secorvo
security consulting

Secorvo Security News

Dezember 2009

Endogene Bedarfsexpansion

Wenn Sie Kinder haben, kennen Sie das Phänomen. Besonders gut ist es jährlich vor dem Weihnachtsbaum zu beobachten: Ganz gleich, wie viele Pakete Ihre Kinder ausgepackt haben – nach dem letzten schweifen die Blicke sehnsüchtig suchend bis zur enttäuschenden Einsicht durch den Raum, dass es tatsächlich das letzte war.

Vielleicht ist diese „Gier nach mehr" ja nicht nur die natürliche Erklärung für die Faszination des österlichen Eiersuchens, sondern der wahre Antrieb hinter dem Streben nach immer mehr Kontrolldaten – wie die Ausweitung der Videoüberwachung im öffentlichen Personenverkehr (Verkehrsministerkonferenz vom 04.12.2009) oder die anlassunabhängige des Individualverkehrs, die erst das Bundesverfassungsgericht stoppen konnte (Beschluss vom 11.08.2009). Auch die Zahl der Telefonüberwachungen, bereits 2007 weltweit auf historisch einmalig hohem Niveau, stieg 2008 erneut – um 11% auf 16.463 Maßnahmen. Dass daher die Vorratsdatenspeicherung von Telekommunikationsdaten, die am 15.12.2009 vom Bundesverfassungsgericht verhandelt wurde, keine gute Idee ist, zeigen auch die Versuche der Strafverfolgungsbehörden, trotz expliziten Verbots im § 7 Autobahnbaumtgesetz („Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig") auf die vom Betreiber Toll Collect an Maut-Kontrollbrücken erhobenen Daten zuzugreifen, Stellungnahmen wie die der Musikindustrie und die Feststellungen des Bundesdatenschutzbeauftragten, dass TK-Unternehmen weit mehr speichern als erlaubt: Einst auf schwere Straftaten beschränkt, droht der Eingriff ins Fernmeldegeheimnis zum Standard-Ermittlungsinstrument zu werden. Fehlen noch die Pflicht zu „intelligenten Stromzählern" und die Abschaffung des Bargelds: Präziser lassen sich Lebensgewohnheiten kaum bestimmen.

„Die Freiheit stirbt scheibchenweise": Worte des Jahres 2001 in „Die ZEIT", von Sabine Leutheusser-Schnarrenberger. Seit dem 28.10. 2009 ist sie Bundesjustizministerin. Die Hoffnung stirbt zuletzt.

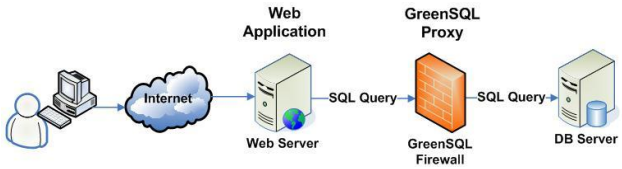
Inhalt

secorvo
security consulting

Security News

SQL-Firewall

Am 02.12.2009 wurde Version 1.2 der OpenSource SQL-Firewall GreenSQL freigegeben. Die Idee hinter diesem speziellen Application Level Gateway ist, Zugriffe von (Web-) Applikationen auf dahinter liegende Datenbanken zentral und unabhängig von der Anwendung filtern zu können.



(Quelle: greensql.net)

Audits von Web-Applikationen zeigen, dass sehr viele Web-Anwendungen keine ausreichende Eingabevalidierung vornehmen und so anfällig für SQL-Injection sind. Zudem besteht immer das Risiko, dass ein Webserver über Schwachstellen der Plattform, des Webservers selbst oder der Anwendung (PHP, .net, J2EE, Ruby etc.) kompromittiert wird. In diesen Fällen kann auf die dahinter liegende Datenbank, selbst wenn sie in einer separaten Netzwerkzone betrieben wird, unberechtigt zugegriffen werden.

Bei einer Kontrolle der Zugriffe mittels GreenSQL ist es beispielsweise möglich zu definieren, auf welche Tabellen und Datenbestände zugegriffen werden darf, oder ob Daten nur gelesen, aber nicht geschrieben werden dürfen. Einen ersten Eindruck zu den Konfigurationsmöglichkeiten kann man sich in einer Live-Demo verschaffen. Derzeit werden MySQL und PostgreSQL unterstützt.

Nichts gelernt ...

