

# Secorvo Security News

Januar 2012



## So klug als wie zuvor

Studien sind beliebt. Häufig stützen sie die „Propheten im eigenen Haus“, deren Worte kein Gehör finden. Gelegentlich befreien sie Entscheider von der Last der Verantwortung. Und manchmal versachlichen sie eine Diskussion, indem sie den einen oder anderen Irrglauben widerlegen.

Weniger beliebt sind allerdings Studien, die nicht das vom Auftraggeber erwartete oder erwünschte Ergebnis liefern. Zwar werden die Verfasser vom Auftraggeber bezahlt („Wes' Geld ich nehm', des' Lied ich sing“), mit einer Tendenzstudie setzen sie aber ihre Glaubwürdigkeit aufs Spiel – und riskieren Ruf und künftige Geschäfte.

Bei überraschenden Resultaten ist zumindest in der Politik die Neigung zu beobachten, missliebige Ergebnisse zurückzuhalten – vielleicht in der so trügerischen wie verzweifelten Hoffnung, damit einer unerwünschten öffentlichen Debatte ausweichen zu können.

So geschehen mit dem vom Justizministerium beim Max Planck Institut in Freiburg in Auftrag gegebenen Gutachten zur Frage der Erforderlichkeit der [Vorratsdatenspeicherung](#). Die Existenz der „2., erweiterten Fassung“ einer zwischen Mai und August 2010 (!) durchgeführten und im Juli 2011 abgeschlossenen [Untersuchung](#) machte erst eine [Veröffentlichung von Auszügen in Spiegel Online](#) am 27.01.2012 bekannt. Danach konnten die Autoren keine Hinweise dafür finden, dass der Wegfall der Vorratsdatenspeicherung negative Folgen für Strafverfolgung und Gefahrenabwehr habe: Wasser auf den Mühlen des Justiz- und Öl im Feuer des Innenministeriums.

Liest man die Schlussfolgerungen genau, so wird hinter dem tobenenden öffentlichen Säbelrasseln deutlich, dass die Autoren mit einer „sehr unsichere(n) statistische(n) Datengrundlage“ und „sehr unterschiedlichen Einschätzungen bei den unmittelbar betroffenen Praktikern“ arbeiten mussten – sprich: keine belastbaren Erkenntnisse gewinnen konnten. Eines ist daher sicher: Die nächste Studie kommt bestimmt. Und in diesem Fall wäre das auch sehr zu begrüßen.



## Inhalt

**So klug als wie zuvor**

**Security News**

Ungemach für Surf-Tracker

Smartphone-Sicherheit

Authentifikation systematisch

Kuck mal, wer da...

Verwirrungs-Taktik

**Secorvo News**

Neue Seminare

Karlsruher IT-Sicherheitsinitiative

**Veranstaltungshinweise**

**Fundsache**

## Security News

### Ungemach für Surf-Tracker

Am 08.12.2011 hat die [Art. 29 Gruppe](#), der beratende Zusammenschluss der europäischen und nationalen Datenschutzaufsichtsbehörden eine [Stellungnahme](#) zur künftigen Anwendung der so genannten [Cookie-Richtlinie \(RL 2009/136/EG\)](#) abgegeben. Sie bezieht sich auf [Vorschläge](#) der European Advertising Standards Alliance (EASA) sowie des Internet Advertising Bureau Europe (IAB), die ein Opt-out-Verfahren zum Gegenstand hatten.

Als unzureichend abgelehnt werden sowohl ein selbstregulativ von den Tracking-Netzwerken einzusetzendes Icon zur Information des Nutzers als auch das Angebot, über eine zentrale Seite Sperrcookies zu laden. Der geänderte Art. 5 Abs. 3 der E-Privacy Richtlinie (RL 2002/58/EG in der Fassung der RL 2009/136/EG) fordere eine klare und umfassende Information vor dem Setzen eines Cookies und ein Opt-In. Dabei sei unwesentlich, ob der Cookie personenbezogene Daten speichere. Tracking-Dienste setzten eindeutige Identifikatoren ein, die ein Erfassen einzelner Nutzer erlaubten und seien damit selbst ein personenbezogenes Datum.

