

PRESSEMELDUNG

Server der Bundespolizei gehackt – wie sicher sind unsere Daten in den Systemen der Bundesbehörden?

Frankfurt am Main, 11.07.2011. Hacker machen erneut auf die Sicherheitslücken in der gegenwärtigen Datensicherung aufmerksam. Nach militärischen Zielen wie zum Beispiel Lockheed Martin im Mai dieses Jahres wurde nun auch die Bundespolizei (BPOL) angegriffen. Die sogenannte „no-name-crew“ hatte sich in der Nacht zum Donnerstag auf elektronischem Wege Zugang zu einem Computer verschafft. Daraufhin speicherte der Zollfahndungsdienst Daten des Ortungssystems „PATRAS“, welches Standorte von Personen, Fahrzeugen oder Waren dokumentiert. Mit dem gezielten Angriff konnten Überwachungsdatensätze, Telefonnummern, Kennzeichen, Orte und Daten zum GPS-Tracking bei der Überwachung von Verdächtigen ausgelesen und entwendet werden. Auf dem Server liegen weiterhin zahlreiche interne Dokumente der Behörde. Also eine erste Einsatzmöglichkeit für das brandneue Nationale Cyber-Abwehrzentrum? Nach Abstimmung mit dem Zollkriminalamt heißt es, man prüfe die Daten auf kritische Informationsinhalte. Das ist für den mutmaßlichen Verursacher der Panne, den Zoll, besonders peinlich, weil das Zollkriminalamt selbst (assoziiertes) Mitglied des Cyber-Abwehrzentrums ist. Was wir nicht genug betonen können: Eine akademisch betriebene Behörde, die Bedrohungen lediglich analysiert, benötigen wir aktuell wie das sprichwörtliche Loch im Knie. Denn die Bedrohung durch neue digitale Waffen sollte man nicht studieren, sondern von vorneherein verhindern.

Um zu verstehen, warum das aktuelle IT Sicherheitssysteme nicht leisten können, muss man sich zunächst die Interessenslagen der Anbieter von Antivirensoftware ansehen.

Thomas Blumenthal, Geschäftsführer der QGroup GmbH, meint dazu: „Sichere Systeme, die nicht ausfallen – damit lässt sich nichts verdienen. Der Zustand der IT-Sicherheit lässt sich am besten daran ablesen, welche Umsätze weltweit im Bereich Antiviren/Malicious-Code-Erkennung ausgegeben werden. Antivirenprogramme funktionieren nicht. Der Grund ist ganz einfach: Antivirenprogramme können nur das erkennen, was der Programmierer der Lösung dem Programm beigebracht hat. Gänzlich unbekannte Viren kann kein Antivirenprogramm der Welt finden und löschen. Aber wir alle setzen Antivirensoftware ein und zahlen Jahr für Jahr eine erhebliche Summe an ein Kartell von Sicherheitsfirmen, die an echter Sicherheit aus finanziellen Gründen gar kein Interesse haben! Wir sehen das anders!“

Unser QTrust Server ist mit dem Trusted Operating System PitBull, einem mehrstufigen Firewallkonzept ausgestattet. Im Vergleich zu den meisten Firewalls wird bei diesem Sicherheitsprinzip die Sandboxing- Methode angewendet. Sandboxing wird in der Schifffahrt bereits seit Jahrhunderten betrieben. Schotten verhindern, dass im Falle eines Schadens an einer Stelle eindringendes Wasser das ganze Schiff zum kentern bringt. Bezogen auf die IT-Sicherheit bedeutet dies, dass bei einem Angriff zwar Daten einer „Schotte“ betroffen sind, das ganze System aber nicht gefährdet ist. Wenn man zur Sicherung aber lediglich nur eine Mauer aufbaut, so ist bei einem Hack das ganze System gefährdet. Auf den QTrust Server ist ein Zugriff des Weiteren nur durch eine dreifache Authentifizierung möglich. Neben Passwort und Smart Card ist die Anmeldung nur per Fingerabdruck, also einer zusätzlichen biometrischen Identifikation, möglich. Seit 2000 ist die QGroup GmbH das einzige IT- Sicherheitsunternehmen, das eine dreifache Authentifizierung zur Sicherung von Daten anbietet und diese auch in eine komplett neue IT- Sicherheitsstrategie einbindet.

Anmerkungen für den Herausgeber:

Über QGROUP GmbH

Die QGroup wurde 1993 als klassisches Systemhaus gegründet. Aus der Unterstützung von Unternehmenskunden beim strategischen Einsatz von IT und den damit verbundenen Prozessen bildeten sich rasch die heutigen Kompetenzschwerpunkte Sicherheit und Hochverfügbarkeit heraus. Die Grundphilosophie des Unternehmens lautet: Sicherheit durch Einfachheit. Die unter dem Markennamen QTrust angebotenen Technologien für den sicheren Zugang zu Unternehmensnetzwerken werden komplett von der QGroup in Deutschland entwickelt und betreut.

www.qgroup.de

Medienkontakt:

QGROUP GMBH

Phoenix Haus
Berner Straße 119
60437 Frankfurt am Main

Dirk Kopp
Tel.: +49 69 17 53 63-014
E-Mail: d.kopp@qgroup.de

VIER FÜR TEXAS * Ideenwerk GmbH

Taunusstraße 21
60329 Frankfurt am Main

Jill-Evelyn Hellwig
Tel.: +49 69 25 49 24-34
E-Mail: hellwig@4ft.de

Immer auf dem aktuellsten Stand:

www.qgroup.de/presse
twitter.com/QGROUP_DE
twitter.com/QTrust
twitter.com/ftServer