secorvo
security consulting

# Secorvo Security News

**Mai 2010**

## Die Vernunft stirbt nie

Wiederholt gerieten in den vergangenen Monaten „Social Networks“ wie Xing, StudiVZ und Facebook aufgrund von Datenschutzvorfällen in die Schlagzeilen. Aber keineswegs allen lagen Gesetzesverstöße zu Grunde.

Die meisten Fälle gründeten auf einem sehr grundsätzlichen Missverständnis. Denn anders als die Betreiber Glauben machen möchten, sind „Social Networks“ keineswegs ein digitales Abbild sozialer Netze. Sie entsprechen nicht den fein gewobenen sozialen Beziehungen, die Menschen knüpfen, und in denen sie in unterschiedlichen Rollen auftreten: als Partner, Geschwister, Gönner, Kumpel, Mitbewerber, Kollegen, Bekannte, Freunde. Selbst ähnliche Rollenbeziehungen unterschieden sich im Detail erheblich: Denn Freund ist nicht gleich Freund, und Kollege nicht gleich Kollege.

In echten sozialen Beziehungen werden Informationen und Gerüchte, Tipps und Erlebnisse sehr selektiv und kontextabhängig getauscht – keine zwei Personen aus dem sozialen Beziehungsgeflecht eines Menschen verfügen über dieselben persönlichen Kenntnisse. Auch Sprache, Stil und Ton der Kommunikation unterscheiden sich.

„Social Networks“ sind hingegen große Verflacher: Jeder „Freund“ („Kontakt“) kann auf dieselben Daten und Informationen zugreifen – jederzeit und fast überall. Jede Person erscheint allen „Freunden“ gegenüber in derselben undifferenzierten Rolle. Und wer „twittert“, spricht im selben Ton und Wortlaut zu allen „Followern“. Im „echten Leben“ käme kein Mensch auf die Idee, jedem, den er kennenlernt, gleich seinen Geburtstag in den Kalender einzutragen, seine bisherige berufliche Laufbahn und alle Qualifikationen lückenlos zu offenbaren, unbegrenzten Zugriff auf sein Fotoalbum einzuräumen und gleich noch die Liste aller Freunde und Bekannten vorzulegen.

Der Irrsinn wird wohl immer mehr Menschen bewusst: Angeblich planen 60 % der deutschen Facebook-Nutzer eine Kontolöschung. Offenbar ist ein Hype doch nicht das Ende aller Vernunft.

## Inhalt

secorvo
security consulting

# Security News

## DECT-Verschlüsselung gebrochen

Die Liste der gebrochenen proprietären Krypto-Verfahren ist erneut um eines angewachsen: Auf dem diesjährigen Fast Software Encryption Workshop (FSE 2010) vom 07.-10.02.2010 in Korea war das DECT-Verschlüsselungsverfahren an der Reihe.

Karsten Nohl, Erik Tews und Ralf-Philipp Weinmann gelang eine vollständige Rekonstruktion und die Feststellung ernsthafter Schwachstellen der DECT Standard Cipher (DSC). Dabei handelt es sich um eine 64-Bit Stromchiffre, die strukturell der GSM-Chiffre A5/1 ähnelt. Das Design beruht auf irregulär getakteten, linear rückgekoppelten Schieberegistern, einer Konstruktion, die typisch für Umgebungen ist, bei denen es auf eine möglichst einfache Implementierung und hohe Performanz ankommt.

Der Angriff ermöglicht es, den geheimen Schlüssel mit Hilfe leistungsstarker Hardware innerhalb weniger Stunden zu finden. Seit dem 04.04.2010 sind die Ergebnisse der Kryptoanalyse verfügbar.

Der Vorgang zeigt wieder einmal, dass von der Verwendung Hersteller eigener Kryptoverfahren dringend abzuraten ist – insbesondere, wenn das Verfahren (wie DSC) in zig-Millionen Endgeräten implementiert wird. Selbst wenn bald ein sicherer Nachfolger für DSC zur Verfügung stehen sollte, so wird DSC wegen seiner enormen Verbreitung noch auf Jahre in Gebrauch bleiben. Auch wenn es vom Standpunkt der Alcatel aus verständlich erscheint, mit einem geheim gehaltenen Verfahren Patentgebühren einnehmen zu wollen, so rechtfertigt dies nicht den Einsatz minderwertiger Algorithmen auf Kosten der Sicherheit der Verbraucher.

## Das BDSG ist nicht genug

Während die Unternehmen noch an der Umsetzung der jüngsten Novellierung des BDSG arbeiten, leitete der Hamburger Senat, veranlasst durch Google Streetview, am 07.05.2010 dem Bundesrat einen Gesetzesentwurf zur Ergänzung des BDSG (BR-Drs. 259/10) zu. Schon am 01.04.2010 hatte das Bundesinnenministerium (BMI) Eckpunkte zum Arbeitnehmerdatenschutz vorgestellt, die ebenfalls auf eine Gesetzesänderung zielen.