Als zulässige und geeignete Varianten neben Pop-up Fenstern zur Information und Einwilligung werden vorgeschaltete Seiten, die von Heise vorgeschlagene [2-Klick Lösung](#), ein [statisches Informationsbanner](#) und Tracking verhindernde Browser-Voreinstellungen angesehen. Auch genüge eine einmalige Einwilligung für ein gesamtes Werbenetzwerk.

Damit rücken – aus berechtigten Gründen – statt der IP-Adresse die Tracking-Cookies als Identifizierungsmerkmal ins Zentrum der Regulierung. Mit Secorvo Security News 01/2012, 11. Jahrgang, Stand 01.02.2012

der überfälligen Umsetzung der „Cookie-Richtlinie“ werden daher die mühsam erreichten Übereinkünfte mit Tracking-Betreibern wie z. B. Google Makulatur: Der Einsatz von Google Analytics verstößt dann – ohne eine informierte Einwilligung des Seitenbesuchers – gegen geltendes europäisches Datenschutzrecht. Bei Verstößen wird mit Abmahnungen der deutschen Datenschutz-Aufsichtsbehörden zu rechnen sein.

### Smartphone-Sicherheit

Vor etwa zehn Jahren hat die NSA mit [SELinux](#) eine Linux-Variante veröffentlicht, die dank starker Sicherheitsmechanismen erheblich widerstandsfähiger gegen Angriffe ist als ein „normales“ Linux.

Am 06.01.2012 veröffentlichte die NSA die erste Version von [SEAndroid](#), ein Projekt, in dem die SELinux-Architektur auf Android übertragen wurde. Derzeit steht noch keine fertige Firmware zur Verfügung; interessierte Nutzer müssen daher noch selber kräftig Hand anlegen.

Das hinter SELinux und SEAndroid stehende Sicherheitsmodell ist durchaus geeignet, verschiedenen Sicherheitsproblemen wirksam zu begegnen. Ob es sich durchsetzen kann, hängt jedoch stark vom Engagement der Smartphone-Hersteller ab.

Die größte Herausforderung bei der Umsetzung ist die Komplexität der Konfiguration. Dafür müssen die Hersteller einen gut durchdachten Ansatz wählen, bei dem die Sicherheitsmechanismen wirksam werden, ohne dass sich der Nutzer mehr als nur oberflächlich mit dem System beschäftigen muss. Gelingt das nicht, wird auch ein unter SEAndroid betriebenes Smartphone bestenfalls „gefühlter sicherer“ sein.

### Authentifikation systematisch

Am 12.12.2011 erschien, fünf Jahre nach der Erstfassung, die erheblich überarbeitete und erweiterte Revision 1 der [Electronic Authentication Guideline \(SP 800-63\)](#) des [NIST](#). Darin wird das Thema Authentifikation über unsichere Netze von der initialen Registrierung der Teilnehmer bis hin zum Weiterreichen der Information über den authentifizierten Benutzer an nachgeordnete Anwendungen systematisch betrachtet. Vier aufeinander aufbauende Sicherheitsniveaus und konsistente Anforderungen an alle Nutzungsphasen eines Authentifikationsverfahrens werden definiert.

Auch wenn das Dokument primär für US-Behörden gedacht ist und daher auf Behördenstandards wie [FIPS-140-2](#) oder [PIV-Cards](#) abhebt, so bietet es doch eine sehr gute Grundlage für eine angemessene Präzisierung des oft schwammig verwendeten Begriffs „starke Authentifikation“.

### Kuck mal, wer da...

Der am 28.11.2011 publizierte [20. Tätigkeitsbericht \(2009-2010\)](#) des [Landesbeauftragten für den Datenschutz Niedersachsen](#), Joachim Wahlbrink, legt einen Schwerpunkt auf das Thema Videoüberwachung. So wurden in einer großen Fastfood-Restaurantkette nicht nur ein hoher Anteil unzulässiger Überwachungen, sondern auch zahlreiche Datenschutzmängel bei der Installation, Dokumentation und der Erfüllung allgemeiner Datenschutzanforderungen festgestellt.

