secorvo
security consulting

# Secorvo Security News

**September 2012**

## Das „Einweg-Paradigma“

Wer mit aufmerksamem Blick bewährte Schutzmaßnahmen in Bereichen außerhalb der Informationstechnik verfolgt, kann ein Phänomen beobachten, dass ich das „Einweg-Paradigma“ nennen will.

Ein Sanitäter oder Arzt, der sich und seine Patienten vor Infektionen schützen will, verwendet Einweg-Handschuhe, eine Einweg-Spritze, Einweg-Spatel und desinfizierte Einweg-OP-Kittel. Spurensicherer verhindern mit Einweg-Überschuhen und Einweg-Overalls die Kontamination eines Tatorts. Mit Einweg-Taschentüchern versuchen wir bei einem Schnupfen die Ansteckungsgefahr zu bannen. Den Fahrradhelm tauschen wir nach einer heftigen Kollision, und im Fahrzeug schützt der Einweg-Airbag die Insassen. Einweg-Alkoholtester bewahren die Testperson vor Infektion und den Tester vor Manipulation. Einweg-Gläser und –Trinkbecher aus Kunststoff oder Karton verhindern Schnittverletzungen, Einweg-Kontaktlinsen Unfälle. Kleine Kinder wickeln wir in Einweg-Windeln. Einweg-Verpackungen sorgen für hygienisch einwandfreie Lebensmittel, und Einweg-Umschläge schützen unsere Briefe während des Transports vor unbefugter Kenntnisnahme und Beschädigung.

Zwar belastet der Erfolg dieses Einweg-Paradigmas unsere Umwelt. Dennoch ist der Sicherheitsgewinn meist erheblich. In der modernen Informationstechnik hingegen – dort, wo Einweg-Lösungen nicht einmal die Umwelt belasten würden – beschränken wir uns geradezu antiquarisch auf's Reparieren: Die Bugs im Betriebssystem werden *gefixt*, der Browser beim Auftauchen von Zero-Day-Exploits *gepatcht*, die Web-Applikation mit Schwachstelle bekommt ein *Update*. Man stelle sich einmal vor, die Löcher in OP-Handschuhen würden in ähnlicher Weise über Jahre mit Flicken gedichtet.

Ach, wie schön wäre doch ein Einweg-Betriebssystem mit Einweg-Browser: morgens gestartet und abends gelöscht – keine Chance für Exploits, und der Patch-Marathon hätte endlich ein Ende.

## Inhalt

# Security News

## Nicht ganz zufällig

Forscher der Uni Cambridge veröffentlichten am 10.09.2012 eine Analyse, der zufolge Kriminelle an einem manipulierten POS-Terminal (vgl. SSN 08/2012) von einer eingelegten EMV-Bankkarte Transaktionsdaten abzapfen könnten, die sich später am Geldautomaten einspielen und in Bares umwandeln lassen. Die technische Ursache des Problems ist, dass manche Geldautomaten einen mehr oder minder vorhersagbaren (und damit unbrauchbaren) „Zufallswert" als Schutz gegen Replay-Angriffe verwenden. Bei der Lektüre des Papiers weiß man nicht, worüber man mehr den Kopf schütteln soll: Darüber, dass die Entwickler als „Unpredictable Number" (UN) einen fortlaufenden Zähler verwendeten, dass bei Abnahmetests nur geprüft wird, ob vier nacheinander erzeugte UN sich unterscheiden, oder dass man als Reverse-Engineer echte Geldautomaten günstig bei eBay erstehen kann.

Vielleicht ist es keine so gute Idee, wichtige Teile des Schutzes des Bankkunden in die Hand der Hersteller von POS-Terminals und Geldautomaten zu legen.

## Kontrollierter Benutzer

Ein prägnantes Beispiel, wozu die in SSN 08/2012 thematisierte Kontrolle der Benutzerschnittstelle durch einen Angreifer missbraucht werden kann, wurde am 04.09.2012 aufgedeckt. Dabei klinkt sich ein Man-in-the-Browser-Trojaner in eine Online-Banking-Sitzung ein und verweist auf „technische Probleme", derentwegen zunächst eine „Testüberweisung" durchgeführt, mit dem ChipTAN-Generator geprüft (sic!) und freigegeben werden müsse. Die Transaktion ist allerdings echt. Noch perfider ist der Trojaner, vor dem das BKA bereits am 15.07.2011 warnte (vgl. SSN 07/2011) – er täuscht eine irrtümliche Gutschrift auf dem Konto des Opfers vor, die nun „zurücküberwiesen" werden müsse. Schließlich gibt es da noch den im Juli 2012 aufgetauchten Telefonbanking-Trojaner, der zum „Datenvergleich" Angaben zum Kontoinhaber abfragt – zuletzt auch die Telefonbanking-PIN.

„Technische Probleme" sind ein bei Trojanern beliebter Vorwand für seltsame Anweisungen. Ihnen sollten daher mit größter Skepsis begegnet werden.

