secorvo
security consulting

Secorvo Security News

April 2008

Editorial: „(T)Räumst du noch oder identifizierst du schon?“

Kontaktlose Chipkarten haben sich inzwischen auch in mittelständischen Unternehmen als Betriebsausweis durchgesetzt. Sie dienen als bargeldloses Zahlungsmittel im Betriebsrestaurant, regeln den Gebäudezugang und vereinfachen die Zeiterfassung. Von einer ähnlichen Infrastruktur träumt auch die IT: Gesteuert durch aktuelle HR-Prozesse (Eintritt, Austritt, interner Wechsel etc.) ließen sich Zugriffsrechte für zentrale Systeme und kryptographische Schlüssel (VPN-Einwahl, E-Mail- und Festplattenverschlüsselung) automatisch vergeben und wieder entziehen – abhängig von Aufgabe und Stellenbeschreibung, mit striktem Freigabeprozess nach dem Need-to-Know-Prinzip. Schließlich kann der Ausweis als Single-Sign-On-Token leidige Mehrfach-Logins ablösen.

Der Sicherheitsgewinn wäre erheblich – keine „vagabundierenden“ Accounts mehr, Schluss mit notierten, weitergegebenen oder trivialen Passworten, Ende der „Rechteakkumulation“ bei Mitarbeitern, die häufig den Zuständigkeitsbereich wechseln. Administrationsprozesse würden einfach, Hotline-Anrufe zur Passwortrücksetzung entfallen. Die subjektive Wahrnehmung von Sicherheitsmechanismen als Arbeitsbehinderung wäre endlich Geschichte.

Technisch ist dies keine Zauberei mehr. In der Praxis sind zuvor jedoch ein paar Aufräumarbeiten zu erledigen, die schon in mittelgroßen Unternehmen wie die Reinigung des Augiasstalls anmuten: So müssen Rechte in Rollen verdichtet, Freigabeprozesse etabliert und HR-Daten konsolidiert werden. Die Bewältigung dieser Herausforderungen, die ohne höchsten Management-Support nicht gelingen kann, lohnt jedoch – das zeigten die Vorträge und Diskussionen auf dem ersten „Identity Management Symposium“ in Ettlingen: Wer Ordnung schafft, gewinnt – Geld, Überblick und Sicherheit.

Wer beim Schachspiel nicht einmal die Figuren in Ordnung zu stellen weiß,
der wird es schlecht zu spielen verstehen; und wer nicht Schach bieten kann,
der wird auch nie schachmatt setzen können." - *Theresa von Ávila*

Inhalt

secorvo
security consulting

Security News

Online-Durchsuchung in der EU

Am 09.04.2008 hat die 42köpfige interministerielle Arbeitsgruppe „Online-Durchsuchung“ des österreichischen BMJ/BMI ihren Schlussbericht zur Online-Durchsuchung vorgelegt. In dem knapp 100seitigen Dokument kommen die Autoren zu dem Schluss, „dass die geheime Überwachung von privaten Rechnern ein besonders schwer wiegender Eingriff ist“, der unter Gesetzesvorbehalt stehe – und für den es derzeit in Österreich keine Rechtsgrundlage gibt. Der öffentlich gewordene Einsatz einer „Remote Forensik“-Software vom Herbst 2007, bei dem in kurzen Abständen Screenshots eines überwachten Systems an die Strafverfolgungsbehörden gesandt worden waren, wird in einem rechtlichen „Graubereich“ angesiedelt. Lesenswert ist die vergleichende aktuelle Übersicht der Regulierung und des Standes der politischen Diskussion zur Online-Durchsuchung in den Mitgliedsstaaten der EU.

Registry Ripper

Immer öfter erfordert die forensische Analyse von Windows-Rechnern eine zeitaufwändige Untersuchung der Registry (NTUSER.DAT, etc.), da das Betriebssystem dort eine Vielzahl von Aktionen protokolliert, beispielsweise die zuletzt geöffneten Dateien und eine Liste gestarteter Anwendungen, geöffneter Netzwerk-Ports und besuchter Webseiten.

Obwohl nicht nur frei verfügbare Registry-Viewer, sondern auch (fast) alle Forensik-Toolkits detaillierte Auswertungsmöglichkeiten für die Registry bieten, artet die Analyse in der Praxis oft in "Herumgestochere" mit manueller Auswertung bestimmter Registry-Schlüssel aus. Dagegen hilft das am 09.04.2008 veröffentlichte Tool RegRipper (v2.01A vom 20.04.2008): Es wertet die ca. 50 wichtigsten in der Registry vorhandenen Schlüssel aus, kodiert dabei Binärwerte in eine lesbare Form, extrahiert vorhandene Zeitstempel und speichert das Ergebnis in einer effizient weiter zu bearbeitenden Textdatei. Die zu untersuchenden Teilbäume der Registry werden über programmierbare, leicht anpassbare Plugins gesteuert. Das Tool erfordert dabei keine Installation und verfügt neben einer Kommandozeile auch über eine graphische Benutzeroberfläche; außerdem wird der Perl-Quellcode mitgeliefert. Bereits diese vom Autor "Basic edition" genannte Version sollte in keiner forensischen Tool-Sammlung fehlen – der Autor hat bereits angekündigt, an einer stark erweiterten Version zu arbeiten.