Einer Beschwerde folgend wurden vier Restaurants der Kette geprüft, die mit insgesamt 94 Kameras förmlich gespickt waren. Diese überwachten vielfach den Sitzbereich – unzulässig nach einem Urteil des [AG Hamburg von 2008](#), denn in öffentlichen

Bereichen, in denen sich Personen typischerweise länger aufhalten, tritt das Beweis- und Präventionsinteresse des Betreibers hinter das Persönlichkeitsrecht der Betroffenen zurück. Nicht vom Personal einsehbare Bereiche dürfen nur noch für eine Übergangszeit weiter beobachtet werden; finden keine nennenswerten Vandalismus-Vorfälle statt, ist auch diese Überwachung mangels Erforderlichkeit einzustellen.

Das betroffene Unternehmen hat infolge der Prüfung seine gesamten einschlägigen Richtlinien überarbeitet, eine Löschfrist von 72 Stunden eingeführt und von den Franchisenehmern die Bestellung von Datenschutzbeauftragten eingefordert.

Auf die andauernde Ausweitung von Videoüberwachungen in Unternehmen reagieren die Aufsichtsbehörden mit einer Intensivierung der Prüfungen. Eine kritische Überprüfung der eigenen Prozesse und Löschfristen erscheint daher angeraten.

## Verwirrungs-Taktik

Man stelle sich vor, für jedes Produkt, das man in einem Kaufhaus erwerben möchte, müsste man einen separaten Eingang zum Gebäude mit eigenem, individuellen Ladenschild nutzen. Bald wüssten viele Kunden nicht mehr, bei wem sie da eigentlich gerade einkaufen.

Vielleicht weil die Türen im Internet billiger sind, reservieren viele Marketing-Experten – zur Betonung der Wichtigkeit einer Aktion oder eines neuen Angebots – bei jeder sich bietenden Gelegenheit eine neue [Second-Level-DNS-Domain](#), anstatt [Subdomains](#) des eingeführten Namens zu nutzen. So ist es nicht ungewöhnlich, wenn man bei der Online-Buchung eines Flugtickets von der Suche nach passenden Verbindungen über die Eingabe der

Daten bis hin zu Zahlung und Buchungsbestätigung über drei oder vier verschiedene Domains geleitet wird.

Dabei bereitet gerade diese verbreitete Praxis Phishing und ähnlichem Trickbetrug den Boden – denn die Nutzer gewöhnen sich durch die alltägliche Verwirrung an ständige Domain-Wechsel und schöpfen im Angriffsfall keinen Verdacht.

Richtig bedenklich aber stimmt es, wenn auch im Sicherheitsbereich derartigen Unsitten Vorschub geleistet wird. So [empfahl](#) das BSI am 11.01.2012 einen durchaus sinnvollen Test auf Befall mit der DNSChanger-Malware. Allerdings nicht auf den eigenen [amtlichen Webseiten](#), sondern unter der Domain [dns-ok.de](#). Wenig später tauchte unter dem homophonen Namen [dns-okay.de](#) eine (glücklicherweise harmlose) Verballhornung der Seite auf. Und auf der Webseite [bka-trojaner.de](#) wird unter der Titelzeile [botfrei.de](#) und den Logos von [BSI](#) und [eco](#) Hilfe gegen [Ransomware](#) angeboten – eine Webseite, die auf den ersten Blick keinen Deut seriöser wirkt als die Schadsoftware, vor der da gewarnt wird.

Kein Wunder also, wenn – wie am 12.01.2012 [berichtet](#) – zahlreiche Internetnutzer [fürchten](#), sich auf derartigen Seiten eher mit einem [Staats-trojaner](#) zu infizieren als Hilfe zu finden.

