secorvo
security consulting

Secorvo Security News

August 2008

Editorial: Vom Urteilen

Ein Urteil, so die eingängige Definition in Wikipedia, ist „eine wertende Entscheidung über einen Sachverhalt oder Erkenntnisgegenstand". Entscheidungen zwischen alternativen Bewertungsmöglichkeiten treffen wir ständig – mit mehr oder weniger guter Kenntnis der Zusammenhänge. Viele unserer Urteile sind daher genau besehen Vorurteile, also eine „im Allgemeinen wenig reflektierte Meinung – ohne vollständige Würdigung aller relevanten Eigenschaften eines gewerteten Sachverhalts oder einer Person". Vorurteile sind voreilige Urteile, sie verallgemeinern ohne Berücksichtigung des Einzelfalls.

Das ist nicht notwendig schlecht und manchmal überlebenswichtig. Für viele unserer wertenden Entscheidungen steht uns zu wenig Zeit zur Verfügung, um den Sachverhalt angemessen zu analysieren. Vorurteile geben eine (erste) Orientierung und erlauben sofortiges Handeln. Dabei müssen wir uns aber bewusst machen, dass das Vorurteil nur ein vorläufiges Urteil sein kann, das durch zusätzliche Informationen oder Erkenntnisse in ein reiferes münden sollte.

Die „vollständige Würdigung aller relevanten Eigenschaften" erfordert Disziplin, Zeit und die Offenheit für die Revision eines (Fehl-)Urteils. Daher wurde für Urteile mit besonderer Tragweite für Betroffene das Amt des Richters geschaffen und die Möglichkeit zur Revision institutionalisiert. Im Finanzwesen ist derzeit jedoch ein Trend zur vermeintlichen Objektivierung von z. B. Kreditentscheidungen durch den Rückgriff auf personenbezogene Informationen Dritter zu beobachten, verschleiernd „Rating" genannt. Verständlich vielleicht, dass ein Online-Anbieter nicht gegenüber einem notorischen Zahlungsverweigerer in Vorleistung gehen möchte. Aber soll eine Bank die Kreditbedingungen verschärfen dürfen, weil ein direkter Verwandter des Kunden Privatinsolvenz angemeldet hat? Oder einen Kredit verweigern, weil der Kunde in einem schlecht beleumundeten Viertel wohnt? Da fehlt nicht viel, und aus „automatisierten Einzelentscheidungen" werden nicht-revidierbare Vorurteile – und damit gesamtgesellschaftliche Freiheitsbegrenzer.

Inhalt

secorvo
security consulting

Security News

Rutkowska strikes again

Die auf virtuelle Rootkits spezialisierte Forscherin Joanna Rutkowska hat wieder zugeschlagen: Auf der diesjährigen Blackhat stellte sie am 07.08.2008 mit ihren Kollegen Rafal Wojtczuk und Alexander Tershkin vor, wie man den Hypervisor der Virtualisierung Xen mit Rootkits trojanisieren kann. Die technischen Details sind anspruchsvoll und interessant: Der modifizierte Code wird dem bereits laufenden Hypervisor über eine Netzwerkkartentreiber-Software oder den Festplattencontroller untergeschoben und im laufenden Betrieb über Direct Memory Access (DMA) zur Ausführung gebracht.

Wie bereits bei ihrem 2006 vorgestellten Rootkit BluePill (siehe SSN 8/06), das die Virtualisierungsfunktionen von AMD-Prozessoren nutzt, ist die Erkennung dieser Angriffssoftware sehr schwierig. Derzeit entwickeln Rutkowska und ihre Kollegen im Projekt HyperGuard die BIOS-Funktionen von Mainboards weiter, um einen Integritätsschutz der Hypervisor-Software zu ermöglichen – damit wäre wirksame Abhilfe möglich.

Schwachstellen-Primus Browser

In einer am 14.08.2008 vom Deutschen Sicherheitsnetz e.V. vorgestellten Untersuchung wurde festgestellt, dass von 253 geprüften privaten PC-Systemen gut die Hälfte Browserschwachstellen aufwies. Deutlich repräsentativer, aber im Ergebnis vergleichbar sind die am 10.08.2008 vorgestellten Ergebnisse einer von der ETH Zürich gemeinsam mit Google und IBM durchgeführten Studie: Von ca. 1,4 Milliarden PCs setzten danach 45,2 % nicht die aktuellen Versionen der jeweiligen Browser ein.

Je nach Art der Schwachstelle reicht es aus, eine entsprechend präparierte Website zu besuchen, um im schlimmsten Fall einem Angreifer die vollständige Kontrolle über das System zu überlassen. In der Tat tauchen – wie beispielsweise eine von Google am 30.07.2008 vorgestellte Studie zeigt – gerade vor Großereignissen wie den olympischen Spielen immer wieder zahlreiche manipulierte Webseiten auf, deren Besuch mit anfälligen Browsern zur Kompromittierung des Systems führen kann.

