DuD
Datenschutz und Datensicherheit

Zur Technik der heimlichen Online-Durchsuchung

Hartmut Pohl

Zur Durchführung der (heimlichen) so genannten Online-Durchsuchung existieren eine ganze Reihe falscher Vermutungen wie universell einsetzbare Würmer oder Viren, die der (ebenfalls falsche) Begriff 'Bundestrojaner[1]' suggeriert. Im Folgenden wird das seit drei Jahren von den Behörden praktizierte Verfahren zur Online-Durchsuchung vorgestellt: Less-Than-Zero-Day-Exploits.

Prof. Dr.
Hartmut Pohl

Informationssicherheit, Fachbereich Informatik, Fachhochschule Bonn-Rhein-Sieg

E-Mail: Hartmut.Pohl@fh-brs.de

[1] Erstmals geprägt von Peter Welchering [Kloiber 2007]

1 Ziele der Sicherheitsbehörden

Über kommunizierte Daten hinaus wie das gesprochene Wort, den versandten Brief und die E-Mail (die mit anderen technischen Mitteln zur Kenntnis genommen werden können) wollen Sicherheitsbehörden die nur gespeicherten (und ggf. noch nicht kommunizierten) Daten auswerten wie Kontaktlisten, Planungsdokumente etc. [Ziercke 2007]. Dazu ist ein Zugriff auf die Daten der jeweils genutzten IT-Systeme (Server, PC, Notebook, PDA, Mobiltelefon aber auch LAN und Intranets) in Unternehmen, Behörden und bei Privaten erforderlich. Der Zugriff soll – vom Benutzer des Zielsystems unerkannt – heimlich erfolgen.

Im polizeilichen Bereich (Bundeskriminalamt und Landeskriminalämter) sind zumindest bis zum Frühjahr 2007 keine Online-Durchsuchungen von IT-Systemen durchgeführt worden [Ziercke 2007]; das BKA plant dies jedoch (in Abhängigkeit von einer Novellierung des BKA-Gesetzes) und prüft derzeit die technische Umsetzbarkeit im Rahmen eines Entwicklungsprojektes [Bundestag 2007]. Die ablehnende Entscheidung des Bundesgerichtshofs [BGH 2007] bezieht sich nur auf den Polizeibereich und bemängelt die fehlende Ermächtigungsgrundlage: § 102 StPO gestattet nicht eine auf heimliche Ausführung angelegte Durchsuchung. Zur Verfassungsverträglichkeit der Online-Durchsuchung liegt eine Bewertung vor [Roßnagel 2007].

Seit 2005 sind etwa ein Dutzend verdeckte Online-Durchsuchungen vom Bundesnachrichtendienst durchgeführt worden [ARD 2007]. Neben eigenen Aktivitäten ist der BND auch in der Vergangenheit in Amtshilfe für andere Behörden tätig geworden [Denninger 1980]; als Auftraggeber kommen das Bundesamt für Verfassungsschutz, die Landesämter für Verfassungsschutz, das Amt für den Militärischen Abschirmdienst in Betracht. Etwa ein Viertel der Online-Durchsuchungen dürfte daher diesen anderen Behörden zuzuordnen sein.

2 Relevante Angriffe auf IT-Systeme

Hier soll nicht auf unzureichend abgesicherte IT-Systeme und PC eingegangen werden, auf denen z. B. Bereiche auf Platten und Dienste zur Nutzung durch Dritte aus dem Internet freigegeben sind. Vorausgesetzt werden vielmehr mit Firewalls, Intrusion Detection Systemen und Intrusion Protection Systemen abgesicherte Systeme; Virensuchprogramme, Schutz gegen Spyware und Spamfilter sollen installiert sein. Die folgenden drei Angriffsklassen können dann erfolgreich sein.

2.1 Viren, Würmer und Trojanische Pferde

Schadprogramme wie Viren, Würmer und Trojanische Pferde lassen sich durch sog. Virensuchprogramme erkennen, sofern diese die Schadprogramme kennen. Hersteller von Suchprogrammen untersuchen daher ständig die neu aufgetauchten Schadprogramme und bilden aus ihnen ein spezifisches Bitmuster ('Signatur'), an dem das Virensuchprogramm das Schadprogramm zukünftig erkennen und angemessen behandeln kann (Löschung, Quarantäne etc.). Virensuchprogramme unterschiedlicher Hersteller finden auch unterschiedliche Viren; sicherheitsbewusste Unternehmen setzen daher verschiedene Produkte ein und reduzieren damit das Risiko, von einem diesem Hersteller noch nicht bekannten Schadprogramm erfolgreich attackiert zu werden.

