secorvo
security consulting

Secorvo Security News

August 2015

Das bislang beste Windows?

Was ein unaufgefordert erschienenes hartnäckiges Windows-Symbol wochenlang angekündigt hatte, stand am 29.07.2015 endlich zum Download bereit: Windows 10. Microsoft hat von Apple gelernt: Upgrades verteilen sich einfach besser, wenn sie nichts kosten. Und, man muss es Microsoft lassen, das Upgrade klappt schnell und problemlos. Bei Windows 8 fühlt es sich eher wie ein Update an, bei dem der nervige Metro-Screen abgeschaltet wird.

Nachdem Microsoft sich mit Windows 8 – einer komplett am Bedarf von Windows-Nutzern vorbeigegangenen Entwicklung – eine blutige Nase geholt hatte, sollte nun alles besser werden. Und eigentlich hatte man bisher das Gefühl, Microsoft hätte im Rahmen von Office 365 gelernt, dass – zumindest in Europa und speziell in Deutschland – der Datenschutz ein entscheidendes Kriterium ist.

Die Ernüchterung folgt nach der Installation, denn die nächste Stunde benötigt man dafür, die Datensammelwut – inklusive der Vergabe einer eindeutigen Werbe-ID – in unzähligen Einstellungen zu begrenzen. Vollständig abstellen lässt sie sich nicht. Dass man zur Installation ein Microsoft-Live-Konto benötigt, daran hatten sich Windows 8-Nutzer schon gewöhnt. Man konnte (und kann) anschließend immerhin den Offline-Modus aktivieren. Karl Klammers Nachfolgerin heißt nicht Siri, sondern Cortana und sammelt alles, was sie zu lesen oder hören bekommt.

Überflüssig zu erwähnen, dass ein Aufschrei zur Datensammelwut folgte. In Russland prüft der Generalbundesanwalt bereits Anzeigen. Microsofts Selbstwahrnehmung ist hingegen eine andere – und natürlich ist man unheimlich transparent.

Microsoft scheint das Prinzip „Lernen durch Schmerzen“ fest in seinen Entwicklungsprozessen verankert zu haben. Das bislang beste Windows? Funktional mag das stimmen, dennoch bleibt XP ungeschlagen. Vielleicht lernen sie es ja noch ...

Inhalt

secorvo
security consulting

Security News

Websites im Fokus

Bereits im Juni haben die Datenschutzaufsichtsbehörden von Hamburg, Bayern und Baden-Württemberg bekanntgegeben, gezielt Webportale auf Datenschutz und Datensicherheit zu prüfen. Derzeit prüfen die Aufsichtsbehörden die Datensicherheit noch auf der Grundlage von § 13 Abs. 4 TMG anhand von Fragebögen.

Nun sind die gesetzlichen Sicherheitspflichten aus dem TMG durch das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz verschärft worden. Es ergänzt § 13 TMG um weitere Pflichten: Geschäftsmäßige Anbieter von Telemedien haben nun technisch-organisatorische Maßnahmen zu ergreifen, um unerlaubte Zugriffe auf die genutzten technischen Einrichtungen zu verhindern. Außerdem sind die Angebote gegen Störungen, auch durch Angriffe, und unbefugte Zugriffe auf personenbezogene Daten nach dem Stand der Technik zu schützen. Eine Maßnahme hierzu sollen anerkannte Verschlüsselungsverfahren sein. Bei Verstößen können die Datenschutz-Aufsichtsbehörden Bußgelder von bis zu 50.000 € verhängen.

Bei Vorfällen wie dem Ashley Madison Hack müssen deutsche Anbieter künftig neben allem anderen ein Ordnungswidrigkeitsverfahren wegen unzureichender Sicherheitsmaßnahmen fürchten. Dabei werden sich dokumentierte Sicherheits-Maßnahmen und Sicherheitskonzepte auszahlen. Damit steigt der Druck auf Anbieter, sich systematisch mit Sicherheitsfragen auseinanderzusetzen. Der pauschale Verweis des Gesetzes auf Verschlüsselungstechnik wirkt allerdings ein wenig naiv.

Automatisierbare Bedrohungen

Am 31.07.2015 stellte Colin Watson das OWASP-Projekt „OWASP Automated Threat Handbook v1.00“ vor. Mit diesem Handbook will die Projektgruppe auf relevante, automatisierbare Bedrohungen von Webanwendungen hinweisen, die bisher höchstens am Rande betrachtet wurden. Wir empfehlen dieses Dokument jedem Entwickler, um geeignete Schutzmechanismen gegen solche weniger bekannten Bedrohungen zu implementieren. Entscheidern und Architekten sei zumindest ein Blick in die zweiseitige Zusammenfassung angeraten.