Datenschutz international

Im Auftrag der Europäischen Kommission erstellten wik-Consult und RAND Europe eine Gegenüberstellung der Datenschutz-Regulierung in Europa, den USA, Japan, Südkorea, Malaysia und Indien. Die vom 20.07.2007 datierende Endfassung der Studie wurde am 29.02.2008 von der EU-Kommission publiziert.

Bewertet wurden insbesondere der Rechtsschutz, der Grad an Selbstregulierung, die Effektivität, die Rechtsdurchsetzung und das Spannungsverhältnis zu Sicherheitsgesetzen. Die 230seitige Studie basiert auf rund 40 Interviews mit Experten aus unterschiedlichen gesellschaftlichen Bereichen (Unternehmen, Regierungen, Datenschutzbehörden, Juristen und Verbraucherschutzverbänden) und bietet einen guten Überblick der Datenschutz-Gesetzgebung der jeweiligen Länder sowie des dahinter stehenden Regulierungskonzepts.

Voreingestellte WPA-Keys

Am 14.04.2008 veröffentlichte Kevin Devine unter gnucitizen.org den von Britisch Telekom für den WLAN-Router Thompson Speedtouch verwendeten Algorithmus zur Erzeugung der voreingestellten WEP- und WPA-Schlüssel: ein einfacher SHA-1-Hash der hexadezimal dargestellten Seriennummer. Für die WEP-Keys von Netopia-Routern entdeckte und publizierte er das Verfahren schon am 29.09.2007: ein SHA-1-Hash der Seriennummer mit angehängter Textzeile aus „Third Stone From The Sun" von Jimi Hendrix liefert den Schlüssel. Von „James67“ wurde kürzlich auch der Erzeugungsalgorithmus der Default-Keys des Routers Netgear V1 DG834GT gefunden – am 21.02.2008 riet Sky Broadband zum sofortigen Wechsel des WiFi-Keys.

Ursache des Übels, von dem viele weitere WLAN-Router unterschiedlicher Hersteller und vielleicht auch deutsche Provider betroffen sein dürften, sind das fehlende Verständnis für die Wichtigkeit einer *zufälligen* Schlüssel-Wahl – und die Bequemlichkeit der meisten Nutzer, die den voreingestellten Schlüssel nicht wechseln. Dazu raten wir dringend – denn auch wenn der Erzeugungsalgorithmus nicht veröffentlicht ist oder sogar Zufallswerte erzeugt, kennen Hersteller oder Online-Provider den Schlüssel. Damit ist die Kommunikation – auch ohne „Bundestrojaner“ – potentiell Dritten zugänglich.

All Your iFrames Point to Us

Seit mehr als 1,5 Jahren untersucht Google Webseiten auf Malware, die automatisch beim Aufruf der Seite installiert wird. Dabei wurden über drei Millionen unterschiedliche, mit Malware verseuchte URLs auf mehr als 180.000 Webseiten gefunden, wie Niels Provos am 11.02.2008 berichtete. Der

Anteil infizierter Seiten hat sich dabei von April 2007 bis Januar 2008 auf ca. 1,3% verdreifacht; mehr als die Hälfte (über 60%) der Seiten stammt aus China.

Details der zusammen mit der Johns Hopkins University durchgeführten Untersuchung finden sich in einem von Niels Provos veröffentlichten, 22seitigen Technical Report. Besonders lesenswert ist das vom 07.04.2007 datierende (9seitige) Grundlagenpapier The Ghost in the Browser, in dem Provos mit seinen Koautoren an Javascript-Beispielen erläutert, wie Webseiten-Malware arbeitet – und entdeckt werden kann.

Wurm inklusive

Am 03.04.2008 wurde bekannt, dass „USB Floppy Drive Keys" der Firma HP, eine optionale Ergänzung für ca. 40 Modellvarianten der Proliant-Serie, mit zwei Würmern verseucht ausgeliefert worden waren. Bei den Würmern handelte es sich um Fakerecy und SillyFDC, die sich auf alle angeschlossen lokalen und vernetzen Laufwerken verbreiten. Sie waren erstmals Mitte Januar bzw. Ende Februar 2008 aufgetaucht. Über eine Schadfunktion verfügen beide Würmer glücklicherweise nicht, und aktuelle Virenscanner erkennen und beseitigen sie vollständig. Dennoch zeigt der Vorfall, was bei mangelhafter Qualitätssicherung in der Hardwareproduktion drohen kann – erst im September 2007 waren einzelne iPods mit dem Virus RavMon.Exe ausgeliefert worden. Der nächste Wurm kommt bestimmt. Hoffentlich einer, den der Virenscanner erkennt.

