

# Secorvo Security News

Juli 2009



## Zenon und die Verfügbarkeit

Die Beispiele sind zahlreich und reichen von der RZ-Blackbox, die im Notfall die gespeicherten Daten via WLAN preisgibt, bis zum Verlust der PKI-Root-Keys bei der Gematik: Immer wieder verursacht der Konflikt zwischen den Sicherheitszielen Vertraulichkeit und Verfügbarkeit Sicherheitsvorfälle oder zumindest – wie beim Thema Schlüssel hinterlegung (Key Escrow) – heftige Auseinandersetzungen.

Tatsächlich geraten diese beiden Sicherheitsziele bei fast jeder Sicherheitslösung aneinander. Wer Backups erstellt, um eine hohe Datenverfügbarkeit zu erreichen, schafft unvermeidlich einen neuen Angriffspunkt auf deren Vertraulichkeit. Wer Daten verschlüsselt abspeichert, riskiert mit dem Verlust des Schlüssels auch den der Daten. Und ein Passwortrücksetzungsverfahren kann die Vertraulichkeit bedrohen, wenn Unberechtigte es veranlassen können.

Das Spannungsverhältnis ist beiden Zielen immanent – warum aber werden in der Praxis allzu häufig Maßnahmen für das eine Ziel auf Kosten des anderen umgesetzt? Zu vermuten ist, dass bei vielen Konzepten übersehen wird, dass jede Maßnahme zur Erreichung eines der Sicherheitsziele das Schutzobjekt des anderen Ziels verändert: Auch die Backups sind bei den Vertraulichkeitsmaßnahmen zu berücksichtigen, und für Passwörter und Schlüssel müssen Verfügbarkeitsmaßnahmen getroffen werden.

Das klingt verdächtig nach Zenon von Eleas Paradoxie von Achilles und der Schildkröte, deren Vorsprung er trotz höherer Geschwindigkeit nicht einholen kann: Sobald er die Stelle erreicht, auf der die Schildkröte eben noch stand, ist diese bereits weitergekröchen.

Ein Trugschluss – denn auch eine unendliche Reihe (wie die schrumpfenden Abstände zwischen Achilles und der Schildkröte) kann eine endliche Summe besitzen. So müssen auch Vertraulichkeit und Verfügbarkeit nicht ad infinitum konkurrieren – geeignete Schutzkonzepte müssen jedoch immer beide angemessen berücksichtigen.



## Inhalt

### Zenon und die Verfügbarkeit

#### Security News

Sicher ist sicher – oder?

BDSG novelliert

Bedrohungsanalysetools

Nmap/Zenmap v5.0

Rechtssicherheit beim § 202c

Urlaubsrätsel

### Secorvo News

Secorvo College aktuell

Security News Symposium

Vertrag ist Vertrag

### Veranstaltungshinweise

### Fundsache

## Security News

### Sicher ist sicher – oder?

„[Sicherheitsmechanismen bei Root-Zertifikaten wirksam](#)“ meldete am 15.07.2009 die [gematik](#), als Projektgesellschaft zuständig für die elektronische Gesundheitskarte (eGK) und die Heilberufsausweise (HBA) für medizinisches Personal. Anfang Juli hatte [D-TRUST](#), Betreiber des Trustcenters für eGK und HBA, ein [neues Root-Zertifikat](#) erstellen müssen – übrigens nicht nach [X.509](#), sondern im „[card verifiable](#)“ Zertifikatformat gemäß [ISO-7816](#), das u. a. auch beim [digitalen Tachographen](#) verwendet wird: Das für den Schutz der Schlüssel eingesetzte Hardware Security Modul (HSM) hatte Probleme in der Stromversorgung als Angriff gewertet und folgerichtig – alle Schlüssel gelöscht.

Nun müssen etliche Hundert „Musterkarten“ ausgetauscht werden. Zwar hätte man für Tests mit fiktiven Daten besser auf die hohe Sicherheit durch HSMs verzichtet und eine Root-CA in Software eingesetzt, oder die geplante Produktivumgebung inklusive Backup und Restore des Root-Schlüssels nachgebildet. Der Entscheidung für ein HSM ohne Backup verdankt die Welt jedoch zwei wichtige Ergebnisse: Erstens einen seltenen, realitätsnahen Test des Worst-Case Szenarios, und zweitens ein geschärftes Bewusstsein dafür, dass Sicherheit nicht nur bedeutet, dass Daten nicht in die falschen Hände fallen, sondern auch, dass sie in den richtigen verbleiben.

