

Secorvo Security News

Dezember 2008



Editorial: Pyrrhussiege

Einige zehntausend Kreditkartennummern der Landesbank Berlin auf Microfiche, vom Kurier gegen einen Christstollen getauscht. Bankverbindungen von 21 Mio. Bundesbürgern auf dem Schwarzmarkt, für kleines Geld von Call-Center-Mitarbeitern eingesammelt. CD mit 17 Mio. Kundendaten von T-Mobile aufgetaucht, von einem Dienstleister mit umfangreichen Berechtigungen entwendet. Alles Variationen desselben Themas: Zunehmend vertrauen Unternehmen sensible Unternehmens- und Personendaten Dritten an – die das Vertrauen nicht immer verdienen.

Zwar sind die Motive für eine Auslagerung von Tätigkeiten an externe Dienstleister ebenso berechtigt wie nachvollziehbar. Für größere Flexibilität und transparentere Kosten zahlt man aber einen versteckten Preis: geringere Loyalität und Bindung an das beauftragende Unternehmen, eingeschränkter Einfluss auf die Prozesse und geringes Verständnis der Kerngeschäftsprozesse beim Dienstleister.

Für zahlreiche Tätigkeiten mag das unproblematisch sein. Immer öfter aber sind sensible Daten betroffen, die eine hohe Zuverlässigkeit und Vertrauenswürdigkeit des Personals erfordern: Reinigungskräfte, die sich außerhalb der regulären Arbeitszeiten im Unternehmen bewegen; Kuriere, die vertrauliche Daten unverschlüsselt transportieren; IT-Dienstleister, die Zugriff auf unternehmenskritische Daten erhalten.

Unabhängig von der erforderlichen Basis-Qualifikation, die für eine Dienstleistung erforderlich ist, erfordert ein angemessener Umgang mit sensiblen Daten jedoch sowohl hohe Loyalität und Vertrauenswürdigkeit als auch ein Mindestmaß an Verständnis für die Bedeutung der Daten, um Schäden durch Nachlässigkeit zu vermeiden.

So entpuppen sich die schönen Reduktionen auf der Ausgabenseite der Bilanz immer öfter als Pyrrhussieg. Denn externe Dienstleistung erfordert sorgfältige Auswahl und Kontrolle – wer das vernachlässigt, zahlt meist einen hohen Preis, wenn etwas schief geht.



Inhalt

Editorial: Pyrrhussiege

Security News

Autorun deaktiviert?

Handys aller Orten

Blackberry zertifiziert

ePA-Akzeptanzstellen gesucht

Forensische Päckchen

OWASP-Start in Deutschland

Flickwerk Patchen

Secorvo News

Secorvo College aktuell

Zum Schluss ...

Veranstaltungshinweise

Fundsache

Security News

Autorun deaktiviert?

Seit vielen Jahren predigen Security-Experten, wie gefährlich das automatische Starten von Anwendungen auf Wechseldatenträgern mittels Autorun-Funktionalität ist, haben Viren und Würmer so doch leichtes Spiel. Glücklicherweise ist das Deaktivieren der Autorun-Funktion in Windows technisch trivial und wird daher in vielen Unternehmen zentral über Group Policy Objekte durchgesetzt.

Aber ist es wirklich so trivial? Still und heimlich gestand Microsoft in einem Technet-Artikel vom 10.10.2008, dass das Setzen von NoDriveTypeAutorun in der Windows-Registry nicht ausreicht – und beschrieb die [korrekte Erzwingung der Deaktivierung des Autorun-Registrierungsschlüssels in Windows](#). In vielen Umgebungen wird „die Autorun-Features nicht ordnungsgemäß deaktiviert“, selbst wenn die Registry-Schlüssel korrekt gesetzt waren. Microsoft reagierte nun mit zahlreichen [Updates](#) sowie einem weiteren Registry-Schlüssel, genannt „HonorAutorunSetting“. Nomen est omen. Peinlich, peinlich.

Handys aller Orten

Die Positionsbestimmung von Mobiltelefonen durch eifersüchtige Ehepartner und andere Bedarfsträger ist schon seit einer Weile einer der gefragtesten [Location Based Services](#) (LBS) für Mobilfunknetze. Zwar lassen sich LBS am Handy deaktivieren; dazu haben die deutschen Provider am 14.10.2008 eine [Selbstverpflichtung](#) auf ein einheitliches Verfahren veröffentlicht. Aber auch wenn auf dem Handy keine LBS aktiviert sind, werden Bewegungsdaten an Dritte weiter gegeben: So [meldete T-Traffic](#) am

03.11.2008, dass für die Stauprognose auf die Bewegungsdaten von 34 Millionen Handys im Netz der T-Mobile zugegriffen wird – „natürlich anonym“. Pikant: T-Traffic wurde am 20.11.2008 von einer Nokia-Tochter in den USA [übernommen](#); die Daten verlassen also den Geltungsbereich der EU-Datenschutzrichtlinie. Auch der Mitbewerber gibt sich nicht zugeknöpfter: Bereits am 14.01.2008 [vereinbarte](#) Vodafone Ähnliches mit TomTom.

