secorvo
security consulting

Secorvo Security News

Mai 2009

Der Feind in meinem PDA

„Es ist also die Geschichte der Natur wie der menschlichen Gesellschaft, aus der die Gesetze der Dialektik abstrahiert werden. (...) Und zwar reduzieren sie sich der Hauptsache nach auf drei: das Gesetz des Umschlagens von Quantität in Qualität und umgekehrt, (...)“
Friedrich Engels, Dialektik der Natur

Es gibt gute Gründe, der Neudefinition der Hegelschen Dialektik durch Marx und Engels mit Skepsis zu begegnen. Die rasante Entwicklung der Informationstechnik liefert jedoch zahlreiche Belege für die Plausibilität von Engels erstem dialektischen Gesetz: Immer wieder ist es deren Verbreitung, die zu qualitativ neuen Sichtweisen zwingt. Das gilt besonders für die IT-Sicherheit: Erst die Allgegenwart von PCs machte sie als Angriffsziel interessant, Client-Server-Architekturen erhöhten den Schutzbedarf, und deren universelle Vernetzung führte zu gänzlich neuen Schutzkonzepten.

Nun ist es wieder so weit: Der Siegeszug moderner Personal Digital Assistants (PDAs) fordert Sicherheitsarchitekturen heraus. Vor wenigen Jahren noch waren PDAs bestenfalls persönliche Kalender mit Adressbuch auf proprietären Spezialsystemen. Schadsoftware hatte Seltenheitswert, da Inkompatibilität und rudimentäre Kommunikationsschnittstellen eine nennenswerte Verbreitung verhinderte.

Das hat sich geändert. PDAs sind dabei, Laptops zu verdrängen. Die Beliebtheit von Blackberry und iPhone haben ebenso dazu beigetragen wie der Preisverfall bei Mobilfunk-Flatrates und die gestiegene Leistungsfähigkeit. Unternehmen reagieren auf diese Entwicklung, indem sie über Hersteller-APIs den PDA-Zugriff auf Unternehmenssoftware freigeben. Damit stellt ein PDA heute aus der Perspektive des Informationsschutzes dasselbe Risiko dar wie ein Laptop.

Allerdings: PDAs gehen häufiger verloren, sind ständig „online“ (oft ohne Passwortsperre), werden selten „sauber“ entsorgt und verfügen fast nie über eine Vollverschlüsselung. Und sind das perfekte Tool für Industriespione: Mit Kamera, Mikrofon, Online-Verbindung, GPS-Empfänger und Zugriffsrechten – und einem Nutzer, der jeden Hinweis auf eine „hippe“ neue Applikation sofort dankbar umsetzt.

Inhalt

secorvo
security consulting

Security News

Websecurity-Statistik

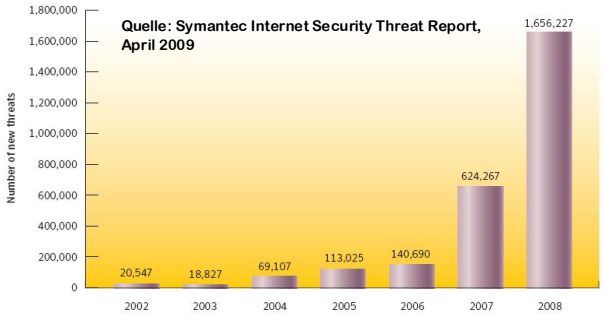
Zwar sollte man Statistiken grundsätzlich mit einer kritischen Distanz begegnen. Dennoch soll an dieser Stelle auf den Web Site Security Statistics Report der amerikanischen Firma WhiteHat Security, der am 18.05.2009 vorgestellt wurde, hingewiesen werden: Hinter diesem Bericht steckt unter anderem der Firmengründer und in Web-App-Security-Kreisen sehr geschätzte Jeremiah Grossman. Erschreckend ist, dass von den im ersten Quartal 2009 untersuchten Websites 82 % eine Schwachstelle aufwiesen, die von WhiteHat mit HIGH, CRITICAL oder URGENT bewertet wurde. Bei 63 % der Sites waren die Schwachstellen zum Veröffentlichungszeitpunkt noch nicht beseitigt.

Der Bericht stellt interessante aktuelle Entwicklungen vor und belegt viel diskutierte Sicherheitsprobleme von Webanwendungen mit konkreten Zahlen. Er kann auf der Webseite von WhiteHat zum Download angefordert werden.