Darüber hinaus werden so genannte heuristische Techniken eingesetzt, um z. B. Manipulationen (Schreibversuche) an entscheidenden (Betriebsystem-)Dateien zu erkennen; daraus kann auf Angriffe geschlossen werden. Beide Techniken sind nicht vollständig, weil Virensuchprogramme

- grundsätzlich nur Schadprogramme erkennen, die sie kennen ('Signatur'),

- eine als Virus-typische Bitfolge auch in einer korrekten/berechtigten Datei vorkommen kann.

2.2 Zero-Day Exploits

Nach dem Stand der Technik enthalten IT-Systeme (hier relevant insbesondere sicherheitsrelevante Programme wie Kommunikationsprotokolle, Kommunikationssoftware, Betriebssysteme und Anwendungssoftware) sicherheitsrelevante Schwachstellen, die ein Eindringen in ein IT-System ermöglichen – unabhängig von bekannten Sicherheitsmaßnahmen wie Firewalls, Virensuchprogrammen, Zugriffskontrolle etc.

Wird eine solche Sicherheitslücke entdeckt, wird sie typischerweise an den betroffenen Produkthersteller gemeldet oder in einschlägigen Foren publiziert [Bugtraq 2007]. Hersteller veröffentlichen Sicherheitslücken zusammen mit einer (nach Bewertung der Lücke) erstellten Fehlerkorrektur (Fix, Patch, Update); Unternehmen [ZDI 2007] und auch Behörden [BSI 2007a] weisen anschließend darauf hin. Z. T. werden die Sicherheitslücken zeitnah nur an 'Vertrauenswürdige' weitergegeben und erst um etwa 45 Tage verzögert veröffentlicht oder noch länger zurückgehalten [CERT/CC[2] 2005]. Einige sicherheitsrelevante Fehler bleiben lange Zeit unkorrigiert. Im Einzelfall wird auch eine Sicherheitslücke vom Hersteller ohne Patch veröffentlicht [Fox 2007]. Ein Verfahrensvorschlag zur Veröffentlichung existiert [Christey 2002]; einige praktizierte Veröffentlichungsstrategien sind veröffentlicht [VulnWatch 2007].

So genannte Zero-Day-Exploits stellen Angriffsprogramme[3] auf veröffentlichte Sicherheitslücken dar, zu denen bereits ein Proof-of-Concept erfolgte; ein solcher Exploit kann bei allen ungepatchten IT-Systemen (in Ermangelung von Gegenmaßnahmen) erfolgreich sein und wird von Angreifern häufig noch am Tag der Veröffentlichung (daher 'Zero Day') eingesetzt in der Hoffnung, noch vor dem Einspielen des Patches erfolgreich angreifen zu können. Zero-Day-Exploits werden zur Online-Durchsuchung grundsätzlich nicht eingesetzt; das Risiko ist groß, dass sie während der Laufzeit einer Online-Durchsuchung gepatcht werden.

Zur Unterstützung der Exploit-Erstellung können zeitsparend Werkzeugkästen eingesetzt werden [Metasploit[4] 2007, Martinez 2007]; als Open-Source-Projekt werden Informationen über Sicherheitslücken angeboten. Das Metasploit Framework bietet ein Werkzeug zur Entwicklung und Ausführung von Exploits gegen Zielsysteme. Eine Einführung mit Literaturhinweisen ist verfügbar [Eidenberg 2006, Wikipedia 2007].

2.3 Less-Than-Zero-Day Exploits

Als Less-Than-Zero-Day-Exploits werden Angriffsprogramme bezeichnet, die bisher unveröffentlichte Sicherheitslücken ausnutzen und dem Hersteller noch nicht bekannt sind. Tatsächlich erkennen oder suchen (auch in Auftrag) Einzelpersonen und Unternehmen [Stone 2007] zielgerichtet Sicherheitslücken in Programmen und verkaufen die programmierten Exploits an ihre Kunden [PandaLab 2007]. Less-Than-Zero-Day-Exploits können grundsätzlich erfolgreich sein, weil sie von Sicherheitssoftware wie Firewalls, Intrusion Detection oder Intrusion Prevention Systemen nicht erkannt werden (können). Signaturen für diese Angriffe liegen nicht vor; die Angriffe sind – genau wie die ausgenutzte Sicherheitslücke – unbekannt.

Einzelpersonen bieten ihr erworbenes Wissen in der Form ablauffähiger Exploits Unternehmen und Behörden gegen Entgelt an und werden auch im Auftrag tätig. Auch Serviceanbieter suchen von sich aus nach Sicherheitslücken in Standardsoftware wie Kommunikationssoftware, Betriebssystemen und auch in Sicherheitssoftware wie Firewalls, Intrusion Detection Systemen [Stone 2007].