... aus den Datenschutzskandalen der jüngsten Zeit hatten offenbar die Verantwortlichen des Sozialen Schülernetzwerks haefft.de. Am 04.12.2009 deckte der Chaos Computer Club (CCC) Scheunentor große Sicherheitslöcher bei dem Portal auf. Erschreckend in diesem konkreten Fall: die schlechten Implementierungen von Sicherheitsmaßnahmen zum Schutz intimer personenbezogener Daten von Kindern.

Nachdem in einer inzwischen gelöschten Pressemitteilung der Fall von den Verantwortlichen herunter gespielt worden war, eskalierte der Vorgang. Nun ist das Portal offline – der Betreiber entschuldigt sich in einer neuen Stellungnahme für die Fehler und erläutert das nun geplante Vorgehen.

Der Vorfall ruft drei Grundregeln ins Gedächtnis:

1. Sorgen Sie *als Entwickler* von Web-Anwendungen, die personenbezogene Daten speichern und verarbeiten, für korrekte Implementierung, sicheren Betrieb und wirksame Schutzmaßahmen.

2. Achten Sie *als Betreiber* bei Sicherheitsvorfällen auf eine angemessene Krisenkommunikation.

3. Bedenken Sie *als Betroffener* genau, welche Daten Sie über sich wo preisgeben – und sprechen Sie mit Ihren Kindern über das Thema.

Forensik-Folklore

Zu dem bereits am 15.04.2009 veröffentlichten 2009 Data Breach Investigations Report des Sicherheitsdienstleisters Verizon Business (vgl. SSN 04/2009) erschien am 09.12.2009 – als Nachschlag – ein Supplemental Report, der die Bedrohung durch die 15 häufigsten Angriffsarten, von Keyloggern über Social Engineering bis hin zum Durchforsten des RAM-Speichers in Kassensystemen und zum „*ishing“, ausführlicher analysiert und jeweils ein anonymisiertes Fallbeispiel schildert.

Bei einigen dieser anekdotischen Schwachstellenbeschreibungen lässt sich ein Schmunzeln kaum unterdrücken (wie beim manuellen Ersetzen von „validUser=0“ durch „...=1“ in einer Web-Anwendung, um die Anmeldung einzusparen), bei anderen beschleicht einen das ungute Gefühl, möglicherweise selbst nicht ausreichend gegen ähnliche Angriffe gefeit zu sein.

Schöner neuer Personalausweis

Nachdem am 10.11.2009 bekannt geworden war, dass das BMI ein Konsortium unter Siemens-Führung mit der Bereitstellung der Middleware für den neuen elektronischen Personalausweis, den „Bürger-Client“ beauftragt hatte, meldete die mtG media transfer AG am 30.11.2009, dass sie den Zuschlag für den Aufbau der Root CAs für die Nutzung und den Zugriff auf die Daten des künftigen Personalausweises erhalten habe.

Bemerkenswert: Diese Root CAs werden beim BSI in Anlehnung an die bestehende Verwaltungs-PKI (die im gleichen Zuge runderneuert wird) aufgebaut. Hingegen bleiben die Zertifizierungsdiensteanbeiter für die elektronische Signatur und deren bei der BNetzA betriebene Root CA ein optionales Anhängsel der Ausweiskarte. Darf das als späte Einsicht in die Erfolglosigkeit überregulierter Signatur-Infrastrukturen gewertet werden?

ISO 2700x mit x=4

Mit Veröffentlichungsdatum vom 15.12.2009 ist ein neuer Standard in der ISO-27000er-Reihe zur Messung der Informationssicherheit erhältlich – ISO/IEC 27004:2009 „Information technology – Security

techniques – Information security management – Measurement".

Darin wird endlich verbindlich geregelt, was unter Messungen und Bewertungen im Rahmen eines Informationssicherheitsmanagements nach ISO 27001 zu verstehen ist. Neben den Erklärungen zu einem sinnvollen Vorgehen bei der Entwicklung von Messungen finden sich auch Hinweise zur Verantwortung des Managements sowie zu Durchführung und Dokumentation von Messungen.

Einen großen Teil der über 50 Seiten des Standards füllen praktische Beispiele und eine Dokumentationsvorlage im Anhang. Damit wird dem Praktiker eine nützliche Arbeitshilfe zur Verfügung gestellt. Der neue Standard ergänzt das Dokument „BIP 0074 – Measuring the effectiveness of your ISMS implementations" nun verbindlich.

Übrigens: Seit etwa sechs Monaten ist das Rahmenwerk – der Standard ISO 27000 – auch Lizenzkosten frei verfügbar.