Veteranen der PKI-Szene mag bei der Meldung ein Deja-vu-Gefühl beschlichen haben: Vor knapp zehn Jahren verlor eine weltweite Banken-PKI kurz nach Betriebsbeginn auf dieselbe Weise die Root-Schlüssel. Ob es ein schlechtes Omen für die eGK ist, dass

besagte Banken-PKI inzwischen als Beispiel für einen überkomplexen, grandiosen Fehlschlag gilt?

### BDSG novelliert

In der letzten regulären Sitzung dieser Legislaturperiode hat der Deutsche Bundestag am 03.07.2009 den „[Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften](#)“ der Bundesregierung vom 18.02.2009 (BT-Drs. 16/12011) entsprechend den [Beschlussempfehlungen des Innenausschusses](#) vom 01.07.2009 (BT-Drs. 16/13657) verabschiedet. Im Hau-Ruck-Verfahren wurde damit in letzter Minute auf die teilweise vernichtende Kritik selbst engagierter Verfechter eines gesetzlich geregelten Datenschutzaudits reagiert und das Datenschutzauditgesetz, seit 2001 in § 9a BDSG angekündigt, erneut vertagt. Das Resultat wäre anderenfalls ein mit heißer Nadel gestricktes Gesetz voller handwerklicher Mängel im Detail gewesen – ohne Aussicht, den Datenschutz wirksam zu verbessern.

Nach der nun beschlossenen „Novelle II“, die am 01.09.2009 in Kraft tritt, ist der betriebliche Datenschutzbeauftragte zukünftig nur noch „aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist“ kündbar, und die verantwortliche Stelle verpflichtet, die Teilnahme an Fort- und Weiterbildungsmaßnahmen zu ermöglichen und zu finanzieren. Die Zulässigkeit der Nutzung listenmäßig zusammengefasster Daten für Zwecke des Adresshandels bleibt erhalten. Konsequenter geregelt wurde die Auftragsdatenverarbeitung in § 11 BDSG – eine Überprüfung der Verarbeitung beim Auftragnehmer hat nun vor Beginn der Verarbeitung und regelmäßig während dessen Verlaufs zu erfolgen; die Ergebnisse sind zu dokumentieren. Als neuer § 32 wurde eine Regelung zum Arbeitnehmerdatenschutz ergänzt –

gut gemeint, aber inhaltlich nicht mehr als ohnehin bereits geltendes Recht. Schließlich wurden die Geldbußen auf bis zu 300.000 Euro angehoben und damit unmissverständlich klar gestellt: Die Zeit, in der Datenschutzverstöße als Kavaliersdelikt durchgehen, ist endgültig vorbei.

### Bedrohungsanalysetools

Wieder war es ein Softwarefehler in BIND 9 des [ISC](#), der ziemlich genau ein Jahr nach der letzten großen Attacke ([SSN 07/2008](#)) am 28.07.2009 das weit verbreitete Softwarepaket BIND 9 erneut [in die Knie zwang](#). Diesmal reichte ein einzelnes „dynamic update message“-Paket, um Master-DNS-Server zum Absturz zu bringen – ein weiterer Beleg für die Dringlichkeit sichererer Softwareentwicklung.