Zukünftig wird nicht nur der BND, sondern werden auch die anderen deutschen Sicherheitsbehörden Sicherheitslücken kennen, die sie nicht veröffentlichen, aber ausnutzen. Für den Erwerb einer Sicherheitslücke sollen bis zu $ 10.000 und für die Erstellung eines Exploits zwischen $ 1.000 und 50.000 gezahlt werden. [Heise 2006, Schneier 2007, Stone 2007]. Die Zahl Sicherheitslücken erkennender und Exploits erstellender Spezialisten in der Bundesrepublik dürfte allerdings eng begrenzt sein, so dass die Sicherheitsbehörden auf ausländische Unterstützung einschlägiger Unternehmen angewiesen sind. International wird der Kreis der Spezialisten sehr viel größer eingeschätzt – allein für China werden fünfstellige Zahlen angegeben; dies klingt plausibel, legt man das Verhältnis der Informatik Studierenden in Deutschland und China zugrunde. Relevant sind auch Personen und Unternehmen aus Russland und Israel, weniger aus den USA.

Auch sind Unternehmen bekannt, die Informationen über unveröffentlichte Sicherheitslücken an ihre Kunden verkaufen [iDefense 2007]; es kann davon ausgegangen werden, dass hierunter auch Nachrichtendienste sind. Mindestens seit 2006 existiert ein Markt für Exploits bis hin zur (halb-) öffentlichen Versteigerung [Heise 2006, Wabisabilabi 2007]. Die Bedeutung von Less-Than-Zero-Day-Exploits für die Wirtschaftsspionage wird allerdings nur ausnahmsweise erkannt [BITKOM 2007]; meist wird auf anderweitige Risiken hingewiesen [McAfee 2006].[5] Nur vereinzelt wird abstrakt und unbewertet auf die Existenz unveröffentlichter Sicherheitslücken und ihre Ausnutzung durch Kriminelle Bezug genommen [BSI 2007b, MessageLabs 2007]. Auf zugriffsbeschränkten Blogs und in E-Mail-Verteilern mit hochdynamischen Adressen werden relevante Informationen über Sicherheitslücken und sie ausnutzende Less-Than-Zero-Day-Exploits zwischen Fachleuten weltweit ausgetauscht. Diese Szene bildet Nachwuchs aus und wirbt Jugendliche gezielt mit nachrichtendienstlichen Methoden an [McAfee 2006]. Die Anzahl von Less-Than-Zero-Day-Exploits wird im Einzelfall genannt – so in einem Monat allein für die Office Suite 180 [MessageLabs 2007].

3 Vorgehen bei Online-Durchsuchung

Ziel der Online-Durchsuchung ist in erster Linie, eine Kopie des Inhaltsverzeichnisses von Datenträgern zu erhalten, um die Relevanz der gespeicherten Daten bewerten zu können – in zweiter Linie eine Kopie der relevanten Dateien. Zum Vorgehen vgl. [Ziercke 2007]:

[2] Früher US-CERT United States Computer Emergency Readiness Team.

[3] Ein Beispiel für ein Programm, das eine Sicherheitslücke ausnutzt, ist der Pufferüberlauf, bei dem eigener Code eingeschleust und ausgeführt werden kann (siehe DuD 10/2006).

[4] 'The goal is to provide useful information to people who perform penetration testing, IDS signature development, and exploit research. This site was created to fill the gaps in the information publicly available on various exploitation techniques and to create a useful resource for exploit developers.'

[5] 'Most cybercriminals do not have the skills to discover and exploit software vulnerabilities.'

- Ausspähen des Zielsystems

Voraussetzung ist eine detaillierte Kenntnis der Hardware-/Software-Konfiguration des Zielsystems (‘Umfeldanalyse’) [Telepolis 2007, Schmidt 2007] wie Firewall, Betriebssystem, Virensuchprogramm, Spywareprogramm, jeweils mit Typ, Version, Level, Build, Update etc. Diese Informationen können z. T. auf technischem Wege gewonnen oder dürften per Social Engineering bekannt werden. Sie sind unverzichtbare Voraussetzung für die Erstellung eines Exploits zur Online-Durchsuchung. Exploits für Online-Durchsuchungen stellen jedenfalls (für eine Hardware-/Software-Konfiguration) Individuallösungen dar.

- Starten des Exploits und Eindringen in das Zielsystem

Zur Online-Durchsuchung werden in erster Linie Less-Than-Zero-Day-Exploits eingesetzt.

