secorvo
security consulting

Secorvo Security News

April 2012

Fluch der Vielfalt

Eigentlich ist es der Kern seines Erfolgs: Das „Multi-Purpose"-Konzept des Personal Computers eröffnete Rechenmaschinen einen Multi-Milliardenmarkt. Unvorstellbar heute, dass ein Computer nur eine spezielle Nutzung erlaubt: ein „Word-Prozessor" als Schreibmaschinenersatz, ein „Adress-Manager" statt des Registers im Kalender oder ein Handy, das nur zum Telefonieren taugt. Überlebende Exemplare solcher „Spezial-PCs" (gleichwohl Traum jedes Herstellers, da sie besseren Kopierschutz und höhere Margen bieten) verlieren stetig Marktanteile – wie derzeit Spielkonsolen und mp3-Player.

Das war in der Frühzeit des Computers anders. Ken Olsen, Präsident der Digital Equipment Corp., meinte noch 1977: „Es gibt keinen Grund, warum irgendjemand einen Computer in seinem Haus wollen würde." Im gleichen Jahr erschien der PET von Commodore, und vier Jahre später der IBM-PC. Damit war der Geist aus der Flasche: Heute erwarten wir, dass ein Computer, und heiße er auch „Smartphone" oder „Tablet", via Apps und Internet-Verbindung ein schier grenzenloses Angebot an Funktionen in sich vereint.

Für diese Funktionsvielfalt zahlen wir jedoch einen Preis. Wenn „alles geht", gehen auch Dinge, die wir uns weniger wünschen. Denn Schadsoftware ist vor allem eines – nämlich Software. Und ein „Multi-Purpose"-Gerät kann nicht entscheiden, ob eine App als Nutz- oder als Schadsoftware einzustufen ist. Auch den Hersteller können wir kaum dafür in Haftung nehmen, dass er auf seinen Geräten (fast) alles zulässt – denn genau das haben wir ja gewollt.

So kommt es spätestens beim Online-Banking zum Schwur. Denn ohne ein „One-Purpose-Device" zur Abwicklung unserer Bank-Transaktionen bleibt immer ein Trojaner-Risiko – das wir streng genommen schwerlich der Bank anlasten können, denn wir sind ja die Betreiber des „Alles-Geht-PC". Auch wenn die Einsicht schwerfällt: Wenn wir Sicherheit wollen, müssen wir auf Vielfalt verzichten. Und wenn wir – aus funktionalen Gründen oder aus Bequemlichkeit – nicht verzichten wollen, akzeptieren wir unvermeidlich das Risiko.

Inhalt

Security News

Zielgerade oder Sackgasse?

Auf der Crypto-Konferenz Mitte August 2005 wurde ein Angriff gegen SHA-1 präsentiert, der zwar noch nicht praktikabel aber effizienter als Brute-Force-Angriffe war. Seither wurde dieser Angriff verbessert, MD-5 praktisch gebrochen und auch ein Angriff auf die SHA-2-Familie schien in Reichweite.

In dieser Situation, in der die Welt der Krypto-Hashfunktionen, unverzichtbar für Signaturen, Integritätsschutz oder Schlüsselableitung, in Flammen stand, rief das NIST 2007 – ähnlich wie bei der erfolgreichen Entwicklung des AES – einen Wettbewerb für das Nachfolge-Hashverfahren SHA-3 ins Leben.

Nun biegt der Wettbewerb auf die Zielgerade ein: Fünf Finalisten sind benannt, unter denen noch in diesem Quartal der Sieger gekürt werden soll. Anders als beim AES hält sich das NIST jedoch bedeckt. Denn der vermeintliche Flächenbrand entpuppte sich als Strohfeuer: der SHA-2 erscheint heute sicherer als vor sieben Jahren. Und wie NIST-Vertreter Tim Polk am Rande des 83. IETF-Meetings Ende März 2012 erläuterte, wird SHA-3 in den meisten Anwendungsfällen langsamer sein als SHA-2.

Viele Mitglieder des Standardisierungsgremiums schrecken daher davor zurück, eine Unterstützung von SHA-3 verbindlich zu fordern. Angesichts langer Produktzyklen, die dazu führen, dass selbst SHA-2 heute noch nicht durchgängig genutzt werden kann, könnte dies jedoch ein riskantes Spiel sein: ein anderes „Fall-Back"-Verfahren gibt es nicht. Anwender sollten daher in den kommenden Jahren bei ihren Lieferanten auf eine Unterstützung des SHA-3 drängen.

