

BKA-Beamte mit Zero-Day-Bugs überfordert – Für unbekannte Schwachstellen werden 50 000 bis 100 000 Dollar bezahlt



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

Online-Durchsuchung: Behörden müssen wohl Know-how im Ausland kaufen

Von Armin Barnitzke

04. September 2007

Zur umstrittenen Online-Durchsuchung wollen deutsche Behörden geheime Schwachstellen in Software einsetzen, berichtet die Gesellschaft für Informatik. Solche Hackereinbrüche mit Zero-Day-Exploits sind in der Geheimdienst-Szene gang und gäbe. Sicherheitsexperten bezweifeln jedoch, ob das Bundeskriminalamt dazu überhaupt vom Know-how her in der Lage ist.

Im Prinzip sei es bei fast jeder heute gängigen Software möglich, bislang unbekannte Schwachstellen zu finden, betont der Reverse-Engineering-Experte Thomas Dullien von der Bochumer Sabre Security. „Das ist nur eine Frage der Zeit und des Aufwandes, den man betreiben will.“ Dazu könne man entweder den Source Code nutzen, wenn dieser zugänglich ist, oder man greife auf Reverse-Engineering-Werkzeuge zurück, so Dullien, der für sein Code-Analyse-Tool Bindiff neulich den [deutschen Sicherheitspreis](#) erhalten hat.

Schwarzmarktpreise von um die 50 000 Dollar (siehe Kasten) für einen solchen Exploit dokumentieren für Dullien allerdings, dass dies nicht ganz trivial ist. Doch abgesehen von den Kosten ist auch für die Zero-Day-Bug-Expertin Terri Forslof, Manager Security Response von Tipping Point, klar: [„Wenn jemand dich angreifen will, wird er es schaffen.“](#) Für Dullien ist es daher nahe liegend, dass Nachrichtendienste, deren Job schließlich die Informationssammlung ist, auch Programme auf Schwachstellen analysieren, um damit Daten auf Rechnern zu durchsuchen.

Folgende Preise für Exploits werden laut Charlie Miller in der Szene kolportiert:

- *Bedeutender verlässlicher Exploit: 125 000 Dollar (Quelle Adriel Desautels, Snosoft)*
- *Internet Explorer Exploit 60 000 bis 120 000 (H.D. Moore)*
- *Vista Exploit 50 000 (Raimund Genes, Trend Micro)*
- *WMF Exploit 4000 (Alexander Gostev, Kaspersky)*
- *Security-Firmen wie Tipping Point oder Idefense zahlen unabhängigen Forschern 2000 bis 10000 Dollar, Mozilla belohnt Bug-Finder mit 500 Dollar plus T-Shirt.*

Ähnlich argumentiert Stefan Strobel, Geschäftsführer beim Beratungshaus Cirosec: „Geheimdienste wären ja blöd, wenn sie nicht mit Hackermethoden auf anderen Rechnern einbrechen würden.“ Deutsche Dienste würden das laut Strobel wohl auch praktizieren. Allerdings sei das

Ganze technisch durchaus schwierig.

Laut Professor Hartmut Pohl, IT-Security-Experte der Fachhochschule Bonn-Rhein-Sieg und Datensicherheits-Sprecher der Gesellschaft für Informatik, sollen künftig auch die umstrittenen Online-Durchsuchungen des Bundeskriminalamtes (BKA) durch das Ausnutzen solcher unbekanntem Schwachstellen von statten gehen ([Online-Durchsuchung: Bundesregierung will über eigene geheime Softwarelöcher schnüffeln](#)).

Strobel und Dullien sehen es aber durchaus skeptisch, Geheimdienstansätze auf den Bereich polizeilicher Ermittlungen zu übertragen. Dullien: „Zwar kann man davon ausgehen, dass Nachrichtendienste anderswo auf Rechnern schnüffeln, aber die Polizei hat ganz andere Aufgaben als ein Geheimdienst.“ Zudem äußert er Zweifel, ob die so gefundenen Beweismaterialien überhaupt gerichtsfest sind.

Außerdem: Wenn das BKA Verwundbarkeiten ausnutzen wolle, müsse man Teams aufstellen, die solche Schwachstellen suchen. „Und ist es in Ordnung, dafür Steuergelder auszugeben?“, fragt Dullien rhetorisch. Ganz abgesehen davon, bezweifelt er, dass man für BAT 2A wirklich die notwendigen Experten findet, die sich mit Zero-Day-Exploits auskennen.

Zumal das BKA eben nicht James Bonds Labor, sondern eine deutsche Behörde ist, in der Beamte arbeiten, die ohnehin mit ihrem Tagesgeschäft alle Hände voll zu tun haben. Für diese seien Themen wie Zero-Day-Exploits eher Science-Fiction, die schütteln darüber nur mit dem Kopf, munkeln Behördenkenner.

Auch Pohl glaubt indes nicht, dass das BKA die Zero-Day-Attacks aus eigener Kraft stemmen kann, sondern sich wohl dazu Hilfe aus dem Ausland holt: „Wegen der vergleichsweise geringen Zahl deutscher Informatiker und der naturgemäß noch kleineren Zahl derjenigen, die fähig und willens sind, Sicherheitslücken zu suchen, sind Unternehmen und Behörden in der Vergangenheit auch im Ausland aktiv geworden; so existiert eine hoch qualifizierte Sicherheitsszene in Russland, Israel oder China.“

Doch unabhängig von der deutschen Debatte um die Online-Durchsuchung warnt Pohl, dass gänzlich unbekanntem Schwachstellen (Pohl nennt diese Less-than Zeroday-Exploits) durchaus gegen Firmen eingesetzt werden: „Less-Than-Zero-Day Exploits werden weit häufiger eingesetzt, als gemeinhin angenommen. Die Schäden der damit seit Jahren praktizierten Wirtschaftsspionage dürften extrem hoch sein.“

Ihre immense Bedeutung für die Wirtschaftsspionage werde allerdings bisher nur ausnahmsweise erkannt und es werde nur vereinzelt auf die unveröffentlichten Sicherheitslücken und ihre Ausnutzung durch Kriminelle hingewiesen. „Von den zuständigen Behörden werden sie erstaunlicherweise bisher nicht als Risiko genannt“, kritisiert Pohl.