- Aneignung von Rechten zum Auslesen von Daten und zur Datenübertragung auf dem Zielsystem
- Übertragen von Inhaltsstrukturen

Zugriff auf das Inhaltsverzeichnis der Datenträger und Übertragung (bis auf Dateinamen-Ebene) über das Internet auf einen Speicherserver.

Sofern Datenträger nicht ständig an das Zielsystem angeschlossen sind oder nicht ständig in Schreib-/Lesegeräte eingelegt sind wie CDs, SD-Karten o.ä. muss abgewartet oder sogar ein Trigger gesetzt werden, der das Kopierprogramm startet, wenn ein Datenträger eingelegt ist.

- Inhaltsstruktur analysieren

Die auf dem Speicherserver gespeicherten Daten werden (hinsichtlich Integrität und Vertraulichkeit geschützt) auf portablen Datenträgern gespeichert und offline in der Behörde ausgewertet.

- Aus dem Inhaltsverzeichnis werden die relevanten Dateien ausgewählt und vom Zielrechner kopiert.
- Beenden der Online-Durchsuchung.

Nach erfolgreicher Online-Durchsuchung wird diese abgeschaltet. In bestimmten Fällen kann es aus Sicht der durchsuchenden Behörde sinnvoll sein, sie zu wiederholen oder auch weiterlaufen zu lassen.

Soweit wird also grundsätzlich auf die (ggf. auffallende) Installation eines eigenen Programms auf dem Zielsystem verzichtet – vielmehr werden ausschließlich vorhandene und zum Betrieb des IT-Systems unverzichtbare Systemprogramme genutzt.

- Alternativen bei Fehlschlägen

In seltenen Fällen führt ein Less-Than-Zero-Day-Exploit (aus hier nicht betrachteten Gründen) nicht zum Erfolg. Bei Misserfolg können drei Wege gegangen werden, die allerdings ein (zumindest fahrlässiges) ‘Fehlverhalten’ des Betreibers des Zielsystems voraussetzen und ein erhebliches Erkennungsrisiko bergen:

- Es wird ein individuell entwickeltes ‘Schadprogramm’ wie ein Virus, ein Trojanisches Pferd oder ein Wurm genutzt mit denselben ab Schritt drei dargestellten Zielen. Voraussetzung ist ein ‘Schadprogramm’, das von den auf dem Zielsystem ggf. installierten Sicherheitsprogrammen nicht erkannt wird.
- Dieses ‘Schadprogramm’ wird dem Zielsystem zugeschickt – per Internet oder per Datenträger, bspw. einer CD unter der Legende eines Updates, oder es kann einem vom Zielsystem initiierten Download (vom ISP, oder an ein Software-Update) angehängt werden.[6]
- Gelingt auch dies nicht, wird das ‘Schadprogramm’ händisch auf dem Zielrechner installiert – ein klassisches nachrichtendienstliches Vorgehen.

Nur bei Misserfolg des Exploits wird also mit Hilfe dieser ‘Schadprogramme’ tatsächlich ein Programm auf dem Zielsystem installiert und verdeckt genutzt. Diese Maßnahme birgt das stark erhöhte Risiko der Erkennung: Nutzung eines (auch vorübergehend und endgültig abschaltbaren, möglichst löschbaren) Kopierprogramms für das Inhaltsverzeichnis der genutzten Datenträger und Versand über das Internet. Diese Vorgehensweise führt insgesamt zu einem erhöhten Aufwand. Bei Weitergabe eines Datenträgers (Wechselplatte, USB-Stick, Flash-Speicher o.ä.) mit dem ‘Schadprogramm’ kann nicht ausgeschlossen werden, dass der Datenträger (ggf. vom Zielsystem unbenutzt) an unbeteiligte Dritte weitergegeben und anderweitig eingesetzt wird; dies kann zu einem erhöhten (ungewollten) Datenaufkommen auf dem Speicherserver führen. Nützlich ist ein Monitoring-Programm zur Überwachung des Zielsystems, um bewerten zu können, ob die Online-Durchsuchung bereits erkannt wurde (oder auch von Dritten genutzt wird) und der durchsuchenden Behörde womöglich gefälschte Daten vorgesetzt werden.

Der Begriff ‘Online-Durchsuchung’ ist technisch falsch. Die Online-Schaltung des Zielsystems ist nur eine (notwendige) Voraussetzung. Entscheidend an der Durchsuchung ist, dass sie nicht vor Ort (Hausdurchsuchung) durchgeführt wird. Vielmehr werden unberechtigt kopierte Daten an die durchsuchende Behörde über das Internet übertragen – durchsucht wird also ‚remote’.

