Hackerangriff

Cyberkrieg im Pentagon

dpa

15.07.2011 3,5 (2) **Legende**

Die USA haben eine neuen Strategie zur Cyber-Abwehr. Dafür ist es auch höchste Zeit, denn allein in dieser Woche wurde das Pentagon allein zweimal von Hackern attackiert und zehntausende sensibler Rüstungsdaten gestohlen.

Cyber-Attacke auf das Pentagon dpa

Vor einem Jahrzehnt hat Al-Kaida das Pentagon mit einem entführten Flugzeug angegriffen. Heute sieht sich die Militärmacht USA mit einer weit größeren Bedrohung konfrontiert: „Die globale Reichweite der Computernetze und Systeme des Verteidigungsministeriums bieten Gegnern breite Möglichkeiten für Angriffe“, heißt es in einem jetzt veröffentlichten Strategiepapier des Pentagons mit dem Titel „Department of Defense Strategy for Operating in Cyberspace“.

Bei der Vorstellung dieser Strategie zur Abwehr der Cyber-Krieger gab der stellvertretende Verteidigungsminister William Lynn am Donnerstag (Ortszeit) fast beiläufig bekannt, dass der Militärapparat im März einem der bisher schwersten Cyber-Angriffe ausgesetzt war: Die einem ausländischen Geheimdienst zugerechneten Täter gelangten an 24 000 Pentagon-Dokumente, die auf dem Server eines Unternehmens lagen, das mit dem Ministerium Geschäfte macht. Um welche Vertragsfirma es sich handelte, sagte Lynn nicht. Ebenso wenig nannte er den Staat, von dem der Angriff ausging. „Der Verdacht richtet sich zuerst gegen China“, sagt der Münchener Behörden- und Unternehmensberater Arno Schönbohm, der gerade ein Buch veröffentlicht hat mit dem Titel „Deutschlands Sicherheit - Cybercrime und Cyberwar“.

„Für China ist die Frage hochspannend, wie das Pentagon denkt, welche Militärstrategien und Ziele es verfolgt.“ Als Urheber eines solchen Angriffs seien aber auch Russland und Staaten wie der Iran denkbar. Die Fähigkeit dazu könne man inzwischen weltweit kaufen, erklärt der Experte. So gebe es auch Hinweise auf Kontakte zwischen staatlichen Diensten und der organisierten Computerkriminalität. Die Täter aus diesem Bereich verfügen über effiziente Werkzeuge für das Eindringen in Computernetze und das Verschleiern der eigenen Spuren. Neben Cyber-Attacken durch rivalisierende Staaten rechnet das Pentagon auch mit möglichen Aktionen von Extremisten. „Wenn eine terroristische Gruppe den Zugriff auf Cyber-Werkzeuge für Störungen oder Zerstörungen erhält, müssen wir davon ausgehen, dass sie ohne großes Zögern zuschlagen werden“, sagte Lynn.

Das neue Sicherheitskonzept der USA im Cyberspace

Eine andere Art von Angriffen geht von Cyber-Anarchisten aus, die sich erst zu Beginn der Woche das Pentagon als Ziel ausgesucht haben: Bei der Aktion „Military Meltdown Monday“ (Militärkollaps am Montag) verschaffte sich die Hackergruppe Anonymous nach eigenen Angaben den Zugang zu 90 000 E-Mail-Daten von Angehörigen der US-Streitkräfte und Mitarbeitern von Rüstungsunternehmen und veröffentlichte diese im Internet. Sie seien dafür in einen Computer des Beratungsunternehmens Booz Allen Hamilton eingedrungen, „der grundsätzlich keine Sicherheitsmaßnahmen installiert hatte“, erklärten die Anonymous-Aktivisten im Internet.

„Vielleicht sind Gruppen wie Anonymous die Vorboten einer neuen APO“, also einer außerparlamentarischen Opposition, sagt Schönbohm. „Früher saß man mit Blümchen vor der Kaserne. Heute versucht man, das staatliche Informationsmonopol zu brechen.“

Das neue Konzept der USA beschreibt einen Vier-Punkte-Plan:

1) In einem ersten Schritt soll die „Cyber-Hygiene“ verbessert werden, also das bei jedem Einzelnen ansetzende Bemühen um Sicherheit.

2) Daneben sollen die Risiken durch eigene Mitarbeiter eingedämmt werden, unter anderem durch „internes Monitoring“.

3) Eine aktive Cyber-Abwehr soll Eindringlinge an den Grenzen zum eigenen Netz stoppen. Gelingt dies nicht, sollen spezielle Sensoren innerhalb der Netzwerke schädliche Aktivitäten rechtzeitig aufdecken und beenden.

4) Das Pentagon will neue Konzepte für den Betrieb von Computernetzen entwickeln, die eine sichere Nutzung mobiler Geräte und den Schutz der „Cloud“ gewährleisten, also der Netz-Infrastruktur zur Bereitstellung von Daten.

Schlagworte zum Thema

Internet USA IT-Sicherheit

In der Aufklärung und bei der internationalen Verfolgung der Täter gebe es noch viel Nachholbedarf, sagt der Karlsruher Sicherheitsexperte Christoph Fischer. „Da können noch viele Prozesse optimiert werden.“ Für die Prävention von Angriffen seien die Cyber-Abwehrstrategien indes kaum wirksam. Es liege in der Natur von Software, dass sie nie hundertprozentig sicher sei. „Die Systeme sind so komplex, die haben alle Fehler. Und aktuell ist der Druck aus dem Netz so groß, dass eine Schwachstelle auch missbraucht wird, sobald sie bekanntwird.“