Dabei ist zu beachten, dass die Schwachstellen nicht nur die Kernkomponenten des Browsers, sondern in vielen Fällen auch Erweiterungen wie Java, Flash und Quicktime betreffen. Diese Komponenten werden gelegentlich beim Patch-Management übersehen. Eine Überprüfung der Aktualität eigener Browser-Erweiterungen und die Suche nach weiteren Schwachstellen kann bei Secunia online erfolgen. Empfehlenswert sind auch die Browserchecks vom Deutschen Sicherheitsnetz und Heise online.

Phalanx2-Rootkit

Das DFN-CERT warnte am 04.08.2008 vor einer neuen Version des bereits seit 2005 bekannten Linux-Rootkits „Phalanx“, welches in aktuellen Angriffen aus dem Internet beobachtet wurde. Phalanx2 manipuliert dabei – wie andere Rootkits auch – bestimmte Systemdateien, um sich vor Benutzer und Administrator zu verstecken. Die Infektion des Systems erfolgt überwiegend über gestohlene SSH-Schlüssel.

Linux-Administratoren sollten demnach kurzfristig überprüfen, ob ihre Systeme betroffen sind: Das DFN-CERT stellt in dem entsprechenden Security Advisory ein einfaches Shell-Skript zur Verfügung, welches nach Phalanx2-Spuren sucht.

Update legt ESX-Server lahm

Wer der Überzeugung ist, seine Sicherheit durch den Einsatz von Virtualisierung automatisch gesteigert zu haben, ist einem populären Irrglauben erlegen. Zwar kann beispielsweise durch den Einsatz von VMware ESX Server die Verfügbarkeit von Serversystemen erhöht werden. Damit handelt man sich jedoch auch zusätzliche Risiken ein. So führte ein Update für ESX in den Versionen 3.5/3.5i vom 12.08.2008 dazu, dass virtuelle Systeme auf dem ESX Server nicht mehr gestartet werden konnten. Kritisch ist dabei, dass von ESX-Fehlfunktionen unvermeidlich zahlreiche virtualisierte Serversysteme betroffen sein können. Schlimmstenfalls können komplette Serverlandschaften ausfallen.

Das Beispiel zeigt, dass bei der Einführung von Virtualisierung die damit verbundenen Risiken zu betrachten sind und – wie bei jeder kritischen Komponente einer Infrastruktur – ein besonderes Augenmerk auf den Patch-Prozess gelegt werden muss.

Eisspray gegen Krypto-Schlüssel

Dass die Inhalte des Hauptspeichers (RAM) weniger flüchtig sind als lange Zeit angenommen, weiß man aufgrund forensischer Analysen bereits seit einiger Zeit: Je nach betroffener Hardware-Betriebssystem-Kombination „überleben“ große Mengen interessanter Daten sogar das (mehrfache) Booten des Rechners.

Forscher aus Princeton, die ihre (vorab schon am 21.02.2008 unter anderem als Film in YouTube publizierten) Ergebnisse am 30.07.2008 auf dem diesjährigen USENIX Security Symposium präsentierten, gingen noch einige Schritte weiter. So fanden sie heraus, dass sich auch mehr als 60 Sekunden nach dem kompletten Ausschalten des Rechners Inhalte

aus bestimmten DRAM-Speicherchips größtenteils rekonstruieren lassen. „Behandelten“ sie die Speicherriegel eines Laptops zusätzlich mit Eisspray, bevor sie den Rechner ausschalteten, und bauten sie die gekühlten RAM-Bausteine in ein anderes Laptop ein, so konnten sie auch noch nach mehreren Minuten ohne Strom problemlos auf sämtliche RAM-Inhalte zugreifen.

Spektakulärer wird dieser Angriff durch die Tatsache, dass die Forscher zeitgleich Algorithmen und Tools zum Auffinden kryptographischer RSA- sowie AES-Schlüssel entwickelten: Mit deren Hilfe muss auf der Suche nach BitLocker-, FileVault-, dm-crypt- oder TrueCrypt-Schlüsseln nicht mehr der komplette Speicherinhalt manuell „durchstöbert“ werden. Vielleicht sollten Laptop-Nutzer zukünftig ein Wärmepflaster als Zubehör mit sich führen.

Verflüchtigung 1.3

Die künstliche Verlängerung der Flüchtigkeit von RAM-Inhalten könnte zukünftig auch bei forensischen Analysen interessant werden, da die Untersuchung des Hauptspeichers im Rahmen so genannter „Live-Analysen“ immer wichtiger wird. Längst spielt die dynamische Analyse in vielen Forensik-Projekten eine größere Rolle als die rein statische. Anzahl und Qualität der entsprechenden Tools zur Untersuchung des Hauptspeichers hielten sich bislang jedoch in Grenzen – viele Tools besaßen diesbezüglich nur rudimentäre Funktionen.