Eine Kooperation mit den jeweiligen Software-Herstellern mit dem Ziel, Backdoors zu nutzen, erscheint verzichtbar und sogar kontraproduktiv, weil der Kreis der Eingeweihten stark erweitert würde und eine vielfach bekannte Schnittstelle genutzt wird. Absprachen mit Herstellern werden „dabei nicht angestrebt“ [Bundestag 2007]. Zukünftig muss damit gerechnet werden, dass die Behörden andere – auch bisher unbekannte – Verfahren einsetzen.

4 Grenzen der Online-Durchsuchung

Zu den begrenzenden Faktoren gehört in erster Linie eine restriktive Verbindungspolitik des Zielsystems zum Internet oder physisches Abschalten (z. B. bei Nicht-Nutzung). Weiter wirkt die zur Verfügung stehende Bandbreite des Zielsystems begrenzend; nicht bei allen Zielsystemen kann von einem DSL-Anschluss oder auch nur ISDN ausgegangen werden. Auch sind nicht immer die Platten und der Prozessor auf dem neuesten Stand. Mit den zur Verfügung stehenden Ressourcen (Übertragungskapazität, Rechenzeit, Speicherkapazität) muss daher restriktiv umgegangen werden.

Meldungen und Protokolleinträge sollen bei der Online-Durchsuchung vermieden bzw. rechtzeitig und vollständig gelöscht werden. Virenscanner und Intrusion Detection Systeme erkennen aber in bestimmten Fällen Aktivitäten wie Durchsuchungen oder zumindest die Vorbereitungshandlungen. Um die Online-Durchsuchung vom Zielsystem unbemerkt durchzuführen, können Rootkit-Techniken genutzt werden, die allerdings mit Spezialprogrammen erkannt [Bachfeld 2005] und abgeschaltet werden können [Bager 2007]; ggf. werden auch Teile des Betriebssystems wie der Kernel ausgetauscht, um unerkannt zu bleiben.

Keineswegs kann aber ausgeschlossen werden, dass die Online-Durchsuchung auf dem Zielsystem erkannt wird – ggf. auch ohne dies selbst bei der Online-Durchsuchung erkennen zu können. Werden auf dem Zielsystem z. B. nicht-selbsterklärende Dateinamen benutzt, müssen die Dateien zeitaufwändig inhaltlich untersucht werden.

[6] Z. B. kann ein Download-Manager über die erwünschten Daten hinaus noch das Durchsuchungsprogramm auf dem anfordernden Ziel-System speichern.

Das erfordert mehr Übertragungskapazität. Allerdings lassen sich zeitsparend die Thesauri von Suchprogrammen auf den Zielsystemen auswerten.

Der Speicherserver muss hochgradig geschützt werden. Identifizierung des Speicherservers und Rückverfolgung und Kompromittierung der durchsuchenden Behörde müssen erschwert werden – z. B. durch Nutzung einer nicht näher identifizierbaren dynamischen IP-Adresse im Ausland, Server Hopping und physischem Abschalten bei Nicht-Nutzung – der Sleep-Modus wäre unzureichend.

Gleichwohl könnte der Speicherserver identifiziert, selbst angegriffen und durchsucht werden. Um Folgeschäden zu vermeiden, wird der Server keinerlei weitere Netzanschlüsse besitzen. Vielmehr werden die kopierten Daten auf einem nur einmal beschreibbaren und auf diesem System nicht lesbaren Datenträger gespeichert; die Daten werden dann (zeitaufwändig) offline ausgewertet. Das Risiko der erfolgreichen Platzierung eines Überwachungsprogramms auf dem Speicherserver durch einen Angreifer kann aber nicht ausgeschlossen werden.

Es kann auch nicht ausgeschlossen werden, dass der Exploit – wie jede andere Software auch – insbesondere sicherheitsrelevante Fehler enthält und sich dadurch auf dem Zielsystem bemerkbar macht, die Adresse des Speicherservers kompromittiert wird etc. Derartige Fehler dürften kaum von den durchsuchenden Behörden vollständig getestet und vermieden werden können.

Wird die dem Exploit zugrunde liegende Sicherheitslücke bekannt, muss (wiederum aufwändig) eine andere für einen Exploit genutzt werden. Im Einzelfall bleiben jedoch selbst gravierende veröffentlichte Sicherheitslücken von den Herstellern über ein Jahr ungepatcht; dazu werden von Beratungsunternehmen vorübergehende Sicherheitsmaßnahmen angeboten. Die Lebensdauer unveröffentlichter Sicherheitslücken dürfte bei bis zu vier Jahren liegen.