Finger-Logger

Nicht erst seit der Ausspähung und Publikation des Fingerabdrucks des Bundesinnenministers durch den Chaos Computer Club Ende März 2008 ist bekannt, dass biometrische Merkmale gefälscht werden können – siehe z.B. den von Matsumoto auf der Eurocrypt 2002 publizierten Beitrag „Gummi Fingers" (SSN 1/2002).

Auf der Blackhat Europe wurde am 04.04.2008 eine exemplarische Analyse für einen biometrischen Scanner nebst Infrastruktur (Türzugang) vorgestellt. Durch eine Man-in-the-Middle-Attacke wurden die Daten aus dem Kommunikationsstrom erfolgreich rekonstruiert, da sie unverschlüsselt übertragen wurden. Die gewonnen Datenschablonen (Position, Datensatz und Fingerfolge) und Bilddaten wurden nach einem bekannten Verfahren zu einem funktionsfähigen Fingerabdruck weiterverarbeitet. Nach Keyloggern, Mini-Videokameras und Skimming-Attrappen müssen wir uns möglicherweise bald auch nach Biodaten-Loggern umschauen.

Vorratsdatenspeicherung

Am 11.3.2008 entschied das Bundesverfassungsgericht im Eilverfahren über die Verfassungsbeschwerde von über 34.000 Beschwerdeführern gegen die mit der Änderung von TKG und StPO eingeführte Vorratsdatenspeicherung. Zwar setzte es nicht – wie von den Beschwerdeführern erhofft – die Speicherung selbst außer Vollzug, sondern verbot befristet bis zum 11.09.2008 lediglich die Datenherausgabe an die Strafverfolgungsbehörden.

Das Gericht verpflichtete die Bundesregierung zur Abfassung eines Berichts über die praktischen Auswirkungen der Sperrung. Damit traf das BVerfG keine Vorentscheidung über die Speicherung, sondern vermied zunächst nur etwaige negative Folgen für die Betroffenen im Falle einer späteren Feststellung der Verfassungswidrigkeit der Regelungen.

Secorvo News

Secorvo College aktuell

Einen tiefen Einblick in IT-Sicherheitsaudits in der Praxis bietet Secorvo College am **06.–08.05.2008**. Am **27.–30.05.2008** findet wieder der „aktuelle Klassiker" statt – IT-Sicherheit heute. Nur noch wenige Plätze gibt es für das TISP-Seminar, das Secorvo College am **02.–06.06.2008** mit anschließender Prüfung durchführen wird. Programm und Online-Anmeldung unter http://www.secorvo.de/college.

DuD 2008 – die zehnte

Für die diesjährige 10. Fachkonferenz „DuD 2008" am **09.–10.06.2008** in Berlin unter der fachlichen Leitung der Herausgeber der Zeitschrift „Datenschutz und Datensicherheit" konnten wieder spannende Vorträge gewonnen werden. Darunter finden sich die Themen Whistleblowing, Internet-Bewertungen von Lehrkräften, IT-Virtualisierung, das Audit-Gesetz, Computerkriminalität und das „Web 2.0". Burkhard Hirsch, Bundesinnenminister a.D., wird zu den gesellschaftlichen Folgen staatlicher Überwachung Stellung beziehen, Prof. Christof Paar seine Attacke auf Wegfahrsperren vorstellen und Jan Krissler vom Chaos Computer Club über die jüngsten Angriffe auf Biometrie-Systeme berichten.

Pimp your web

Am **29.05.2008** widmet sich die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) dem Schutz von Web-Applikationen. Maximilian Dermann von Lufthansa Technik wird vorstellen, wie diese sich insbesondere vor DoS-Angriffen schützen lassen.

Veranstaltungshinweise

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

Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
29.05.	Pimp your web (KA-IT-Si, Karlsruhe)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Fundsache

Das freie E-Book „Security Concepts“ von Travis Howard, veröffentlicht am 12.04.2008, hat zwar mit 120 Seiten noch Projektcharakter, aber die übersichtliche Struktur, die Inhalte und insbesondere die starke Verlinkung zu externen Quellen machen das Werk zu einem lesenswerten Reiseführer für Sicherheitsinteressierte. Bemerkenswert ist der Versuch des Autors, zentrale und allgemeingültige Sicherheitsprinzipien herauszuarbeiten.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Stefan Kelm, Jochen Schlichting

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