Beiden Vorschlägen ist eine überbordende Einzelfallorientierung gemein. Der Hamburger Entwurf sieht zahlreiche Ergänzungen des ohnehin wuchernden § 28 vor, darunter eine eingeschränkte Erlaubnis für georeferenzierte Straßenansichten und ein Widerspruchsrecht, sowie eine Benachrichtigungspflicht in einem neuen § 33a. Die Eckpunkte des BMI greifen insgesamt elf Beispiele auf, wie Videoüberwachung, Datenerhebung im Bewerbungsverfahren und private Kommunikationsmittelnutzung. Sie sollen in einem neuen Kapitel „Arbeitnehmerdatenschutz" zusammengefasst werden.

Aber beide Entwürfe springen zu kurz: Weder lösen sie grundsätzliche Fragen des Datenschutzrechts, noch bieten sie angesichts des zu erwartenden ständigen Anpassungsbedarfs Rechtssicherheit.

## iPhone der ID-Karten?

Zum 01.11.2010 wird der elektronische Personalausweis eingeführt. Das Bundesinnenministerium hat den Informationsbedarf angesichts des optionalen Charakters vieler Neuerungen erkannt und präsentiert nun eine eigene Website. Dort wird der ePersonalausweis als multifunktionaler Problemlöser angepriesen – quasi als iPhone der ID-Karten.

Die Informationen insbesondere über den elektronischen Identitätsnachweis sind sehr einfach gehalten. Es stehen eine Reihe von zum Teil fehlerhaften Formularen bereit. Vergeblich sucht man überzeugende Argumente für die Nutzung der neuen Funktionen, Hinweise zu dem für den elektronischen Identitätsnachweis erforderlichen Lesegerät oder die zu erwartenden Kosten. Auch über die benötigte Software schweigt sich das Portal aus.

Auf dem versteckt verlinkten Informationsangebot des BSI zu elektronischen Ausweisen finden sich die technischen und organisatorischen Einzelheiten – in Gestalt von fast 20 Technischen Richtlinien. Die schiere Menge und das Ausblenden kritischer Aspekte dürfte selbst dem professionell interessierten Publikum den Zugang erschweren. Dass der ePersonalausweis so zum Kultobjekt wird, darf bezweifelt werden.

## Fish and Cheese

Am 04.05.2010 erweiterte Google seine Sammlung von Tools zur Sicherheit von Web-Anwendungen um Jarlsberg – eine Microblogging-Anwendung, löchrig wie dänischer Käse. Sie soll wie z. B. auch OWASP WebGoat (siehe SSN 2/2010) zum Experimentieren mit Web-Schwachstellen einladen. Erst kurz zuvor hatte Google am 19.03.2010 als Pendant den Application-Scanner skipfish veröffentlicht. Nun vergnügen sich Fisch und Käse in unserem Labor miteinander ...

## Zeitläufte

Seit dem 08.04.2010 ist die stark überarbeitete Version 2 des SANS Investigative Forensics Toolkit (SIFT) als VMware mit über 350 Werkzeugen verfügbar. Wesentliche Neuerung ist der Logparser log2timeline, der mit Hilfe von timescanner alle Zeitinforma-

tionen aus über 23 Logformaten in 13 Artefaktklassen (u. a. EXIF, PCAP, Flash Cookies) automatisiert extrahiert. Nutzt man weitere in SIFT enthaltene Werkzeuge wie TSK (aktualisierte V 3.12 vom 23.05.2010) und RegRipper (modifizierte Windows-Version vom 10.05.2010), lässt sich die Menge korrelierbarer Zeitquellen vervollständigen. Durch eine abschließende chronologische Sortierung werden Aktivitäten eines untersuchten Systems oder interaktiven Benutzers im Zeitverlauf nachvollziehbar.

Da der überwiegende Teil der auswertbaren Informationen aus Verlaufsdaten besteht, die während der Systemnutzung automatisch anfallen, lässt sich so auf jedem länger genutzten (und unmanipuliertem) Linux- bzw. Windows-System das Nutzungsverhalten im Zeitverlauf rekonstruieren. Nicht nur Google und Facebook machen gläsern – auch das eigene System vergisst nie.

### MoPS 2010

Gut drei Jahre nach dem Month of PhP Bugs (MoPB 2007, siehe SSN 3/2007) wurde der Mai 2010 zum Month of PHP Security (MoPS 2010) umgewidmet. Bisher veröffentlichte das vierköpfige Initiatoren-Komitee neun Artikel und vierzig neue Bugs – ein weiterer Beleg, dass eine konzertierte Aktion zur Verbesserung der Sicherheit von Software auch kurzfristig enorme Fortschritte bewirken kann.