Hintertür

Nicht auszurotten ist offenbar die Neigung von Herstellern, einen permanenten Remote-Zugang in ihre Geräte oder Programme in Gestalt versteckter „Hintertüren" einzubauen. So warnte das US-CERT am 24.04.2012 vor hard-kodierten Accounts in Produkten der Siemens-Tochter RuggedCom, die auch zwölf Monate nach der ersten Warnung nicht behoben sind, und wurde am 26.04.2012 bekannt, dass Telekom-Router vom Typ Speedport einen trivialen Zugang zu privaten WLAN-Netzen via Backdoor ermöglichen.

Diese Vorfälle reihen sich ein in eine lange Liste ähnlicher Probleme. Prominente Beispiele sind eine Schwachstelle in Siemens S7-Geräten vom August 2011 und eine kritische Lücke in Apple Quicktime vom August 2010.

Die Implementierung undokumentierter Zugänge zu Systemen oder Anwendungen ist, wie der Hausschlüssel unter der Fußmatte, eine Einladung für ungebetene Gäste – und gehört auch zu Testzwecken untersagt. Unternehmen sollten sich zumindest für kritische, von außen erreichbare Systeme die Abwesenheit solcher Hintertüren vom Hersteller zusichern lassen.

Haftung bei Filesharing

Das Bundesverfassungsgericht hat mit Beschluss vom 21.03.2012 gegenüber dem OLG Köln deutlich gemacht, dass es die Frage der Überwachungspflichten der Inhaber eines Internetanschlusses noch nicht für abschließend entschieden hält.

Das OLG Köln hatte unter Berufung auf das sog. WLAN-Urteil des BGH („Sommer unseres Lebens") vom 12.05.2010 Prüfpflichten des Anschlussinhabers auch für den Fall angenommen, dass der wahre Störer bekannt ist. Im entschiedenen Fall handelte es sich um den Sohn der Lebensgefährtin. Trotz entgegenstehender Rechtsprechung bspw. des OLG Frankfurt ließ das OLG Köln die Revision nicht zu. Das Bundesverfassungsgericht bejahte dagegen die Uneinheitlichkeit der Rechtsprechung und hielt die Revision für offensichtlich zulässig.

In einer Nebenerwägung hat das Bundesverfassungsgericht außerdem bewusst die Frage offen gelassen, ob die anwaltlichen Massenabmahnungen überhaupt eine taugliche und zu vergütende anwaltliche Leistung darstellen. Für die Unternehmen der Musikindustrie und ihre anwaltlichen Vertretungen bedeutet diese Entscheidung, dass mit weiteren Beschränkungen der postulierten Sorgfaltspflichten der Anschlussinhaber gerechnet werden muss – und dass Massenabmahnungen vielleicht in naher Zukunft kein funktionierendes Geschäftsmodell mehr darstellen.

Steueridentifikationsnummer

Mit Urteil vom 18.01.2012 hat der Bundesfinanzhof über die Rechtmäßigkeit der Vergabe der steuerlichen Identifikationsnummer entschieden. Schwerpunkt des Urteils bildet die Prüfung eines möglichen Verstoßes gegen das Grundrecht auf informationelle Selbstbestimmung der Betroffenen. Anhand der Gesetzesbegründung werden die hier Zwecke der Einführung sowie die über die Steueridentifikationsnummer abgewickelten Übermittlungen untersucht. Die Nummer gelte der Verfahrensvereinfachung, der Durchsetzung der Belastungsgleichheit der Steuerzahler und dem Bürokratieabbau. Dabei kommt das Gericht zu der Einschätzung, dass der Eingriff in die informationelle Selbstbestimmung durch die überragende Bedeutung der verfolgten Schutzziele gerechtfertigt wird.

Mit den Gefährdungen, die mit dem Eingriff verbunden sind, setzt sich das Gericht jedoch kaum auseinander und kommt so zum Schluss, dass die jeweiligen rechtlich verankerten Zweckbindungen der übermittelten Daten den Eingriff ausreichend beschränken. Die Frage, inwieweit bereits die Nummer als Mittel der Datenzusammenführung einen Eingriff darstellt, bleibt unberücksichtigt. Überhaupt werden als Risiken lediglich die gesetzlich vorgesehenen Einsatzzwecke betrachtet und der Eingriff infolge dessen als gering eingestuft.

