

Onlinedurchsuchung: BKA ist mit Zero-Day-Exploits überfordert



cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Spione lauern auf Softwarelöcher

10. September 2007

Stuttgart (ab) – Das gezielte Ausnutzen von Softwareverwundbarkeiten ist unter Geheimdiensten weltweit gang und gäbe. Davon weiß nicht nur die Bundesregierung ein Lied zu singen. Sogar das gut abgesicherte US-Verteidigungsministerium wurde offensichtlich Opfer chinesischer Hacker im Staatsauftrag.

Neben dem Pentagon gilt das US-Department of Homeland Security (DHS) als besondere Zielscheibe von Cyberangriffen. Durch die vielen Attacken seien „Hunderte von Sicherheitslücken in der Behörde bekannt geworden“, so CIO Scott Charbo. Meist wurden Desktop-PCs attackiert.

Die US-Luftwaffe plant daher einen so genannten War-Room der nicht nur für einen besseren Schutz sorgen soll, sondern auch Gegenangriffe starten kann. „Das hier ist elektronischer Krieg, bei dem auch wir unsere Cyberwaffen einsetzen müssen“, so General Charles Ickes.

Zumal wohl verschiedene Staaten und Organisationen mit gezielten Hackerangriffen die Rechner etwa des US-Verteidigungsministeriums ausspionieren. „Wir wissen, dass eine Reihe von Ländern und Gruppen aktiv diese Fähigkeiten entwickeln“, so Pentagon-Sprecher Patrick Ryder.

Auch für deutsche Security-Experten liegt es auf der Hand, dass Nachrichtendienste über Schwachstellen in Programmen auf anderen Rechnern schnüffeln. So sieht Innenstaatssekretär und Ex-BND-Chef August Hanning „finstere dritte Mächte“ unterwegs, die mit Spähprogrammen versuchten, an sensible Daten heranzukommen: „IT-Angriffe gehören zum Instrumentarium moderner ausländischer Dienste.“ Als Industriestaat sei Deutschland sehr verwundbar und sollte seine IT-Strukturen schützen.

„Geheimdienste wären ja blöd, wenn sie nicht mit Hackermethoden auf anderen Rechnern einbrechen würden“, findet Cirosec-Chef Stefan Strobel. Auch deutsche Dienste praktizierten dies laut Strobel. Allerdings sei das Ganze technisch durchaus schwierig. Thomas Dullien von Sabre Security ergänzt: Zwar sei es im Prinzip bei fast jeder heute gängigen Software möglich, unbekannte Schwachstellen zu finden. „Das ist nur eine Frage der Zeit und des Aufwandes“, so der Reverse-Engineering-Experte. Doch Schwarzmarktpreise von mehreren zehntausend Dollar für Exploits (siehe Grafik oben rechts) belegten, dass dies nicht trivial sei.

Laut Professor Hartmut Pohl, Security-Sprecher der Gesellschaft für Informatik, will auch das Bundeskriminalamt bei den geplanten Onlinedurchsuchungen solche Less-than-Zero-Day-Exploits nutzen. Dullien ist jedoch skeptisch: „Wenn das BKA Verwundbarkeiten ausnutzen will, muss es Teams aufstellen, die solche Schwachstellen suchen.“ Doch er bezweifelt, dass man zu Beamtentarifen die nötigen Experten dafür findet.

Zumal das BKA kein Geheimdienst ist, sondern eine deutsche

Polizeibehörde, deren Beamte ohnehin mit dem Tagesgeschäft alle Hände voll zu tun haben, ergänze Behördenkenner. Für die BKA-Beamten seien so genannte Zero-Day-Exploits eher „Science-Fiction“.

Pohl mutmaßt daher, dass sich deutsche Regierungsstellen dabei Hilfe aus dem Ausland holen: „Unternehmen und Behörden sind bereits in der Vergangenheit im Ausland aktiv geworden – so existiert eine hoch qualifizierte Sicherheitsszene in Russland, Israel oder China.“ Aber auch Wirtschaftsspione haben Interesse an unbekanntem Schwachstellen. Pohl: „Solche Less-than-Zero-Day-Exploits werden auch gegen Firmen eingesetzt – weit häufiger, als meist angenommen. Die Schäden durch die damit seit Jahren praktizierten Wirtschaftsspionage dürften extrem hoch sein.“

Eine Sammlung von Links zu weiter führenden Beiträgen zur Problematik finden Sie www.computerzeitung.de/kn31216482.

Computerzeitung.de 10.09.07