kann.
- Die prinzipielle Funktionsweise der GPS-Ortung war schon vorher durch Presseveröffentlichungen bekannt.
- Laufende Ermittlungsverfahren wurden in keinem Fall gefährdet.

Die PATRAS-Systeme der Bundespolizei und des Zollfahndungsdienstes waren „stand-alone"-Systeme, die sich nicht innerhalb der jeweiligen IKT-Netze der Behörden befanden. Daher wurden keine weiteren Systeme der Bundespolizei und des Zollfahndungsdienstes kompromittiert.

Im Rahmen der polizeilichen Ermittlungen wurden mehrere Tatverdächtige als Mitglieder der Hackergruppe „No-Name Crew" ermittelt. Einige der Tatverdächtigen sind u.a. wegen Computersabotage und anderer Delikte bereits polizeilich in Erscheinung getreten. Bei Durchsuchungsmaßnahmen gegen die Tatverdächtigen wurde umfängliches Beweismaterial sichergestellt. Neben den Feststellungen, die den gegen die Beschuldigten gerichteten Tatverdacht erhärten, liegen Anhaltspunkte auf weitere Straftaten vor, die mittels Computer und Nutzung des Internets begangen wurden. Der mutmaßliche Kopf der „No-Name Crew", ein 23-jähriger Arbeitsloser, ist wegen räuberischer Erpressung vorbestraft und derzeit auf Bewährung aus der Haft entlassen. Der zwischenzeitlich erlassene Haftbefehl ist auf Grund seines umfassenden

Geständnisses und Kooperation mit Polizei und Justiz unter Verhängung von Auflagen außer Vollzug gesetzt worden.

Der PATRAS-Vorfall wurde zum Anlass genommen, die IT-Sicherheitskonzepte sowie deren Umsetzung bei allen Sicherheitsbehörden im Geschäftsbereich des BMI in Zusammenarbeit mit dem BSI zu überprüfen. Über weitergehende Maßnahmen wird die Bundesregierung nach Abschluss der Schwachstellenanalyse entscheiden.

Die staatsanwaltlichen Ermittlungen sowie die sicherheitstechnischen Überprüfungen dauern an.

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) wurde sofort nach Bekanntwerden des Sicherheitsvorfalls am 08.07.2011 eingeschaltet. Entsprechend seiner Aufgabe als Informationsdrehscheibe hat das Cyber-AZ alle verfügbaren Informationen über den Vorfall und die Hackergruppe „No-Name Crew" zusammengetragen und diese den beteiligten Behörden zur Verfügung gestellt.