Voraussetzung für die Online-Durchsuchung ist, dass das Zielsystem mit den gesuchten Datenträgern online ist. Stand-Alone-Systeme können naturgemäß nicht online durchsucht werden. Alle Nutzer eines online durchsuchten IT-Systems sind betroffen – bei mehreren Nutzern besteht allerdings auch ein erhöhtes Risiko, den aktiven Exploit zu erkennen. Bei polizeilichen Online-Durchsuchungen ist eine sorgfältige forensische Behandlung [Hansen 2007] der übertragenen Daten unverzichtbar [Bundestag 2007].

Aus dieser (nicht vollständigen) Auflistung von Herausforderungen wird deutlich, dass Online-Durchsuchungen sehr ressourcenaufwändig sind [Ziercke 2007] und in Abhängigkeit vom Sicherheitsniveau des Zielsystems nicht immer gelingen.

5 Risiken für Unternehmen und Private

Mit Less-Than-Zero-Day-Exploits können auch hoch abgesicherte IT-Systeme erfolgreich angegriffen werden. Durch die Veröffentlichung von Patches entsteht bei den Adressaten der falsche Eindruck, alle (!) Sicherheitslücken würden veröffentlicht. Hier müssen Sicherheitsunternehmen und Behörden gegensteuern und die breite Öffentlichkeit sensibilisieren.

Auf dem Zielsystem vom Benutzer gelöschte Dateien können bei der Online-Durchsuchung ausgelesen werden, da Dateisysteme Kopien von Dateien unter verschiedenen Adressen ablegen, die dem Anwender nicht bekannt sind [BfDI 2007, Bremer 2003]. Bei der Online-Durchsuchung können abgeschaltete Geräte eingeschaltet werden wie z. B. angeschlossene Mikrofone und Kameras.

Von Behörden eingeschleuste Programme können von Dritten wie Nachrichtendiensten, Konkurrenzunternehmen etc. missbraucht werden und z. B. IT-Systeme für den Zugriff Unberechtigter vollständig öffnen – z. B. für Bot-Netze [Kossel 2007]. Der gesamte Internetverkehr (inklusive der E-Mails) kann auch umgeleitet werden [Ramzan 2007]. Einem US-Offizier wurden – gerichtsfest auch technisch nachgewiesen – anlässlich einer Online-Durchsuchung strafrechtlich relevante (kinderpornographische) Daten untergeschoben; in Deutschland ist ein derartiger Vorfall nicht bekannt geworden [Ziercke 2007].

Die Schäden mit der seit Jahren mit Less-Than-Zero-Day-Exploits praktizierten Wirtschaftsspionage dürften extrem hoch sein. Beispielhaft soll hier nur auf einen wohl auf Less-Than-Zero-Day-Exploits basierenden veröffentlichten Spionagefall in Israel hingewiesen werden [Heise 2005].

6 Mögliche Schutzmaßnahmen

Über die o.g. Sicherheitsmaßnahmen hinaus sind die folgenden Maßnahmen möglich.

Mit Honeypot-Systemen und –Netzen [Stevens 2004] kann versucht werden, als berechtigt deklarierte Prozesse als unberechtigte zu erkennen. Verschlüsselung der Daten und Dateinamen macht es einem Durchsuchenden schon schwerer, weil er auf eine Entschlüsselung im Hauptspeicher warten muss, bis er nutzbare Informationen erhält oder einen Key-Logger installieren muss, der Informationen wie Schlüssel, Passworte etc. mitschneidet. Der Durchsuchende kann verschlüsselte Daten downloaden und versuchen, sie zu entschlüsseln. Verschlüsselung ist allerdings – entgegen weit verbreiteter Ansicht – kein Allheilmittel, weil sich noch unverschlüsselte Kopien der Dateien an anderen Stellen des Datenträgers befinden können.

Die einzige widerstandsfähige Sicherheitsmaßnahme ist ein Stand-Alone-System, das keinerlei physische Verbindung (auch nicht über andere IT-Systeme, Netze und z. B. Modems) zum Intranet, Extranet oder Internet hat. Stand-Alone-Systeme werden dementsprechend bereits von vielen sicherheitsbewussten Unternehmen zur Verarbeitung ihrer wertvollsten Daten genutzt. Es muss davon ausgegangen werden, dass dies auch für einige der Zielsysteme von Online-Durchsuchungen gilt.

Fazit

Der durch die Verheimlichung von Less-Than-Zero-Day-Exploits entstehende Vertrauensschaden in die Sicherheit des Internet dürfte beim Bürger groß sein und die Unsicherheit des Bürgers gegenüber den verheimlichenden Behörden und gegenüber dem Internet stark ansteigen.