Bekannt sei, dass Einzelpersonen und Unternehmen zielgerichtet Sicherheitslücken in Programmen suchen – zum Teil auch im Auftrag. Pohl: „Sie verkaufen die programmierten Exploits an Unternehmen und einschlägige Behörden – die sie ebenfalls nutzen und genauso wenig veröffentlichen.“ Für die Weitergabe einer Sicherheitslücke werde bis zu 10 000 Euro im kommerziellen Bereich und für die Erstellung eines

Exploits bis zu 50 000 im kriminellen Bereich bezahlt, so Pohl.

Ähnliche Größenordnungen berichtet Charlie Miller, der früher beim US-Geheimdienst NSA gearbeitet hat und nun als unabhängiger Security-Reseracher sein Geld verdient – und dabei auch versucht, [Zero-Day-Bugs zu Marktpreisen zu veräußern](#). So hat er von US-Behörden für eine Schwachstelle in einem verbreiteten Linux-Daemon zwischen 10 000 und 80 000 Dollar angeboten bekommen. Für 50 000 Dollar hat er den Bug schließlich verkauft.

Insgesamt sei das aber laut Miller ein recht frustrierender Prozess, da es keine zentrale Anlaufstelle für wohlmeinende Bug-Finder gebe sondern diese quasi von Pontius zu Pilatus laufen müssten und noch nicht einmal wüssten, welchen fairen, marktgängigen Preis sie tatsächlich für einen Exploit verlangen könnten. So scheint es kein Wunder, dass der Schwarzmarkt durchaus lockt. Strobel: „An diesem Markt nehmen eben nicht nur die Guten Teil.“

Tipps der Sicherheitsexperten Dullien, Strobel und Pohl, wie sich sich Firmen gegen Spionageeinbrüche über Zero-Day-Bugs schützen können, finden Sie [hier](#):

Thomas Dullien, Sabre Security:

- Weniger Angriffsflächen bieten und zwischen internen und externen Netz trennen.
- Mit einem Penetrationstest simulieren, wie weit ein Angreifer käme, wenn er einen Exploit gegen eine Anwendung einsetzt.
- Microsoft-Kunden sollten Windows Vista einsetzen. Denn bestimmte dort umgesetzte Schutztechniken macht das Schreiben von stabilen Exploits zwar nicht unmöglich, aber aufwändig und damit teuer – und eventuell für den Angreifer uninteressant. Zu den wirkungsvollen Maßnahmen zählt Dullien etwa die zufällige Zuweisung von Adressraum (Address Space Layout Randomization (ASLR)). ASLR sorgt dafür, dass Windows-Vista internen Systemcode stets in verschiedene Speicherbereiche lädt. Hierdurch kann ein Angreifer eventuelle Schwachstellen in diesem Code nicht ohne weiteres nutzen, sondern muss sich die Mühe machen, im Speicher nach dem verwundbaren Code zu suchen. Unter Linux gebe es mit GRSecurity schon lange Patches, die Vista-artige Verteidigungsmassnahmen liefern.
(<http://www.grsecurity.net/index.php>)

Stefan Strobel, Cirosec:

- Host Intrusion Prevention Systeme (HIPS) auf Servern aber auch auf Clients einsetzen. Sie können Bufferoverflows entdecken und unerlaubte Aktionen fremder Programme und Prozesse blockieren.
- Gerade auf Clients kann man zudem mit virtuellen Maschinen arbeiten, um Arbeiten mit sensiblen Daten etwa von Surfen oder E-Mails zu trennen. Selbst wenn der Angreifer etwa eine Browser-Schwachstelle via Exploits ausnutze, könne er quasi nicht aus der virtuellen Maschine ausbrechen. Mit Vmwares Kauf des Security-Spezialisten Detemina dürfte der Angriffschutz etwa gegen Bufferoverflows noch verbessert werden. Für Unternehmen sinnvoll seien dabei auch Vmwares Management-Funktionen wie ACE oder Snapshot.

- Tools zu Information Leakage Prevention (ILP) verhindern zwar den Einbruch nicht, können aber durch Überwachung des Datenverkehrs auf dem Endgerät oder im Netz einschreiten, wenn sensible Daten die Firma verlassen sollen.

Professor Hartmut Pohl, FH Bonn-Rhein-Sieg:

- Verschlüsselung der Daten und Dateinamen macht es einem Angreifer schwerer, weil er auf eine Entschlüsselung im Hauptspeicher warten muss, bis er nutzbare Informationen erhält. Verschlüsselung ist allerdings kein Allheilmittel: Dateisysteme kopieren Dateien aus Sicherheits- und Verwaltungsgründen oftmals auch vor ihrer Verschlüsselung oder nach ihrer Entschlüsselung an mehrere Stellen, die ein Angreifer einsehen kann.

- Die einzige nachhaltig widerstandsfähige Sicherheitsmaßnahme sind Stand-Alone-Systeme, die keinerlei physische Verbindung zum Internet besitzen; sie werden dementsprechend bereits von vielen sicherheitsbewussten Unternehmen zur Verarbeitung ihrer wertvollsten Daten genutzt.

Computerzeitung.de 04.09.07