Feiertagslektüre

Wer schon immer wissen wollte, wie es wäre, wenn Stanley Kubrick eine Anfängervorlesung in IT-Sicherheit gegeben hätte, wird wohl mit Vergnügen den am 15.12.2009 erschienenen Bericht von Matt Blaze über seinen Besuch in einem zum Museum umgewandelten Interkontinentalraketen-Silo lesen. Darin analysiert der bekannte Kryptologe und Autor des Cryptographic Filesystem CFS die Sicherheitsmaßnahmen, mit denen im Kalten Krieg die ins Extrem getriebenen, einander widerstrebenden Anforderungen nach Hochverfügbarkeit bei gleichzeitiger strikter Zugriffskontrolle realisiert wurden, wie Vier-Augen-Prinzip, Physische Zutrittskontrollen oder „Separation of Duties".

Secorvo News

Secorvo College aktuell

Auch im neuen Jahr bieten wir Ihnen im Secorvo College wieder zahlreiche Gelegenheiten, Ihr Wissen zu zertifizieren. Neben der etablierten TISP-Schulung, unter anderem vom 22. bis 26.02.2010, können Sie sich mit dem CPSSE als Experte im Bereich der sicheren Softwareentwicklung zertifizieren. Die erste Schulung im neuen Jahr findet vom 16. bis 18.03.2010 statt. Hintergründe zur Zielsetzung und Entstehung des Zertifikats liefern zwei kürzlich erschienene Aufsätze von Petra Barzin, einer der Initiatorinnen des CPSSE: „A New Qualification to Guarantee Secure Software Engineering Skills" (in: ENISA Quarterly Review, Vol. 5 No. 3, September 2009, S. 18) und „International Secure Software Engineering Council (ISSECO)" (in: SecurityActs No. 1, Oktober 2009, S. 14 f.).

Unsere Grundlagenseminare zu den Themen Sicherheitsmanagement, PKI und IT-Sicherheitsaudit finden Sie ebenfalls im Programm 2010, nicht zuletzt dank der durchweg positiven Rückmeldungen der Teilnehmer. Eine aktuelle Übersicht finden Sie in unserem Seminarkalender 2010. Melden Sie sich an, wir freuen uns auf Sie!

Wege zum Ruhm

Die KA-IT-Si verabschiedet sich nach sechs Events zu spannenden Themen der IT-Sicherheit aus dem Jahr 2009 in eine kurze Verschnaufpause. Am 18.02.2010 stellen Sven Kaun und Lutz Bleyer die Awareness-Kampagne „Security Cup 2009" der FIDUCIA IT AG vor – und sich beim anschließenden Buffet-Net(t)working der Diskussion. Um Anmeldung wird gebeten.

A propos Awareness: Die KA-IT-Si freut sich über jeden weiteren Partner, der die Arbeit der Initiative unterstützt – den Wissenstransfer zur IT-Sicherheit auf den Fachevents, den regen Erfahrungsaustausch unter IT-Sicherheitsverantwortlichen und die Sensibilisierung insbesondere mittelständischer Unternehmen für die Bedeutung der Informationssicherheit. Nähere Informationen zur KA-IT-Si-Partnerschaft finden Sie auf der KA-IT-Si-Webseite.

Teamverstärkung

Seit dem 01.08.2009 verstärkt Dr. Safuat Hamdy das Secorvo-Team – den regelmäßigen und aufmerksamen Lesern bereits vom Editorial der SSN 10/2009 bekannt.

Im kommenden Jahr soll unser Team weiter wachsen: Wir suchen mehrere Beraterinnen oder Berater im Gebiet Datenschutz und IT-Sicherheit mit Berufserfahrung für zahlreiche herausfordernde Projekte – und freuen uns über Empfehlungen und Bewerbungen an personal@secorvo.de.

Veranstaltungshinweise

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

Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
15.-18.02.	SecSE 2010: Fourth International Workshop on Secure Software Engineering (SINTEF, Krakau/PL)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering – CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

Wer noch ein Weihnachtsgeschenk oder Lesestoff für die Feiertage sucht, dem sei ein Blick in die Bücherliste von Tobias Schrödel empfohlen. Fast 500 Werke rund um das Thema Kryptographie hat er zusammengetragen. Allerdings sind einige nicht mehr käuflich zu erwerben, so wie Giovanni Battista Bellasos „Novi et singolari modi di cifrare“ (1555).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, 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