Malware explodiert

Am 14.04.2009 hat Symantec den Internet Security Thread Report für 2008 veröffentlicht. Er dokumentiert die Fortsetzung einer beängstigenden Entwicklung: Die Zahl neuer Schadsoftware, die bereits 2007 auf mehr als das Vierfache angestiegen war, hat sich 2008 erneut vervielfacht – auf 1,65 Mio. Anders ausgedrückt: An jedem Kalendertag wurden 2008 im Schnitt über 4.500 neue Schadprogramme in die Welt entlassen.

Im vergangenen Jahr hatte die Zahl im Mittel noch bei etwa 1.700 gelegen. Eine solche Flutwelle lässt sich nur noch mit Heuristiken bewältigen: Virenscanner können neuartige Schadsoftware, die auf einen Schlag via Botnetz verteilt wird, nicht mehr an einer bekannten Signatur, sondern nur noch an „auffälligen" Eigenschaften erkennen. Daher steigt die Bedeutung einer alten Empfehlung wieder: Durch den Einsatz unterschiedlicher Scanner auf zentralen und lokalen Systemen und möglichst kurze Aktualisierungszyklen sollte die Qualität der Analyse optimiert werden. Und eine regelmäßige Komplettprüfung (vor allem mobiler) Endsysteme sollte ebenfalls etablierte „Best Practice" sein.



„GSG Botnetz"

Forschern der University of California ist es Anfang 2009 gelungen, das „Torping"-Botnetz zu übernehmen. In einem am 29.04.2009 veröffentlichten Forschungsbericht „Your Botnet is My Botnet" wird im Detail beschrieben, wie die dynamisch wechselnden Zieldomänen für die Command-und-Control-Server vorab bestimmt und reserviert werden konnten. Auf diese Weise konnten die Forscher – aus Sicht des Botnetz-Betreibers „feindliche" – C&C-Server aufbauen und darüber das Botnetz kontrollieren. Ein neues Binary des Botnetz-Betreibers, das an die infizierten Systeme verteilt wurde, unterband die Kontrolle nach zehn Tagen wieder.

Dennoch konnten in dieser Zeit über 70 Gigabyte an Botnetz-Daten, darunter zahlreiche Kennwörter gesammelt werden:

Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

Neben Details zur Funktionsweise stellten die Forscher fest, dass die Größe von Botnetzen vielfach überschätzt wird: Eine Unterscheidung zwischen infizierten Systemen und festgestellten IP-Adressen zeigt, dass aufgrund wechselnder IP-Adressen die reale Anzahl von „Zombies" erheblich kleiner ist als vermutet. Dennoch belegt das Beispiel eindrucksvoll die tatsächliche Gefährdung und verdeutlicht das Erfordernis, Systeme aktuell zu halten und Sicherheitssoftware wie Virenschutz und Personal Firewalls einzusetzen.

News from OWASP

Bei OWASP hat sich auch im Mai 2009 viel getan. Vom 13.-14.05.2009 fand in Warschau die OWASP AppSec Europe 2009 statt. Für Interessierte sind die Präsentationen von Tag 1 und Tag 2 inzwischen online verfügbar. Auf der Konferenz wurden in drei parallelen Tracks spannende Themen zur Sicherheit von Web-Anwendungen behandelt, darunter Vorträge zu den Themen „Threat Modeling", „The Bank in the Browser – Defending web infrastructures from banking malware", „CSRF: the nightmare becomes reality?" und „Factoring malware and

organized crime in to Web application security".

Im Schatten der OWASP-Konferenz wurde im Mai das OWASP PCI Project etabliert. Im Verlauf des Projekts sollen vereinheitlichte Anforderungen an Web-Anwendungen formuliert werden, die den Erfordernissen der Payment Card Industry Data Security Standards (PCI-DSS) der Kreditkartenorganisationen genügen.

Offene Gesellschaften

Bereits am 21.01.2009 veröffentlichte der ZEW-Forscher Dr. Wolfgang Sofka das Ergebnis einer in Zusammenarbeit mit Edlira Shehu von der Universität Hamburg durchgeführten Untersuchung über die Maßnahmen multinationaler Unternehmen zum Schutz vor unerwünschtem Informationsabfluss (Host Country Contingencies on Knowledge Protection Strategies of Multinational Firms).

Die zentrale Erkenntnis der Studie, gestützt durch eine Stichproben-Befragung von 1.500 deutschen Unternehmen, dürfte überraschen: Die ergriffenen Schutzmaßnahmen zur Verhinderung von Know-How-Diebstahl orientieren sich keineswegs an „Best Practices" oder etablierten Standards, sondern folgen überwiegend einem ökonomischen Kalkül: Hat ein ausländischer Standort den Status eines „Technologieführers", verlegen sich Unternehmen auf das Patentrecht und möglichst enge Kooperationen – mit dem Ziel eines für sie profitablen gegenseitigen Wissenstransfers. Umgekehrt steigt die Bedeutung von Abschottungsmaßnahmen, wenn ein Standort als technologisch rückständig gilt.

