secorvo
security consulting

Secorvo Security News

Mai 2013

Im Überwachungsstaat

Am 15.05.2013 veröffentlichte eine interdisziplinäre Arbeitsgruppe der Deutschen Akademie der Technikwissenschaften (acatech) ein 36seitiges Positionspapier zur „Privatheit im Internet“. Neben der Neudefinition etablierter Begriffe („De-Kontextualisierung“ statt Zweckänderung und „Persistenz“ statt unzulässiger Speicherung) gibt das Papier Handlungsempfehlungen: Vermittlung einer „Kultur der Privatheit“ durch Bildung und Ausbildung, Eckpunkte für einen globalen Rechtsrahmen (wie informierter Einwilligung und der Möglichkeit zur Löschung und Befristung) und – schließlich sind die Autoren überwiegend Hochschullehrer – Geld für Forschung.

Wer die Wirklichkeit kennt, kann ob dieser bemühten Beschwörung eines „Kulturwandels“ durch Bildung, Gesetzgebung und Forschung nur den Kopf schütteln. Der Schutz personenbezogener Daten im Internet leidet weder unter einem Mangel an Regulierung oder Aufklärung noch unter zu wenig Verschlüsselung – sondern schlicht an einem dramatischen Umsetzungs- und Kontrolldefizit. Verstöße gegen geltendes Datenschutzrecht wie Webtracking, intransparente Datenschutzerklärungen oder unwirksame Einwilligungen sind so zahlreich wie augenfällig – und trotz wirksamer Instrumente zur Ahndung in der Regel ohne Konsequenzen für die Verantwortlichen. Daher leben wir bereits in einem Überwachungsstaat, der zumindest „ex post“ umfassende Persönlichkeitsanalysen erlaubt: Bewegungsprofile (Mobilfunk), Interessen (Webseitenbesuche, Recherchen), Käufe, Zahlungsverhalten und persönliche Kontakte (Social Networks). Davor schützen weder „Selbstdatenschutz“ noch Risikobewusstsein. Vielleicht hofften wir, dass die Datenmenge eine Analyse verhindert – dank „Big Data“ ist auch dieser Trost heute Makulatur.

Immerhin wirkt die Überwachung noch nicht „ex ante“. Doch es wird bereits mit Szenarien für Verhaltensprognosen experimentiert. Wenn wir es auch da zu einem Umsetzungsdefizit kommen lassen, ist die Fiktion von „Minority Report“ bald harte Realität.

Inhalt

Im Überwachungsstaat

Security News

Untergeschobene Straftat

Wer trackt mich da?

Cloud Computing Extreme

Update-Dschungel

Datenschutz bei Apple

Code-Erkenner

Secorvo News

5. Tag der IT-Sicherheit

Security by Design

Veranstaltungshinweise

Fundsachen

Security News

Untergeschobene Straftat

Nachdem das Bundeskriminalamt bereits im März vor einer neuen Variante der BKA-Ransomware gewarnt hat, die mit kinderpornographischem Material arbeitet, ist nun eine Variante im Umlauf, die kinderpornographische Fotos auf befallene Rechner lädt. Die Schadsoftware, die eine Rechnersperrung im Auftrag des BKA vortäuscht und zur (angeblichen) Wiederfreischaltung eine Geldüberweisung fordert, nutzt mit dieser jüngsten Variante die Bedrohung mit strafrechtlicher Verfolgung als zusätzliches Druckmittel.

Nach § 184b Abs. 4 Strafgesetzbuch (StGB) ist bereits der Besitz kinderpornographischer Darstellungen strafbar. Der Rechtsprechung genügt hierbei bereits ein bedingter Vorsatz, d. h. es reicht aus, dass Anhaltspunkte für den Besitz oder dessen Inkaufnahme vorliegen. Nach dieser Rechtslage bleibt den Betroffenen nur, ihre Datenträger sorgfältig auf von der Ransomware eingeschmuggeltes Material zu untersuchen und dieses unwiederbringlich zu löschen. Wer auf Nummer sicher gehen will, sollte den gesamten Datenträger vollständig überschreibend formatieren.

Auch die Übergabe der Datenträger an die Ermittlungsbehörden ist eine Option – verbleiben die Bilder jedoch nach Entfernung der Rechnersperrung auf dem Gerät, tritt unmittelbar die Strafbarkeit ein. Mit einer Weitergabe des Datenträgers an private Helfer kann zudem bereits der Straftatbestand des „einem anderen Verschaffens" erfüllt sein.

Im Unterschied zu bisherigen Ransomware-Varianten, die die Verfolgung verbreiteten Fehlverhaltens wie etwa Urheberrechtsverletzungen vortäuschten, setzt diese Variante das Opfer zusätzlich der Gefahr einer Strafverfolgung aus – zukünftig ein weiteres Problem der sicheren Tatsachenfeststellung bei forensischen Analysen und bei der Ahndung solcher Straftaten.