Dass Handy-Ortung mit besseren Funkmessdaten noch präziser funktioniert als auf den Radius der mehr oder minder großen Funkzelle genau, gehört zur [Lehrbuchweisheit](#). Am 01.12.2008 [verkündete](#) Bayerns Innenminister den praktischen Vollzug; Das dortige LKA hat in einer Art „[Wardriving per Streifenwagen](#)“ einen Großteil der Mobilfunkzellen im Land vermessen und kartografiert. Eingesetzt wird das System zur Suche nach Verunglückten – und „[noch nicht](#)“ zur Fahndung.

Alles in allem ein paar gute Gründe (mehr), das Handy immer öfter einfach abzuschalten.

Blackberry zertifiziert

Vor mehr als drei Jahren wurde nach einem umstrittenen Kurzgutachten des BSI das Testlabor des Fraunhofer Instituts SIT in Darmstadt vom Hersteller Research in Motion ([RIM](#)) mit einer Analyse der Sicherheit des Blackberry-Dienstes beauftragt. Am 24.11.2008 wurden nun das lange erwartete [Zertifikat](#) (gültig für BES v4.1.6) und der 33seitige [Zertifizierungsbericht](#) veröffentlicht.

Das Ergebnis ist eindeutig und belegt die [Sorgfaltsmängel des BSI-Gutachtens](#) vom Herbst 2005: „In our analysis of the BlackBerry Enterprise Solution, we did not find any evidence for the existence of a master key, back door or a function that would

allow RIM to read customer's emails.“ Es ergänzt die von Secorvo im November 2005 publizierte [Analyse der Blackberry-Architektur](#) um eine Bestätigung der korrekten Implementierung des AES-256 und des Schlüsselmanagements.

Neben den im Zertifizierungsbericht enthaltenen Hinweisen zur sicheren Konfiguration des BES ist der „[Blackberry Hardening Guide](#)“ des australischen Department of Defense vom 18.12.2007 zu empfehlen. Er enthält auf 27 Seiten zahlreiche detaillierte Konfigurationstipps für die sichere Nutzung des Blackberry – einschließlich Vorgaben für die Nutzung von S/MIME, PGP und TLS.

ePA-Akzeptanzstellen gesucht

Es hat etwas von einem Gewinnspiel: Aus Unternehmen, Institutionen und Behörden, die bis zum 28.02.2009 dem [Aufruf zum Anwendungstest für den elektronischen Personalausweis](#) (ePA) – nicht zu verwechseln mit [EPa](#) – folgen, werden zehn ausgewählt. Sie können schon ab 01.10.2009 mit fachlicher Unterstützung des Bundesministeriums des Innern (BMI) die Nutzung des Identitätsnachweises über den ePA im Internet, an Automaten oder anderen Akzeptanzstellen erproben.

Leichtfertig sollte man dem Aufruf vom [IT-Gipfel](#) in Darmstadt am 20.11.2008 jedoch nicht mit seiner [Registrierung](#) folgen. Denn auch dieses Gewinnspiel hat einen Haken: Alle Bewerber – auch die nicht ausgewählten, deren Testphase nach Zeitplan am 01.12. 2009 beginnt – verpflichten sich, zahlreiche Eigenleistungen zu erbringen, von der Beschaffung bisher noch nicht verfügbarer Komponenten über die Akquise von Probanden bis zu gemeinsamen Marketing-Aktionen mit dem BMI. Bei positivem Testverlauf müssen sie ab dem Stichtag der ePA-Ausgabe am 01.11.2010 den ePA-Identitätsnach-

weis auch produktiv allen Ausweisinhabern unter ihren Nutzern anbieten.

Forensische Päckchen

Helix hat es vorgemacht (vgl. [SSN 10/2008](#)) – nun haben zwei weitere Anbieter neue Versionen ihrer kostenlosen forensischen Live-CDs veröffentlicht.

[DEFT Linux](#) (Digital Evidence & Forensic Toolkit) erschien am 28.11.2008 bereits in Version 4.01. Die Unterschiede zu Helix sind allerdings marginal: neben zu erwartenden Tools wie [Autopsy](#), [Sleuthkit](#) oder [foremost](#) umfasst DEFT Linux Tools für Penetrationstests, bspw. [Nessus](#) und [nmap](#). Vorsicht ist jedoch beim Anschluss externer Analyseplatten geboten: entgegen forensischer Best Practice werden diese nicht „read only“ eingebunden.