### Ein Quentchen Trost

„Das kann doch jedem mal passieren…“ – so wirkte die Bewertung des gefühlten Komplettausfalls des deutschen Internets am 12.05.2010 durch den Verursacher, die DENIC eG. Eine sehr knappe Stellungnahme trug zu zahlreichen Spekulationen über mögliche Ausfallursachen bei. Ein wenig gemildert wurde die Verunsicherung durch eine etwas ausführlichere Stellungnahme zu Hintergründen, zwei Tage nach dem Vorfall.

Vorbildlich dagegen der Blog-Eintrag, mit dem die ASF auf einen erfolgreichen Angriff auf das Apache Projekt vom 05.04.2010 reagiert hatte: Darin wurde der Angriff analysiert und sowohl technische als auch organisatorische Maßnahmen als Konsequenzen präsentiert. Auf diesem Niveau hätte man sich die Kommunikation des DENIC gewünscht – das hätte die verunsicherungsbedingten Folgeschäden des Ausfalls begrenzt. Auch Krisenkommunikation will gelernt sein.

## Secorvo News

### Alles auf eine Karte

Der Traum jedes Sicherheitsbeauftragten ist ein durchgängiges Identitätsmanagement, das Betriebsausweis, Gebäude- und Rechnerzugang integriert. Die KIT-Card, die mit der Gründung des „Karlsruher Instituts für Technologie“ (KIT) entstand, führt an diesen traumhaften Zustand heran – sie organisiert die Wege von über 8.000 Mitarbeitern der im Rahmen der Exzellenzinitiative ausgezeichneten Spitzenforschungseinrichtung.

Wie die technisch-organisatorische Umsetzung erfolgte, welche Klippen dabei zu umschiffen waren und was er aus dem Projekt gelernt hat, stellt Projektleiter Michael Gehle auf dem KA-IT-Si-Event am **24.06.2010** im Schlosshotel vor (Anmeldung).

### Lizenz zum Prüfen

Seit dem 01.05.2010 verstärkt Jochen Schlichting als BSI-lizensierter ISO 27001-Auditor auf der Basis von IT-Grundschutz das Secorvo-Grundschutz-Team.

### Best of Consulting

Ein leichter Anfall von Hybris, gewürzt mit einer Prise Chuzpe, ließ uns im vergangenen Jahr als kleiner David bei dem von der WirtschaftsWoche ausgelobten Beratungsranking „Best of Consulting 2010“ in der Kategorie „IT-Strategie“ antreten.

Nach drei Qualifikationsrunden, in denen die Qualität der Beratungsleistung aus der Sicht von zehn verschiedenen Kunden und ein ausgewähltes Referenzprojekt von einem wissenschaftlichen Fachbeirat analysiert und bewertet wurden, erreichte Secorvo im Februar 2010 das Finale.


Am 27.05.2010 wurde die Jury-Entscheidung über die Platzierung der Finalisten in Berlin bekannt gegeben – und Secorvo als Zweitplatzierter in der Kategorie IT-Strategie ausgezeichnet. Ein dritter Preis wurde wegen des großen qualitativen Abstands zu den weiteren Kandidaten nicht vergeben.

## Veranstaltungshinweise

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

| | |
|---|---|
| **Mai 2010** | |
| 30.05.-03.06. | Eurocrypt 2010 (IACR, Nizza/F) |
| **Juni 2010** | |
| 07.-08.06. | DuD 2010 (Computas, Berlin) |
| 07.-11.06. | TISP-Schulung (Secorvo College) |
| **Juli 2010** | |
| 15.07. | 2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe) |
| 24.-29.07. | Black Hat (Las Vegas/US) |
| 29.07.-01.08. | DEFCON 18 (Las Vegas/US) |
| **August 2010** | |
| 02.-04.08. | DFRWS 2010: Digital Forensic Research Workshop (Portland/US) |
| 09.-13.08. | 19th USENIX Security Symposium (Washington/US) |
| 15.-09.08. | Crypto 2010 (IACR, Santa Barbara/US) |
| **September 2010** | |
| 28.-29.09. | 7. Security Awareness Symposium (Secorvo, Ettlingen) |

## Fundsache

Zahlreiche Datenschutz-Verstöße haben in den vergangenen Jahren die Sensibilität für den Schutzbedarf personenbezogener Daten geschärft. Seit September 2009 sammelt das „Projekt Datenschutz“ Berichte über Datenschutzpannen – gute Munition gegen hartnäckige Verweigerer.


## Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, 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
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de