Wer trackt mich da?

Bekanntermaßen listen Datenschutzerklärungen auf Webseiten nur selten alle Datenweitergaben auf. Eine beeindruckende Visualisierung aller aktuellen Tracking-Verbindungen liefert das Firefox Browser-Plugin „Collusion" (Version 0.27 vom 28.03. 2013): Die Webtracker aller besuchten Seiten werden in einer dynamischen Grafik zusammengeführt. So werden die heimlichen „Datenkraken" des Netzes transparent: je größer der Netzknoten, desto mehr Verbindungen – und Daten über das Surfverhalten.

In den Händen einer Datenschutz-Aufsichtsbehörde ließe sich das Plugin unschwer zu einem Goldesel erweitern: Findet das Tool in der Datenschutzerklärung nicht alle verbundenen Domänen, könnte es automatisch einen Mahnbescheid drucken...

Cloud Computing Extreme

Schon seit einigen Jahren forscht IBM an Verfahren zur homomorphen Verschlüsselung. Derartige Verfahren würden es u. a. erlauben, Daten in der Cloud nicht bloß in verschlüsselter Form zu speichern, sondern auch verschlüsselt zu verarbeiten. Nur der Eigentümer der Daten könnte danach das (korrekte) Ergebnis einer Berechnung entschlüsseln.

Am 05.04.2013 gab eine Gruppe von IBM-Forschern die Software-Bibliothek HElib zur homomorphen Verschlüsselung als Open-Source Projekt frei. Ein praktischer Einsatz wird allerdings schnell an Grenzen stoßen: Momentan ist eine Berechnung auf verschlüsselten Daten ca. 100 Millionen Mal langsamer als die gleiche Berechnung auf dem Klartext. Dies ist jedoch ein ernst zu nehmender Fortschritt: Vor einem Jahr hätte die Berechnung noch einen um das Zehnfache höheren Aufwand erfordert.

Wer die Arbeitsweise solcher Kryptoverfahren besser verstehen will, muss nicht den Quellcode von HElib analysieren, sondern kann sich vergleichbare Algorithmen von der neuesten Version des Lernwerkzeugs CrypTool visualisieren lassen.

Update-Dschungel

Die Kennzahlen, die der IT-Sicherheitsdienstleister Secunia in seinem am 14.05.2013 veröffentlichten „Secunia Vulnerability Report 2013" präsentiert, sollten für IT-Verantwortliche Anlass sein, ihr derzeitiges Patch-Management kritisch zu prüfen: Der Report belegt, wie wichtig es ist, Sicherheitsschwachstellen bei *jeder* genutzten Software zu beobachten, sie zu bewerten und erforderlichenfalls darauf zu reagieren.

Zwar sind die Patch-Mechanismen der Hersteller in den vergangenen Jahren besser geworden. Dennoch bleibt die Herausforderung, viele Quellen im Blick zu behalten, wie der im April veröffentlichte „Secunia PSI Country Report – Q1 2013" an Zahlen für Deutschland belegt: Auf einem durchschnittlichen PC sind 75 verschiedene Programme installiert; davon stammt ca. 1/3 von Microsoft. Zwar wird Microsoft-Software in der Regel automatisch aktualisiert – allerdings betreffen 68% aller Schwachstellen Programme anderer Anbieter.

Daher muss ein PC schlimmstenfalls über bis zu 50 verschiedene Update-Mechanismen oder Quellen

aktuell gehalten werden – was zumindest im geschäftlichen Umfeld kaum manuell zu leisten ist.

Datenschutz bei Apple

Das Landgericht Berlin-Mitte hat die Apple Inc. Anlässlich einer Klage des Verbraucherzentrale Bundesverband e.V. (vzbv) am 30.4.2013 zur Unterlassung des Gebrauchs von weiten Teilen ihrer „Apple Datenschutzrichtlinie“ verurteilt.

Apple räumt sich in den beanstandeten Klauseln umfassende Verwendungsrechte an personenbezogenen Daten aus der Nutzung der Website, Bestellvorgängen oder der Verwendung von Apple Produkten ein. Das Landgericht sah in der Datenschutzrichtlinie durch die Einbeziehung in die Bestellvorgänge auf der Internet-Seite Allgemeine Geschäftsbedingungen und prüfte somit Datenschutzrecht nicht direkt, sondern unter dem Gesichtspunkt der unangemessenen Benachteiligung durch die Unvereinbarkeit der Bestimmungen mit wesentlichen Grundgedanken des Datenschutzgesetzes.

Beanstandet wurden vor allem die unterbliebene Differenzierung nach den Erhebungsvorgängen und den diesbezüglichen Rechtsgrundlagen sowie die Unbestimmtheit bei der Angabe, welche Daten zu welchen Zwecken verwendet werden – sofern überhaupt ein Zweck benannt wurde. Außerdem werde der Eindruck erweckt, dass der Nutzer unabwendbar in die Verwendung der Daten einwillige, teilweise sogar zu Lasten Dritter.