Ähnlich kurz verneint das Gericht mit Verweis auf die pauschale Forderung nach technischen und organisatorischen Sicherheitsmaßnahmen in § 5 StIdV das Bestehen von Sicherheitsrisiken durch den Einsatz der Steueridentifikationsnummer.

Tatsächlich stellt das Urteil keine ernsthafte Auseinandersetzung mit den Datenschutzrisiken der Steueridentifikationsnummer dar. Die Rechtfertigung des Grundrechtseingriffs wird allein durch den Nutzen begründet – eine beängstigende Argumentation in einem freiheitlichen Rechtsstaat.

Secorvo News

Cloud kommt von Klauen. Oder?

Die Frage nach Sicherheit und Datenschutz beim Cloud Computing wird derzeit intensiv diskutiert. Wie lassen sich sensible Daten in der Wolke wirksam vor Missbrauch schützen? Und wie kann es gelingen, Anforderungen des Datenschutzrechts an Cloud-Computing-Dienste effektiv umzusetzen? Können diese Anforderungen überhaupt rechtsgestaltend und durch technisch-organisatorische Maßnahmen erfüllt werden, oder sollte man als verantwortungsbewusstes Unternehmen auf Cloud Computing verzichten?

Diesen und weiteren Fragen gehen Dirk Achenbach (Karlsruher Institut für Technologie) und Michael Knopp (Secorvo) beim nächsten KA-IT-Si-Event "Cloud kommt von Klauen. Oder?" am **10.05.2012** im Rahmen der Cloudzone 2012 nach. Die Impuls-Vorträge der beiden Referenten bringen die Herausforderungen auf den Punkt und skizzieren Lösungsansätze – anschließend heißt es „Ring frei" für eine intensive Diskussion.

Das Event beginnt diesmal ausnahmsweise bereits um 17 Uhr – und findet im Konferenzbereich der Messe Karlsruhe statt, wie gewohnt mit anschließendem Buffet-Networking. Als KA-IT-Si-Teilnehmer haben Sie außerdem die Möglichkeit, vorab die Cloudzone 2012 kostenfrei zu besuchen. Wir freuen uns auf Ihre Anmeldung!

4. Tag der IT-Sicherheit

Nach der hervorragenden Resonanz der vergangen Jahre freuen wir uns, Sie auch 2012 wieder zum **Tag der IT-Sicherheit**, einer Gemeinschaftsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL, einladen zu können. Die Veranstaltung beginnt am **12.07.2012** um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwarten Sie wieder spannende Vorträge rund um die IT-Sicherheit. Die Möglichkeit zur Online-Anmeldung finden Sie Kürze unter http://www.ka-it-si.de. Wir freuen uns auf Ihre Teilnahme!

Nächste Seminare

Das kommende T.I.S.P.-Seminar vom 7.-11.05.2012 ist ausgebucht – die nächste Gelegenheit zur Zertifizierung bieten wir am 17.-21.09.2012 sowie am 12.-16.11.2012.

Genug Zeit, um sich bis dahin den Sommerurlaub mit dem T.I.S.P.-Buch zu versüßen – oder eines der beiden folgenden Seminare zu besuchen, die Ihre besondere Aufmerksamkeit verdienen: Aktuelle Herausforderungen der Informationssicherheit (23.-24.05.2012) bietet eine kompakte Auseinandersetzung mit wesentlichen aktuellen Technologien und Trends. In zwei Tagen werden sechs Themenfelder und zugehörige Schutzmaßnahmen diskutiert. Das Seminar Datenschutzaudit: Best Practice (14.-15.06.2012) zeigt auf, wie es gelingt, auch ohne gesetzliche Maßgaben, sinnvolle und effiziente Datenschutzaudits zu planen und durchzuführen. Basis hierfür sind die umfassenden Erfahrungen des Referententeams.

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

Veranstaltungshinweise

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

Mai 2012	
07.-12.05.	T.I.S.P.-Schulung und Prüfung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
10.05.	Cloud kommt von Klauen. Oder? (KA-IT-Si, Kalrsuruhe)
23.-24.05.	Aktuelle Herausforderungen der Informationssicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK Kalrsruhe, CyberForum und KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)

Fundsache

Am 23.04.2012 erschien die 8. Ausgabe des Magazins „hack in the box“ als pdf. Darin werden unter anderem Angriffsmethoden wie die Nutzung von Browser Exploit Packs und gezielte Angriffe auf den Windows-Kernel anschaulich dargestellt.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, 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
(Subject: „subscribe security news“)

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