Äußerst vielversprechend sieht Version 0.4 von [CAINE](#) (Computer Aided INvestigative Environment) aus, die am 05.12.2008 veröffentlicht wurde. Auch CAINE bringt Standard-Tools mit, beinhaltet aber auch unbekanntere Forensiktools wie [guymager](#), [SFDumper](#) oder [Fundl](#). Herausragend ist das für Forensiker so wichtige Erstellen von Reports: CAINE stellt Mechanismen zur Verfügung, den Output der unterschiedlichen Tools in einem einheitlichen Format zu integrieren und erleichtert damit den Analyseprozess erheblich.

OWASP-Start in Deutschland

Über 100 Teilnehmer konnten sich am 25.11.2008 in Frankfurt davon überzeugen, dass das Thema Web Application Security inzwischen auch in Deutschland angekommen ist. Trotz äußerst kurzer Vorlaufzeit war die erste [OWASP-Konferenz OWASP Germany 2008](#) sowohl im Hinblick auf die inhaltliche Qualität als auch auf die Teilnehmerzahl ein voller Erfolg. Es

wurden technische Themen wie z. B. "Server- und Browser-basierte XSS Erkennung" oder "SOA Sicherheitsarchitektur" und nicht-technische Themen wie z. B. "Wirtschaftlichkeitsbetrachtungen von IT-Sicherheitsmaßnahmen" behandelt. Den Besuchern früherer [KA-IT-Si-Veranstaltungen](#) wird der Vortrag "Goldene Regeln der IT-Sicherheit bei der Beauftragung und Erstellung von Software" bekannt vorgekommen sein. Auch diese Konferenz bestätigt, dass sich die OWASP-Organisation national und international zu einer festen Größe im Zusammenhang mit der Sicherheit von (Web-)Applikationen entwickelt hat. Allen, die die Konferenz nicht besuchen konnten oder die Vorträge noch einmal nachvollziehen möchten, stehen die Präsentationsfolien auf der [Konferenzseite](#) zur Verfügung.

Flickwerk Patchen

Dass das Aktualisieren von Systemen und Anwendungen inzwischen eine herausfordernde und aufwändige Aufgabe darstellt, ist nichts Neues. Lücken im Patch-Management finden sich daher nicht selten – und sollten zügig geschlossen werden. Das unterstreicht eine aktuelle [Veröffentlichung](#) des Anbieters Secunia, der am 25.11.2008 Version 1.0 des für den Privatgebrauch kostenlosen [Personal Software Inspector](#) veröffentlichte. Die Auswertung der Analyseergebnisse von über 20.000 (überwiegend privaten) Client-Systemen nach einer Woche zeigte, dass weniger als 2 % der Systeme sowohl beim Betriebssystem als auch bei weiteren installierten Programmen auf einem aktuellen Stand waren.

Angesichts der Zunahme aufgedeckter sicherheitskritischer Bugs und immer kürzerer Reaktionszeiten der Angreifer-Szene ist eine regelmäßige Analyse des Patch-Stands sehr zu empfehlen.

Secorvo News

Secorvo College aktuell

Für Ihr großes Interesse am [Weiterbildungsangebot](#) von Secorvo College im Jahr 2008 danken wir Ihnen. Die starke Nachfrage und die vielen positiven Rückmeldungen haben uns sehr gefreut. Wir hoffen, Sie im kommenden Jahr auf einer unserer Veranstaltungen wiederzusehen – einen aktuellen Überblick finden Sie in unserem [Seminarkalender 2009](#).

Auch für Ihre Anregungen und Themenwünsche an college@secorvo.de sind wir dankbar. Detaillierte Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter <http://www.secorvo.de/college>.

Zum Schluss ...

Hinter uns liegen 10 Jahre aktiver Mitwirkung an IT-Sicherheit und Datenschutz in Deutschland – und das erfolgreichste Jahr unserer Firmengeschichte. Wir danken Ihnen für Ihr Vertrauen und freuen uns auf viele weitere herausfordernde und spannende Jahre der Zusammenarbeit.



Wir wünschen Ihnen [besinnliche Feiertage](#) – und für 2009 neue Ideen, Visionen und gutes Gelingen!

Veranstaltungshinweise

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

Dezember 2008	
27.-30.12.	25th Chaos Communication Congress (CCC, Berlin)
Januar 2009	
20.-22.01.	Omnocard 2009 (inTIME, Berlin)
Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
10.-12.02.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College, Karlsruhe)
19.02.	Bingo-Voting - verifizierbare elektronische Wahlen (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
17.-18.03.	16. DFN Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)

Fundsache

Microsoft hat am 10.11.2008 eine öffentliche Beta-Version des "[SDL Threat Modelling Tool v3.1](#)" zum Download bereitgestellt. Die [Bedrohungsanalyse \(Threat Modelling\)](#) spielt im [Secure Development Lifecycle \(SDL\)](#) eine wichtige Rolle. Erste Tests mit diesem Tool hinterließen einen positiven Eindruck. Das Threat Modelling Tool findet sich u. a. im [Tools Repository zum SDL](#).

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch

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