## Secorvo News

### Neue Seminare

Die stetige Weiterentwicklung auf dem Gebiet der Informationstechnologie bringt auch neue Herausforderungen für die IT-Sicherheit mit sich. Ab dem Frühjahr 2012 erweitern wir daher unser Seminarangebot und bieten mit [Aktuelle Herausforderun-](#)

[gen der IT-Sicherheit](#) vom 23.-24.05.2012 einen Überblick über neue Angriffsszenarien und Risiken sowie wirksame Schutzstrategien und Sicherheitslösungen.

Ihre IT-Security-Grundlagenkenntnisse können Sie vom 13.-15.03.2012 beim Seminar [IT-Sicherheit heute](#) auffrischen. Mehr über den Schutz von Web-Anwendungen erfahren Sie vom 21.-22.03.2012 beim Seminar [Verlässliche Web-Anwendungs-Sicherheit](#). Und vom 26.-30.03.2012 bieten wir mit dem [Certified Professional for Secure Software Engineering \(CPSSE\)](#) eine praxisorientierte Einführung in die sichere Softwareentwicklung. Freie Plätze gibt es auch noch für das [T.I.S.P.-Seminar](#) vom 07.-12.05.2012 – bei frühzeitiger Anmeldung bekommen Sie Ihr Exemplar des [T.I.S.P.-Buchs](#) rechtzeitig vorab zugesandt ([Programme und Online-Anmeldung](#)).

### Karlsruher IT-Sicherheitsinitiative

Einen fulminanten Start ins Jahr 2012 hatte die [Karlsruher IT-Sicherheitsinitiative](#) (KA-IT-Si), die die Kooperation mit dem Kompetenzzentrum für Angewandte Sicherheits-Technologie (KASTEL) am 26.01.2012 mit einer gemeinsamen Veranstaltung einleitete: „[Kryptographie zum Anfassen](#)“ lautet das Thema des Vortrags, der von einer einzigartigen Ausstellung historischer Kryptomaschinen aus zahlreichen Sammlungen begleitet wurde. Zum ersten Mal in der Geschichte der KA-IT-Si musste die Anmeldeliste zwei Tage vor der Veranstaltung wegen Überbuchung geschlossen werden.

Das nächste KA-IT-Si-Event zum Thema „[Sichere Softwareentwicklung](#)“ findet am 01.03.2012 im Schlosshotel Karlsruhe statt. Beginn ist um 18 Uhr. Wir freuen uns auf Ihre [Teilnahme](#)!

## Veranstaltungshinweise

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

Februar 2012	
08.-09.02.	<a href="#">22. SIT-SmartCard Workshop</a> (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	<a href="#">19. DFN Workshop „Sicherheit in vernetzten Systemen“</a> (DFN-CERT Services GmbH, Hamburg)
März 2012	
01.03.	<a href="#">Sichere Software-Entwicklung</a> (KA-IT-Si, Karlsruhe)
13.-15.03.	<a href="#">IT-Sicherheit heute</a> (Secorvo College, Karlsruhe)
14.-16.03.	<a href="#">Black Hat Europe 2012</a> (Blackhat, Amsterdam/NL)
21.-22.03.	<a href="#">Verlässliche Web-Anwendungs-Sicherheit</a> (Secorvo College, Karlsruhe)
26.-30.03.	<a href="#">CPSSE</a> (Secorvo College, Karlsruhe)
April 2012	
15.-19.04.	<a href="#">Eurocrypt 2012</a> (IACR, Cambridge/UK)
23.-26.04.	<a href="#">PKI</a> (Secorvo College, Karlsruhe)
April 2012	
07.-12.05.	<a href="#">T.I.S.P.-Schulung</a> (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)

## Fundsache

Am 20.12.2011 veröffentlichte die amerikanische Electronic Frontier Foundation (EFF) einen 24seitigen [Guide for Travelers Carrying Digital Devices](#) zum Grenzübertritt in die USA mit digitalen Daten – mit vielen hilfreichen Empfehlungen für US-Reisende.

## Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp

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.