Online-Durchsuchungen mit Less-Than-Zero-Day-Exploits erfordern einen erheblichen Aufwand und sind äußerst kostenträchtig. Sie werden bereits seit Jahren vom BND praktiziert – die Anzahl beträgt derzeit etwa vier bis fünf pro Jahr mit steigender Tendenz. Less-Than-Zero-Day-Exploits werden unkontrollierbar an jedermann weltweit verkauft, so dass damit u. a. Wirtschaftsspionage gegen deutsche Unternehmen betrieben werden kann [Bundestag 2007]. Die derzeitige Verheimlichung von Sicherheitslücken und Less-Than-Zero-Day-Exploits durch deutsche Behörden schädigt Unternehmen und Private: Die Behörden erwerben Exploits gegen (hohes) Entgelt und ‚züchten' durch die intensive finanzielle Förderung eine Szene heran. Gleichzeitig ist der Bundesinnenminister für den ‚Nationalen Plan zum Schutz der In-

formationsinfrastrukturen' zuständig [BMI 2005].

Der für die Innere Sicherheit der Bundesrepublik verantwortliche Innenminister und der Wirtschaftsminister sind im Gegensatz verpflichtet, deutsche Unternehmen und alle Bürger vor den Risiken von Less-Than-Zero-Day-Attacks deutlich zu warnen. Alle den Behörden bekannt gewordenen Sicherheitslücken in IT-Systemen und damit auch die darauf aufbauenden Less-Than-Zero-Day-Exploits müssen unverzüglich veröffentlicht werden.

Der Gesetzgeber hat im § 202c des StGB [Bundesrat 2006] Vorbereitungshandlungen zum Ausspähen von Daten unter Strafe gestellt – angefangen mit der Herstellung über den Vertrieb bis hin zur Überlassung entsprechender Programme. Da die Strafbarkeit vom Zweck des Tools abhängt und nicht von den Zielen oder Aktivitäten der Handelnden [GI 2007], machen sich alle (Unternehmen, Mitarbeiter, Ausbilder, Professoren, Studierende) strafbar, die sich mit Sicherheitsverfahren wie Less-Than-Zero-Day-Exploits befassen.

Hier entsteht der Eindruck, dass z. B. Online-Durchsuchungen nicht erkannt werden sollen. Damit ist ausländischer Wirtschaftsspionage zum Schaden der deutschen Unternehmen Tür und Tor geöffnet.

Literatur

[ARD 2007] ARD (Hrsg.): Rund ein Dutzend Mal wurde geschnüffelt. 27.04.2007

[Bachfeld 2005] Bachfeld, D.: Kostenloser Spürhund. Rootkit-Revealer spürt Hintertüren auf. Heise Hannover 2005 http://www.heise.de/security/artikel/58158

[Bager 2007] Bager, J.; Bleich, H.: Mail-Infarkt. c't 2, 80 ff. 2007

[BfDI 2007] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Hrsg.): 21. Tätigkeitsbericht 2005-2006. Bonn 2007

[BGH 2007] Bundesgerichtshof (Hrsg.): Verdeckte Online-Durchsuchung unzulässig. Karlsruhe 2007 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38775&pos=0&anz=16

[BITKOM 2007] BITKOM (Hrsg.): Deutsche ITK-Wirtschaft lehnt Online-Durchsuchung ab. Hacker-Schnittstelle für Ermittler würde Nutzer verunsichern. BITKOM befürchtet Nachteile für Software-Anbieter. http://www.bitkom.org/de/presse/8477_47376.aspx

[BMI 2005] Bundesministerium des Innern (Hrsg.): Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). Berlin 2005

[Bremer 2003] Bremer, L.; Vahldiek, A.: Auf Nimmerwiedersehen. Dateien richtig löschen. c't 5, 192ff. 2003

[BSI 2007a] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Hinweise zum Schutz vor Computer-Viren. Bonn 2007 http://www.bsi.bund.de/av/HinweiseCV.htm

[BSI 2007b] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2007. Bonn 2007 http://www.bsi.de/literat/lagebericht/index.htm

[Bugtraq 2007] BugTraq Archive http://www.securityfocus.com/archive

[Bundesrat 2006] Bundesrat: Drucksache 676/06 Gesetzentwurf der Bundesregierung: Entwurf eines ... Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität. Berlin 2006. http://dip.bundestag.de/brd/2006/0676-06.pdf

[Bundestag 2007] Deutscher Bundestag: Drucksache 16/4997, 16. Wahlperiode. Kleine Anfrage der Abgeordneten Gisela Piltz et al.: Online-Durchsuchungen. Berlin 2007