Selbstverständlich muss eine angemessene Klassifikation sensibler Daten in der Praxis einer realistischen Risikobewertung folgen. Zu kurz gesprungen erscheint allerdings die offensichtliche Zurückhaltung von Unternehmen in technologisch führenden Standorten – denn Wirtschaftsspionage ist schon lange kein nationales Problem mehr. So werden Patentschriften nicht nur im Inland gelesen, und die Spionageaktivitäten von Ländern mit technologischem Nachholbedarf konzentriert sich schon seit Jahren auf die „offenen" Gesellschaften des Westens, in denen das benötigte Wissen, wie die Studie belegt, oft viel leichter zugänglich ist.

Secorvo News

Secorvo College aktuell

In guten wie in schlechten Zeiten bleiben die Weiterentwicklung der persönlichen Qualifikation und deren Nachweis der Schlüssel für Ihre berufliche Entwicklung. Mit dem TISP bieten wir Ihnen die Möglichkeit, Ihre Kenntnisse auf hohem Niveau zu erweitern und mit einem anerkannten Zertifikat zu belegen. Acht Referenten bündeln ihr Wissen, ihre Expertise und ihre langjährige Berufserfahrung, um Ihnen in fünf Tagen die essentiellen Inhalte der Informationssicherheit zu präsentieren. Die nächsten TISP-Seminare finden statt am **22.–27.06.** und **07.–12.09.2009** (jeweils einschließlich Prüfung).

Vom **30.06.–03.07.2009** erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Detaillierte Programme, College-Jahreskalender und Online-Anmeldung unter http://www.secorvo.de/college.

… Zertifizierung ist besser

Am **25.06.2009** dreht sich bei der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) alles um das Thema ISO 27001: Im Rahmen des Events „Vertrauen ist gut – Zertifizierung ist besser" gibt Peter Zimmer von der prego services GmbH in Ludwigshafen mit einem Erfahrungsbericht Einblick in die notwendigen Vorbereitungen zur Erlangung der Zertifizierungsreife sowie die Wirkung des ISO-Standards im Geschäftsalltag. Um Anmeldung wird gebeten.

Tag der IT-Sicherheit

Gemeinsam mit dem Cyberforum und der IHK-Karlsruhe veranstaltet die KA-IT-Si am **16.07.2009** den ersten Karlsruher „Tag der IT-Sicherheit" im Saal Baden der IHK (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro). Neben Fragen der Haftung („Wer hastet, der haftet!") und einer aktuellen Einschätzung der Bedrohungen werden Unternehmen der TechnologieRegion in Erfahrungsberichten ihre „Best Practices" vorstellen: die Telemaxx Kommunikation GmbH, die Fiducia IT AG und die Edelstahl Rosswag GmbH – ausgezeichnet mit dem IT-Sicherheitspreis Baden-Württemberg 2007 bzw. 2009. Die Veranstaltung klingt ab ca. 18 Uhr mit einem KA-IT-Si-typischen „Buffet-Networking" aus.

Anmeldung bitte bis 09.07.2009 an Frau Helen Armbruster (IHK Karlsruhe), Tel.: 0721/174-190, helen.armbruster@karlsruhe.ihk.de.

Anschließend beginnt für die KA-IT-Si die Sommerpause – bevor es am **24.09.2009** mit dem Event „Pacta sunt servanda" zum Thema „Softwaresicherheit – Design by Contract" weitergeht.

Veranstaltungshinweise

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

Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P.-Schulung (Secorvo College)
25.06.	„Vertrauen ist gut – Zertifizierung ist besser“ (KA-IT-Si, Karlsruhe)
30.06.-03.07.	Information Security Management (Secorvo College)
Juli 2009	
06.-07.07.	SANS WhatWorks Summit in Forensics and Incident Response (SANS, Washington/US)
07.-10.07.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Ende August 2008 veröffentlichte Thomas Noon, inzwischen vereidigter Sachverständiger für IT-Systeme, seine Masterarbeit über „Geldspielgeräte und die SpielV“. Das Dokument ist ein weiteres erschütterndes Beispiel für die Risiken inkompetenter Digitalisierung ursprünglich analoger Geräte, wie erst unlängst bei Wahlmaschinen (SSN 10/2008) zu beobachten. Angesichts von Milliardenumsätzen geht es hier jedoch um Lizenzen zum Gelddrucken. Und wieder hat die PTB ihre Hand im Spiel ...

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian

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