## Elektronische Rechnungen

Am 02.07.2012 hat das Bundesministerium für Finanzen in einem Schreiben an die obersten Finanzbehörden der Länder die Auswirkungen des nach längerer Verhandlung mit dem Bundesrat am 01.11.2011 verabschiedeten Steuervereinfachungsgesetzes 2011 (vgl. SSN 06/2011) auf elektronische Rechnungen präzisiert. Danach ist eine qualifizierte elektronische Signatur nicht mehr Voraussetzung für die umsatzsteuerrechtliche Anerkennung. Statt dessen muss lediglich ein „innerbetriebliches Kontrollverfahren" die korrekte Übermittlung der Rechnung sicherstellen. Stimmen die Angaben zu Leistung, Leistendem, Entgelt und Zahlungsempfänger dürfe davon ausgegangen werden, dass die Übermittlung fehlerfrei erfolgt ist. Dafür genügt zukünftig ein manueller Abgleich der Rechnung bspw. mit den zugehörigen Auftrags- oder Vertragsunterlagen. Die Zustimmung des Empfängers zum elektronischen Rechnungsversand kann nun auch durch Annahme der AGB oder konkludentes Handeln erfolgen.

Damit sind qualifizierte elektronische Signaturen wieder um eine „Killerapplikation" ärmer.

## VoIP- und UC-Bedrohungen

Gebührenbetrug bleibt eine der zentralen Bedrohungen gegen IP-basierte Telefonie (VoIP) und Unified Communications (UC). Dies geht aus dem im August veröffentlichten Bericht der SecureLogix Corporation vom 12.06.2012 hervor. Dort wurden für verschiedene Szenarien die jeweils relevanten Bedrohungen auf Grundlage der berichteten Vorfälle der vergangenen sechs bis 12 Monate identifiziert. Danach sind Einzelschäden von 100.000 US$ und mehr nicht ungewöhnlich. Sie entstehen entweder durch massive Anwahl von Premium- und Mehrwertdiensten oder durch eingedrungene Angreifer, die Telefoniekapazitäten „vermieten". Bei letzteren sind zudem weitere illegale Aktivitäten wie Voice SPAM oder Social Engineering möglich. Auch moderne Smartphones – eher Kleinformatcomputer mit Telefonie-App und nicht ausgereiften Sicherheitskonzepten – sind inzwischen Quellen für Gebührenbetrug, wie der Lookout Mobile Security Report 2012 vom 05.09.2012 bestätigt.

Unternehmen, die VoIP- oder UC-Anlagen einführen, dürfen derzeit nicht davon ausgehen, dass sie bereits gehärtete Systeme erhalten – im Auslieferungszustand sind diese meist auf maximale Funktionalität, nicht aber auf Sicherheit konfiguriert. Und das kann teuer werden, wie die angeführten Studien eindrucksvoll belegen.

## Mitarbeiterscreening

Der Bundesfinanzhof hat mit Urteil vom 19.06.2012 die Zulässigkeit von Mitarbeiterscreenings zur Erlangung eines AEO-Zertifikats „Zollrechtliche Vereinfachungen/Sicherheit" bestätigt. Die Erteilung des Zertifikats, das Erleichterungen bei der Abwicklung grenzüberschreitenden Warenverkehrs ermöglicht, ist abhängig von einer Überprüfung des Personals

des Antragstellers gegen die Listen der VO Nr. 2580/2001 und VO Nr. 881/2002.

Dabei handelt es sich um Antiterrorlisten, die durch den Europäischen Rat nach den Vorgaben des Gemeinsamen Standpunkts 2001/931/GASP erstellt werden. Sie unterliegen zwar einer halbjährigen Überprüfung, der Rechtsschutz der Betroffenen ist jedoch schwach ausgeprägt. Finanzielle Zuwendungen an die gelisteten Personen sind verboten.

Der Bundesfinanzhof sieht den Abgleich durch den Arbeitgeber durch § 32 Abs. 1 Satz 1 BDSG erfasst. Verwendet würden ohnehin nur Stammdaten der Beschäftigten. Dem Arbeitgeber stünde das Einholen einer Einwilligung der Beschäftigten oder der Verzicht auf das Zertifikat frei. Daher handele es sich auch nicht um einen staatlichen Eingriff. Den Abgleich als Bedingung für die Zertifikatserteilung zu verlangen, sei verhältnismäßig.

Während die Entscheidung für die betroffenen Unternehmen ein gewisses Maß an Rechtssicherheit schafft, ist die Begründung äußerst fragwürdig. Das Verlangen des Abgleichs ist weder durch den Zollkodex (ZK) noch durch dessen Durchführungsverordnung gefordert. Die Verhältnismäßigkeit des Abgleichs mit den konkreten Terrorlisten wäre daher unter Abwägung von Transparenzpflichten und Rechtsschutzmöglichkeiten der Beschäftigten zu prüfen gewesen. Die Ausführungen zur Möglichkeit der Einwilligungseinholung sind aus Datenschutzsicht mangels Freiwilligkeit zudem rechtlich falsch. Letztlich liegt das Problem jedoch bei der Praxis der Verdächtigenlisten, die im Hinblick auf Datenschutz und Rechtsstaatlichkeit berechtigt in der Kritik stehen.