Experten und Laien

Google-Mitarbeiter publizierten am 23.07.2015 die Ergebnisse einer Studie, in der vergleichend untersucht wurde, welche IT-Sicherheitsmaßnahmen 230 befragte Security-Experten für wirksam halten und an welche Maßnahmen 290 interviewte Laien glauben. Von den zahlreichen detaillierten Ergebnissen der Studie überrascht vor allem die Erkenntnis, dass nur der „Umgang mit Passwörtern“ bei beiden Gruppen zu den fünf wirkungsvollsten Sicherheitsmaßnahmen zählt. Während Laien an die Wirksamkeit von Virenschutz glauben, setzen Experten darauf, ihre Systeme auf einem möglichst aktuellen Stand zu halten. Statt eines regelmäßigen Passwort-Wechsels bevorzugen Experten komplexe und einmalige Passwörter, die sicher aufbewahrt werden, oder Mehrfaktorauthentifizierung. Und nur Laien glauben daran, dass man einer Webseite ihre Vertrauenswürdigkeit ansehen kann.

Die Ergebnisse machen deutlich, dass eine verbesserte Aufklärung von Laien über wirksame IT-Sicherheitsmaßnahmen notwendig ist, wenn man nicht immer mehr Jessicas riskieren will.

Recht auf Vergessen? Vergiss es...

Das so genannte „Recht auf Vergessen“, das der Europäische Gerichtshof in seiner Google Spain-Entscheidung vom 13.05.2014 (SSN 5/2014) geprägt hat, bleibt weiter umstritten. Eine Anordnung der französischen Datenschutzaufsichtsbehörde CNIL vom 12.06.2015, beantragte Sperrungen weltweit auf alle Google-Domains zu erstrecken, beantwortete Google am 30.07.2015 in einem Blog-Beitrag: Das durch den EuGH formulierte „Recht auf Vergessen“ sei auf Europa beschränkt. Es sei keinem Land erlaubt, zu bestimmen, was in einem anderen Land zugänglich gemacht werde. Ansonsten drohe das restriktivste nationale Recht weltweit zum Maßstab der Freiheit im Internet zu werden. Dass Google dabei staatliche Zensurbestrebungen und Daten- oder Persönlichkeitsschutz in einen Topf wirft, zeigt deutlich das andauernde Unverständnis für europäisches Recht.

Derweil hat das OLG Hamburg über die Löschpflicht der Anbieter der Ursprungsseiten entschieden. Es bejaht einen Unterlassungs-Anspruch auch gegen den veröffentlichenden Website-Anbieter. Hintergrund war die Berichterstattung über ein eingestelltes Strafverfahren auf der Seite einer Tageszeitung. Da jedoch auch die Pressefreiheit der Beklagten zu berücksichtigen war, beschränkt sich der Anspruch in Fortsetzung der Google Spain-Rechtsprechung darauf, dass der Anbieter die Auffindbarkeit durch Suchmaschinen anhand des Namens verhindert.

Selbst wenn es gelänge, die Rechtsauffassungen dies- und jenseits des Atlantik anzugleichen, zeigt die OLG-Entscheidung, wie stark beim „Recht auf Vergessen“ das Persönlichkeitsrecht mit anderen Rechten wie bspw. der Pressefreiheit kollidieren kann. Das letzte Wort ist bei diesem Thema sicher noch lange nicht gesprochen.

secorvo
security consulting

Kali 2.0

Am 11.08.2015 erschien die rundum erneuerte Version 2.0 der *Penetration Testing Destribution Kali Linux*. Seit dem Schritt von Backtrack zu Kali Linux im Jahr 2013 konnte die Distribution ihre Stellung als de facto-Standard für Penetrationstests noch weiter ausbauen. Die neue Version bringt neben etlichen aktualisierten Tools, die das Herz eines jeden Testers höher schlagen lassen, auch einen Linux Kernel der Version 4.0 und diverse grafische Benutzerumgebungen mit.

Ab dieser Version erscheint Kali als Rolling-Release mit ständig aktuellen Paketen auf Basis von Debian Testing. Neben den typischen Plattformen stehen auch Versionen für ARM, die mobile Penetration Testing Plattform Nethunter und spezielle Images für den RaspberryPi 2 bereit. Ein Blick auf die neue Version lohnt also auf jeden Fall.