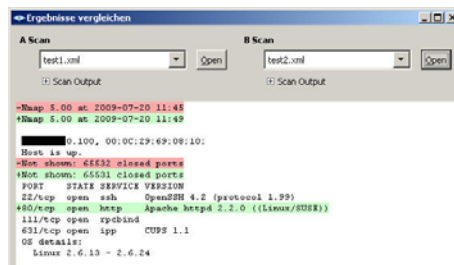
Einen großen Komfortsprung bei der Erstellung von Bedrohungsanalysen für Applikationen verspricht nun Version 3.0 von Microsofts [TAM](#) (Threat Analysis and Modelling). An der am 23.07.2009 erschienenen [ersten Beta-Version](#) lassen sich, wie erste Tests zeigen, signifikante Fortschritte bei der Bedienbarkeit des Werkzeugs feststellen. Getrübt wird der Eindruck durch Instabilitäten in der Testumgebung: So ließen sich manche Funktionen noch nicht richtig oder gar nicht ausführen. Die Verbesserungen der Visualisierungsmöglichkeiten sind vielversprechend. Bei verbesserter Stabilität wird TAM 3.0 eine sinnvolle Ergänzung des Werkzeugkastens zur sicheren Softwareentwicklung darstellen.

Einen anderen Ansatz verfolgt IBM mit seiner auf die Sicherheit von Web Applikationen zielende Rational [AppScan Suite](#), die in der Enterprise Edition neben dem Application Scanner ein Dashboard mit Reports über die Entwicklung der Zahl und Art der gefundenen Schwachstellen enthält. Dazu erschien am 29.05.2009 in der Serie Redguides das 38seitige

Whitepaper „[Improving Your Web Application Software Development Life Cycle's Security Posture](#)“, das auf den ersten 20 Seiten eine sehr anschauliche Einführung in die aktuelle Bedrohungslage und Best Practices zur Entwicklung sicherer Web-Applikationen bietet.

## Nmap/Zenmap v5.0

Am 16.07.2009 wurde Version 5.0 des wohl bekanntesten Netzwerk-Portscanners [Nmap](#) veröffentlicht. Sie ist sowohl für Linux als auch für Windows verfügbar und bietet über die eigentlichen Scan-Funktionen hinaus die Möglichkeit, grafische Netzwerkübersichten zu erstellen und Scan-Ergebnisse mit früheren Resultaten zu vergleichen.



Auch die Verwaltung der Scan-Profile wurde verbessert, und für alle, die keine Kommandozeilen-Gurus sind, wurde die grafische Oberfläche „Zenmap“ intuitiver und übersichtlicher gestaltet. Schon deswegen lohnt der Wechsel auf die neue Version.

## Rechtssicherheit beim § 202c

Mit dem [Nichtannahmebeschluss](#) vom 18.05.2009 über drei Verfassungsbeschwerden im Zusammenhang mit dem „Hackerparagraphen“ § 202c StGB hat das Bundesverfassungsgericht Rechtssicherheit geschaffen und klargestellt, dass Programme, die lediglich für Hacking-Angriffe geeignet, nicht aber Secorvo Security News 07/2009, 8. Jahrgang, Stand 31.07.2009

genau dafür entwickelt wurden (so genannte „Dual Use“-Software) nicht unter die Strafvorschrift fallen. Zur Durchführung von Penetrationstests ist auch die Nutzung von Hacking- und Analyse-Tools wie Nmap zulässig – sollte allerdings nachvollziehbar dokumentiert werden.

## Urlaubsrätsel

Wer auch im Urlaub Security-Themen nicht missen und auch am Strand nicht von der Websicherheit lassen will, dem sei das [OWASP-Kreuzworträtsel](#) empfohlen. Es gibt auch was zu gewinnen – aber Beeilung, das Rätsel ist seit dem 21.07.2009 online.

## Secorvo News

### Secorvo College aktuell

Direkt nach der Sommerpause haben Sie wieder Gelegenheit, Ihre Information-Security Kenntnisse zertifizieren zu lassen: Am 07.09.2009 startet die fünftägige [TISP-Schulung](#) mit anschließender Prüfung. Auch bei allen weiteren Seminaren, die wir im Herbst anbieten, präsentieren Ihnen unsere Experten gebündeltes Wissen und Expertise aus langjähriger Berufserfahrung und Beratungspraxis. Sichern Sie sich einen der wenigen noch freien Plätze für „[IT-Sicherheitsaudits in der Praxis](#)“ vom 21. bis 23.09.2009 oder für „[PKI](#)“ vom 03. bis 06.11.2009.