### Speicherforensik

Am 18.09.2012 wurde Version 2.2 RC2 des Open-Source-Forensik-Tools Volatility freigegeben, das seit August die Betriebssysteme Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 sowie alle verfügbaren Service Packs und 64bit-Architekturen unterstützt. Insgesamt 67 Windows-Plug-Ins ermöglichen seitdem beispielsweise die Auswertung von Eventlogs im Hauptspeicher unter Windows XP und Server 2003 oder der Historie der CMD-Kommandozeile. Sogar Interaktionen in der GUI sind über die Erzeugung von Pseudo-Screenshots aus Fensterpositionsdaten rekonstruierbar.

Nun unterstützen 34 weitere Plug-Ins auch forensische Speicher-Analysen unter allen Linux-Derivaten (Debian, Ubuntu, OpenSuSE, Fedora, CentOS, Mandriva) ab Kernel 2.6.11 bis 3.5.

Volatility hat damit – wieder einmal – die Meßlatte für kommerzielle Lösungen in diesem Bereich deutlich höher gelegt und sollte heute bei keiner forensischen Incident Response mehr fehlen.

## Secorvo News

### Heute schon gefacebookt?

Ende 2011 waren nach einer Studie des Bitkom 74 % der deutschen Internet-Nutzer in einem „Sozialen Netzwerk“ registriert. Inzwischen dürften es einige mehr sein. Und in vielen Unternehmen drängen Marketing- und Personalabteilung auf eine Unternehmenspräsenz bei Facebook & Co. Meist ist ein erheblicher Teil der Mitarbeiter bereits „drin".

In den zu einem erheblichen Teil (Google+, facebook) von amerikanischen Anbietern betriebenen Social Networks lauern jedoch zahlreiche Fallen: Copyrightverletzungen, unkontrollierte Informationspreisgabe und Verstöße gegen Datenschutzbestimmungen gehören dazu.

Beim nächsten KA-IT-Si-Event "Heute schon gefacebookt?" am **08.11.2012** gibt der Jurist Michael Knopp einen Überblick über die wichtigsten Stolpersteine – und praktische Tipps, wie sie sich vermeiden lassen. Für ein besonderes Ambiente ist gesorgt: Erstmals ist die KA-IT-Si mit ihrer Veranstaltungsreihe in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen zu Gast. Das Tagungszentrum liegt ca. 10-15 Minuten Fahrzeit vom Karlsruher Hauptbahnhof entfernt. Beginn der Veranstaltung ist um 18 Uhr. Um Anmeldung wird gebeten. Wir freuen uns auf spannende Diskussionen und interessantes Networking!

### Wissen auffrischen

Unsere Seminare vermitteln nicht nur Grundlagen der IT-Sicherheit für Einsteiger in dem Gebiet (wie IT-Sicherheit heute, **20.–22.11.**), sondern stellen auch die "aktuellen Herausforderungen der Informationssicherheit" vor (**07.–08.11.**).

Experten mit mindestens drei Jahren Berufserfahrung in der Informations- bzw. IT-Sicherheit können ihre Kenntnisse mit dem T.I.S.P.-Zertifikat krönen (**12.–16.11.**). Das von Secorvo verfasste 500seitige T.I.S.P.-Buch Zentrale Bausteine der IT-Sicherheit (siehe die Leser-Rezensionen) ist im Preis eingeschlossen und wird allen Teilnehmern frühzeitig vor Seminarbeginn zugesandt.

Alle weiteren Seminarangebote, das druckfrische Jahresprogramm 2013 und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

## Veranstaltungshinweise

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

| Oktober 2012 | |
|---|---|
| 12.10. | 1. Freiburger Datenschutztag (vivaSoft/Datenschutz individuell, Freiburg) |
| 15.-17.10. | IDACON 2012, (WEKA-Akademie, Würzburg) |
| 16.-18.10. | it-sa 2012 (SecuMedia Verlag, Nürnberg) |
| 22.-26.10. | OWASP AppSec USA 2012 (OWASP Foundation, Austin/US) |
| 23.-24.10. | ISSE 2012 (TeleTrusT/eema, Brüssel) |
| 31.10.-03.11. | hashdays security & risk conference 2012 (DEFCON Switzerland, Luzern/CH) |
| **November 2012** | |
| 07.11. | German OWASP Day 2012 (OWASP Germany, München) |
| 08.11. | Heute schon gefacebookt? (KA-IT-Si, Ettlingen) |
| 07.-08.11. | Aktuelle Herausforderungen der Informationssicherheit (Secorvo College, Karlsruhe) |
| 12.-17.11. | T.I.S.P.-Schulung (Secorvo College, Karlsruhe) |
| 22.-23.11. | 36. DAFTA (GDD, Köln) |

## Fundsache

Als Pendant zu diversen Top Ten der Smartphone-Risiken veröffentlichte die enisa am 25.11.2011 einen Leitfaden, der die zehn wichtigsten Sicherheitsmaßnahmen detailliert, an die App-Entwickler denken sollten – leider noch ohne Plattform spezifische Hinweise zu iOS, Android & Co.


## Impressum

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

ISSN 1613-4311

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