Pseudonyme Nutzung

Der Streit um die Klarnamenpflicht bei Facebook geht mit einer Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, vom 28.07.2015 in eine neue Runde. Darin wird Facebook Ireland Ltd. erneut verpflichtet, die pseudonyme Nutzung seines Dienstes zuzulassen und Sperrungen pseudonymer Accounts aufzuheben. Außerdem wird Facebook untersagt, Ausweiskopien zur Identitätsbestätigung zu verlangen. Anlass ist die Beschwerde einer Nutzerin, die von Facebook zur Angabe ihres echten Namens unter Vorlage einer Personalausweiskopie aufgefordert wurde und deren gesperrtes Profil Facebook gegen ihren Willen auf den Klarnamen umgestellt hatte, allerdings ohne das Profil freizuschalten.

Die Anordnung folgt in den Fußstapfen der im April 2013 durch das OVG Schleswig-Holstein kassierten Anordnung des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein. Caspar beruft sich erneut auf § 13 Abs. 6 TMG und bzgl. des Personalausweises auf § 20 Abs. 2 PAuswG. Durch die Google Spain-Entscheidung des EuGH vom 13.05.2014 (SSN 5/2014) ist das Hauptargument des OVG-Urteils von 2013 jedoch entfallen: Aufgrund der wirtschaftlichen Tätigkeit der in Hamburg niedergelassenen Facebook Germany GmbH kommt nun sehr wohl deutsches Datenschutzrecht zur Anwendung. Die Erfolgsaussichten von Caspers erneuter Anordnung sind damit erheblich gestiegen.

Secorvo News

Für Kurzentschlossene

Nutzen Sie noch im September die Möglichkeit, Ihre Erfahrungen und Kenntnisse zu vertiefen und mit einem Zertifikat zu krönen: Die T.I.S.P.-Schulung (**21.–25.09.2015**) bereitet auf die anschließende T.I.S.P.-Prüfung am 26.09.2015 vor und hilft, durch einen umfassenden Einblick in alle Gebiete der Informationssicherheit verbliebene Wissenslücken zu schließen. Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit".

Der ständigen Weiterentwicklung des Themas IT-Sicherheit trägt das Seminar IT-Sicherheit heute (**29.09.–01.10.2015**) mit der Behandlung aktueller Fragestellungen Rechnung. Hier erfahren Sie das Wesentliche über die aktuellen Entwicklungen und Bedrohungen und lernen Best Practice-Vorgehensweisen kennen, mit denen Sie Ihr Unternehmen wirksam schützen können.

Alle Termine und das komplette Seminarangebot finden Sie unter www.secorvo.de/college.

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung „Globale Überwachung und Zensur" des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade und Dirk Fox am **08.10.2015 um 18 Uhr** im Vortragssaal des ZKM | Karlsruhe einen Rück- und Ausblick auf die Geschichte und Entwicklung geheimdienstlicher Überwachung. Zur Einstimmung bietet das ZKM | Karlsruhe ab 17 Uhr für interessierte Teilnehmer eine Führung durch die Ausstellung an. Da die Zahl der Plätze beschränkt ist, bitten wir um rechtzeitige Anmeldung.

Führung und Vortragsveranstaltung finden auf Einladung des ZKM | Karlsruhe in Zusammenarbeit mit dem KIT und der Karlsruher IT-Sicherheitsinitiative statt. Sie sind **kostenfrei** – und setzen auch keine Fachkenntnisse voraus. Bringen Sie also gerne interessierte Freunde, Kollegen und Bekannte mit!

Im Anschluss an den Vortrag haben Sie die Möglichkeit, den Abend gemütlich im „mint - bistro.café.bar.catering" im Foyer des ZKM ausklingen zu lassen.

Weitere Informationen und die Möglichkeit zur Anmeldung zur Führung finden Sie auf www.ka-it-si.de. Wir freuen uns auf Ihr Kommen!

Veranstaltungshinweise

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

September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)
29.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
29.09.-01.10.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)>
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
13.-16.10.	Java Security (Secorvo, Karlsruhe)

Fundsache

Auf der diesjährigen 23. Konferenz DefCon präsentierten am 08.08.2015 Dan Petro und Oscar Salazar, wie sich die „Smart Safes“ Galileo des Herstellers Brink mit einem USB-Stick öffnen lassen. Auch hier hätte die Empfehlung „Schuster, bleib‘ bei deinem Leisten“ geholfen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial).

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