Bemerkenswert und im vorliegenden Kontext folgerichtig ist die Einordnung der Datenschutzrichtlinie, die ansonsten lediglich an § 13 Abs. 1 TMG gemessen würde, als AGB. Mit Apple hat sich ein weiteres Großunternehmen unter Berufung auf irisches Datenschutzrecht strengeren Vorgaben entziehen wollen, was auf diese Weise unterbunden wurde.

Die vorgenommenen Beanstandungen treffen in ähnlicher Weise eine Reihe weiterer App-Store und Shop-Anbieter, die sich bezüglich ihrer Datenverwendung wenig festlegen und eingrenzen. Sollte das Urteil rechtskräftig werden, dürften sich eine Reihe von Anbietern mit Unterlassungsansprüchen konfrontiert sehen.

Code-Erkenner

In Zeiten, in denen selbst Cyberwar-Trojaner Open-Source-Software enthalten, ist es für den Reverse Engineer, Qualitätsprüfer oder Forensiker hilfreich, schon vorab zu wissen, welche bereits bekannten Software-Bausteine ein zu untersuchender Binärcode beinhaltet.

Dies will die neue Code-Suchmaschine „Rendezvous“ erleichtern, die von Forschern in Cambridge am 14.05.2013 vorgestellt wurde. Eine Online-Demoversion kann bereits beliebige Linux Binaries (im x86/ELF Format) gegen eine große Liste bekannter Open-Source-Software abgleichen.

Secorvo News

5. Tag der IT-Sicherheit

Gemeinsam mit dem CyberForum e.V. und der IHK Karlsruhe und KASTEL veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **04.07.2013** den „5. Tag der IT-Sicherheit“. Beginn ist um 14.00 Uhr im Haus der Wirtschaft (Saal Baden) der IHK Karlsruhe.

Die diesjährige Keynote widmet sich der Sicherheit mobiler Geräte. Prof. Dr. Rainer Gerling, Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, nimmt eine vergleichende Sicherheitsanalyse gängiger Handy-Betriebssysteme vor. Es folgen weitere praxisnahe Fachvorträge zu den Themen Cybersicherheit und Grundschutz (BSI), Umgang mit Sozialen Netwerken (Deutsche Bahn) und IT-Security Management Strategie (SAP). Gelegenheit zum fachlichen und persönlichen Erfahrungs- und Gedankenaustausch bieten die Networking-Pausen.

Nähere Informationen zum Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter www.tag-der-it-sicherheit.de

Wir freuen uns auf Ihre Anmeldung!

Security by Design

Die wirksame und vorausschauende Implementierung von Sicherheit in komplexen Lösungen ist auch dann noch eine Herausforderung, wenn die Entwicklung sich konsequent an dem Prinzip „Security by Design“ orientiert – und erst recht, wenn Sicherheit erst im Laufe des Entwicklungsprozesses als zusätzliches „Feature“ angeflanscht wird.

Einen systematischen und vertieften Einstieg in „Security by Design“ bietet das von Secorvo entwickelte Seminar „Security Engineering – Sichere Systeme durch Security by Design“ vom 23.-26.09. 2013. Inzwischen kann die dort erworbene Qualifikation auch mit einem T.E.S.S.-Zertifikat nachgewiesen werden.

Die Möglichkeit zum Erwerb des T.I.S.P.-Zertifikats bietet Secorvo im Herbst 2013 gleich an zwei Terminen. Alle weiteren Seminartermine sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Veranstaltungshinweise

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

Juni 2013	
03.-07.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
05.-07.06.	Entwicklertag 2013 (VKSI & ObjektForum, Karlsruhe)
10.-11.06.	Cybersecurity 2013 (Handelsblatt & EUROFORUM, Berlin)
13.06.	Swiss Cyber Storm 4 (Swiss Cyber Storm Association, Luzern/CH)
17.-18.06.	DuD 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Juli 2013	
04.07.	5. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
08.-10.07.	IFIP Sec 2013 (IFIP, Auckland/NZ)
27.07.-01.08.	Blackhat USA 2013 (Blackhat, Las Vegas/US)

Fundsachen

Wie wirksam Antivirenschutz ist und wie gefährlich das Leben ohne, das zeigt der aktuelle „Microsoft Security Intelligence Report“ (SIR), Volume 14. Seit Juni 2006 werden in dem halbjährlichen Bericht Daten von Microsoft-Produkten und -Diensten analysiert – eine der umfassendsten Datenbasen der Windows-Welt.

Ein Bild sagt mehr als tausend Worte: Nach diesem Motto präsentiert das US-amerikanische Unternehmen ThreatMetrix wesentliche Gefährdungen und Schutzmaßnahmen für die mobile Arbeit in unsicheren Umgebungen in einer anschaulichen Infografik mit dem sprechenden Titel „Don't Lose Your Caffeine Buzz to Cybercrime“.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Sven Köhler

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