Die am 14.08.2008 erschienene neue Version der Tool-Sammlung Volatility – von ihren Entwicklern als v1.3_Beta bezeichnet – ist eine sehr mächtige, aus der Open-Source-Welt stammende kostenlose Software für Live-Analysen. Sie unterstützt Speicherdumps von Windows XP (SP2 und SP3) sowie ansatzweise Linux, kann die laufenden Prozesse anzeigen, Binaries extrahieren und offene Netzwerkverbindungen auflisten. Sie darf in keinem forensischen Werkzeugkasten fehlen.

Secorvo News

Secorvo College aktuell

Für die nächste T.I.S.P.-Schulung in der zweiten Septemberwoche (**08.–12.09.2008**) mit anschließender Zertifikats-Prüfung durch iSQI gibt es nur noch wenige freie Plätze, und auch unser „aktueller Klassiker“ mit umfangreichem Demo- und Praxisteil, das Seminar PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008**, erfreut sich großer Nachfrage – baldige Anmeldung empfohlen. Im Oktober folgen das Grundlagenseminar IT-Sicherheit heute am **07.–10.10.2008** und IT-Sicherheitsaudits in der Praxis am **28.–30.10.2008**. Termine, Programme und Online-Anmeldung unter http://www.secorvo.de/college

Symposium Wirtschaftsspionage

Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu. Angesichts dieser besorgniserregenden Entwicklung führen wir gemeinsam mit dem Wirtschaftsmagazin Econo am **03.09.2008** ein eintägiges Symposium zur "Wirtschaftsspionage" durch. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, für das wir zahlreiche Fachexperten wie Dr. Udo Ulfkotte und Unternehmensvertreter gewinnen konnten, die die tatsächliche Bedrohungslage analysieren und Schutzmaßnahmen vorstellen. Mit voraussichtlich über 70 Teilnehmern verspricht auch das Auditorium spannende Diskussionen. Für Schnellentschlossene gibt es noch freie Plätze (Programm, Online-Anmeldung und Anfahrtskizze).

Gut gemeint

Was ist ein "gutes" Passwort? Verbessern die verbreiteten Komplexitätsanforderungen tatsächlich die Güte gewählter Passworte? Und wie lässt sich verhindern, dass die Passworte notiert oder weitergegeben werden? Auf diese Fragen gibt eine aktuelle Untersuchung überraschende Antworten, die Thomas Maus auf dem nächsten Event der Karlsruher IT-Sicherheitsinitiative am 25.09.2008 im Schlosshotel Karlsruhe vorstellen wird. Er räumt mit einigen liebgewonnenen "Glaubenssätzen" auf und legt ein Umdenken im Umgang mit Passworten nahe. Anmeldung und weitere Informationen unter http://www.ka-it-si.de.

10 Jahre weiser

In wenigen Tagen, am 01.09.2008, wird Secorvo zehn Jahre alt. Dann werden über 550 herausfordernde Projekte, mehr als 200 veröffentlichte Aufsätze, über 70 Ausgaben der "Security News" und mehrere hundert Seminare, Symposien und Vortragsveranstaltungen hinter uns liegen. Dass wir die Chance hatten, über einen solchen - im IT-Zeitalter geradezu astronomisch langen – Zeitraum die IT-Sicherheit und den Datenschutz in Deutschland mitzugestalten, verdanken wir nicht zuletzt unseren Kunden: Deren Vertrauen in unsere Arbeit, die fruchtbare Zusammenarbeit und wohl auch die eine oder andere Empfehlung waren wesentliche Voraussetzung für diesen Erfolg.

Auch bei unseren treuen Lesern der Security News möchten wir uns bei dieser Gelegenheit bedanken. Die monatlich mehreren tausend Abrufe der News sind eine wichtige Motivation für unsere Arbeit. Und falls Sie uns schon immer einmal ein Lob aussprechen wollten – anlässlich unseres runden Geburtstags würde uns das besonders freuen.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
07.-10.09.	OSS 2008 – 1st Workshop on Open Source Software for Computer and Network Forensics (IFIP, Milano/IT)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008 – 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik - Verfahren, Tools, Praxis (Secorvo College)

Fundsache

Die Kryptoanalyse mathematischer Algorithmen ist seit vielen Jahrhunderten eine anspruchsvolle Wissenschaft. Zahlreiche Fachbücher existieren zu diesem Thema; nicht immer sind die Erläuterungen aber für Einsteiger verständlich. Der Google-Mitarbeiter Mark Chu-Carroll hat am 15.08.2008 in seinem Blog eine sehr informative Einführung in die Kryptoanalyse „zum Nachmachen" gegeben – auch die Kommentare sind lesenswert.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de