Den „Schwarzen Gürtel“ in sicherer Softwareentwicklung können Sie vom 29.09. bis 02.10.2009 in Gestalt des [CPSSE](#)-Zertifikats (Certified Professional for Secure Software Engineering) erwerben oder Ihre IT-Security Grundlagenkenntnisse mit dem Seminar „[IT-Sicherheit heute](#)“ vom 13. bis 16.10.2009 auffrischen. Programme und Online-Anmeldung unter [www.secorvo.de/college](http://www.secorvo.de/college).

## Security News Symposium

Mit den [Secorvo Security News](#) unterstützen wir Sie seit Juli 2002 Monat für Monat dabei, in der Informationsflut der IT-Sicherheit die wichtigsten Entwicklungen nicht aus den Augen zu verlieren, und lassen Sie an unseren Einschätzungen teilhaben. Aber nicht alle wichtigen Entwicklungen der Informations- und IT-Sicherheit lassen sich in einem wenige Zeilen umfassenden Beitrag angemessen beleuchten. Daher greifen wir in diesem Jahr mit dem ersten „[Security News Symposium 2009](#)“ am **06.-07.10.2009** in Ettlingen ausgewählte Themen auf und möchten sie in Vorträgen und Diskussionen mit Ihnen vertiefen. Zusammen mit ausgewählten weiteren Fachexperten bieten wir Ihnen ein spannendes und hoch aktuelles Programm in einem [inspirierenden Ambiente](#) – und freuen uns auf den Austausch mit Ihnen ([Anmeldung](#)).



## Vertrag ist Vertrag

Auf dem Event „[Pacta sunt servanda](#)“ weicht Sie die [KA-IT-SI](#) am 24.09.2009 in „Design by contract – die hohe Schule der sicheren Softwareentwicklung“ ein. Hagen Buchwald, Vorstandsvorsitzender des CyberForum e.V., gibt Einblick in den Prozess, der Softwareentwicklern helfen soll, das reibungslose und Sicherheitslücken freie Zusammenspiel einzelner Programmmodule von Anfang an zu gewährleisten. Im Anschluss gibt es wie immer die Möglichkeit zum Buffet Networking. Das Event beginnt um 18 Uhr im Schlosshotel Karlsruhe ([Anmeldung](#)).

## Veranstaltungshinweise

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

August 2009	
12.-14.08.	<a href="#">USENIX Security '09</a> (Usenix, Montreal/CA)
16.-20.08.	<a href="#">Crypto 2009</a> (IACR, Santa Barbara/US)
17.-18.08.	<a href="#">Digital Forensic Research Workshop</a> (DFRWS, Montreal/CA)
September 2009	
06.-09.09.	<a href="#">CHES: Workshop on Cryptographic Hardware and Embedded Systems</a> (IACR, Lausanne/CH)
07.-11.09.	<a href="#">TISP-Schulung</a> (Secorvo College)
15.-17.09.	<a href="#">IMF 2009: 5th International Conference on IT Security Incident Management &amp; IT Forensics</a> (GI, Stuttgart)
17.09.	<a href="#">RZ-Compliance</a> (Lampertz/Secorvo/Kroll Ontrack, Friedrichshafen)
21.-23.09.	<a href="#">IT-Sicherheitsaudits in der Praxis</a> (Secorvo College)
24.09.	<a href="#">Pacta sunt servanda</a> (KA-IT-Si, Karlsruhe)
29.09.- 02.10.	<a href="#">ISSECO Certified Professional for Secure Software Engineering – CPSSE</a> (Secorvo College)

## Fundsache

Seth Misener systematisiert in seinem am 13.06.2009 bei SANS publizierten Aufsatz „[A Virtually Secure Browser](#)“ die aktuellen Bedrohungen beim Surfen im Internet. Als wirksame Schutzmaßnahme empfiehlt er insbesondere den Einsatz einer lokalen Sandbox: Damit lässt sich die Sicherheit beim Surfen ohne signifikanten Komfortverlust erheblich steigern. Ein Ansatz, den auch Microsoft im Projekt [Office 2010](#) verfolgt.

## Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch und 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](mailto:security-news@secorvo.de)  
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an [redaktion-security-news@secorvo.de](mailto:redaktion-security-news@secorvo.de)

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