[CERT/CC 2005] http://www.cert.org

[Christey 2002] Christey, S.; Wysopal, C.: Responsible Vulnerability Disclosure Process. Internet-Draft. MITRE Bedford 2002

[Denninger 1980] Denninger, E.: Einführung in Probleme des Amtshilferechts, insbesondere im Sicherheitsbereich. Juristische Arbeitsblätter, 280 ff. 1980

[Eidenberg 2006] Eidenberg, A.: Exploits für alle. Heise Security 06.01.2006 http://www.heise.de/security/artikel/67984/

[Fox 2007] Fox, D. (Hsg.): Secorvo Security News Juli 2007. Karlsruhe 2007 http://www.secorvo.de/security-news/secorvo-ssn0707.pdf

[GI 2007] Gesellschaft für Informatik (Hrsg.): Entwurfsfassung des § 202c StGB droht Informatiker/innen zu kriminalisieren. http://www.gi-ev.de/presse/pressemitteilungen-2007/pressemitteilung-vom-3-juli-2007/

[Hansen 2007] Hansen, M.; Pfitzmann, A.: Online-Durchsuchung. Deutsche Richterzeitung 8, 225 ff. 2007

[Heise 2005] Heise (Hrsg.): Trojaner spioniert israelische Unternehmen aus. Hannover 2005 http://www.heise.de/security/news/meldung/60056

[Heise 2006] Heise (Hrsg.): Untergrundauktionen: Vista-Exploit 20.000 $, eBay-Konto 7 $. Hannover 2006 http://www.heise.de/security/news/meldung/82679

[iDefense 2007] iDefense (Ed.): Welcome to iDefense Labs. Sterling Va. 2007 http://labs.idefense.com/

[Kloiber 2007] Kloiber, M.: Rote Karte für Bundes-Hacker. Köln 2007 http://www.dradio.de/dlf/sendungen/forschak/590376/

[Kossel 2007] Kossel, A.; Kötter, M.: Piraten-Software. c't 2, 76ff. 2007

[Martinez 2007] Martinez, V.: PandaLabs Report: Mpack uncovered. O.O. 2007 http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares

[McAfee 2006] McAfee (Hrsg.): Virtual Criminology Report. North American Study into Organized Crime and the Internet. Hamburg 2006 http://www.mcafee.com/de/about/press/corporate/2006/20061208_124141_v.html

[MessageLabs 2007] MessageLabs (Ed.): Intelligence Special Report: Targeted Attacks. April 2007.

[Metasploit 2007] Metasploit (Ed.): Bustin shells since 2003 http://www.metasploit.com/

[PandaLab 2007] Homepage PandaLab http://www.pandasoftware.com/

[Ramzan 2007] Ramzan, Z.: Drive-by Pharming Threat. O.O. 2007 http://seclists.org/bugtraq/2007/Feb/0285.html

[Roßnagel 2007] Roßnagel, A.: Verfassungspolitische und verfassungsrechtlich Fragen der Online-Durchsuchung. Deutsche Richterzeitung, 227-230, August 2007

[Schmidt 2007] Schmidt, J.: Die Super-Trojaner. c't 2, 86ff. 2007

[Schneier 2007] Schneier, B.: Business Models for Discovering Security Vulnerabilities. Mountain View 2007 http://www.schneier.com/blog/archives/2007/02/business_models.html

[Stevens 2004] Stevens, R.; Pohl, H.: Honeypots und Honeynets. Informatik Spektrum 27, 3, 260 ff. 2004

[Stone 2007] Stone, B.: Moscow company scrutinizes computer code for flaws. International Herald Tribune, 01-29-07 http://www.iht.com/articles/2007/01/29/business/bugs.php

[Telepolis 2007] Telepolis (Hrsg.): Die Vaporware des BKA. Hannover 2007 http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/24/24678/1.html&words=Vaporware&T=Vaporware

[VulnWatch 2007] Homepage VulnWatch http://www.vulnwatch.org/index.html

[Wabisabilabi 2007] Wabisabilabi (Ed.): Closer to zero risk. London 2007

[Wikipedia 2007] Wikipedia (Hrsg.): Metasploit. O.O. 2007 http://de.wikipedia.org/wiki/Metasploit

[ZDI 2007] Zero Day Initiative (Ed.): Published ZDI Advisories. Austin 2007 http://www.zerodayinitiative.com/advisories.html

[Ziercke 2007] Ziercke, J.: Zu 'Technische und rechtliche Herausforderungen der Entwicklung'. In: Bündnis 90/Die Grünen Bundestagsfraktion (Hrsg.): Bürgerrechtsschutz im digitalen Zeitalter. Berlin 2007