secorvo
security consulting

Secorvo Security News

September 2015

Eingebettetes Vertrauen

Kaum ein Gerät, das heute nicht von Software gesteuert wird. Die wenigen verbliebenen rein mechanischen Lösungen (wie batteriefreie Armbanduhren) genießen bereits Kult-Status.

Zwar wissen wir, dass Software fehlerhaft sein kann. Aber Fehler fallen auf: Abweichendes Systemverhalten zeigt sich bei Tests, und bei unspezifischen Fehlern stürzt das System meist ab. Daher ist unser Vertrauen in ursprünglich mechanische, aber zunehmend von Software gesteuerte Geräte meist unbeeinträchtigt geblieben. In der Regel ist das auch vernünftig: Eine Waschmaschine, die zu heiß wäscht, erkennen wir an eingelaufener Wäsche. Eine Uhr, die die falsche Zeit anzeigt, erkennen wir beim Vergleich mit anderen Zeitanzeigen. Und ein Auto, bei dem die Motorsteuerung schwächelt, erkennen wir am Fahrverhalten.

Allerdings gibt es auch Systeme, bei denen Fehler weniger offensichtlich sind und eine Überprüfung schwierig ist. Wie sollten wir die Korrektheit eines Taxameters prüfen? Oder die des Kilometerzählers im Gebrauchtwagen? Und wie sollten wir bei einem Spielautomaten feststellen, dass das Gerät auch die gesetzlich vorgeschriebene Menge an Gewinnausschüttungen einhält? Genau aus diesen Gründen hat das Bundesverfassungsgericht 2009 dem Einsatz von Wahlcomputern bei Bundestagswahlen einen Riegel vorgeschoben.

Üblicherweise werden solche Geräte unabhängig geprüft. Aber wie gut kann eine solche Prüfung sein, deren Umfang weit unter dem einer „Common Criteria"-Zertifizierung liegt? Prüft der Prüfer den Source-Code? Und was ist, wenn Schadcode über die Programmierumgebung in den ausführbaren Code gelangt (siehe diese SSN)?

Die Entwicklung effizienter Verfahren, mit denen die Vertrauenswürdigkeit solcher Systeme sichergestellt und transparent gemacht werden kann, wird eine große Herausforderung der Zukunft sein.

Inhalt

secorvo
security consulting

Security News

Komplexität killt Sperrbildschirm

Ein YouTube-Video vom 20.09.2015 legte eine gravierende Schwachstelle der neuen Version 9 von Apples iOS offen: Sie ermöglicht es, den Sperrbildschirm zu umgehen und auf Kontakte und Bilder zuzugreifen. Dabei werden lediglich auf dem Sperrbildschirm verfügbare Funktionen wie der Sprachassistent Siri und die eingebaute Uhr verwendet.

Diese Verwundbarkeit reiht sich ein in zahlreiche gleichartige Schwachstellen, beispielsweise für iOS 7, Android 5 oder Windows 8. Die Ursache aller dieser Schwachstellen liegt darin, dass der Sperrbildschirm um immer mehr Funktionen erweitert wird. Wenn man aber erlaubt, dass ausgewählte Aktionen schnell und bequem durchgeführt werden können, ohne das Gerät zu entsperren, so vergrößert man zugleich die Angriffsfläche. Hersteller sollten den Sperrbildschirm nicht weiter als Platz zum Abladen von Apps oder als Schnellstartseite missverstehen, sondern als ein essentielles Sicherheitsfeature, das man besser nicht aufweicht.

Kamera-Attrappen

Nach einer kürzlich veröffentlichten Entscheidung des Landesarbeitsgerichts (LAG) Mecklenburg-Vorpommern vom 12.11.2014 (Az. 3 TaBV 5/14) unterliegt das Anbringen von Kamera-Attrappen im Außenbereich nicht der Mitbestimmung des Betriebsrats. In seiner grammatischen Auslegung des § 87 Abs. 1 Nr. 6 BetrVG stellt das LAG fest, dass eine Attrappe nicht zur Überwachung der Arbeitnehmer geeignet ist. Dass auch die Vorschriften des Bundesdatenschutzgesetzes (BDSG) keine Anwendung finden, hat der Bundesgerichtshof in einem Nachbarschaftsstreit bereits am 16.03.2010 entschieden (Az. VI ZR 176/09). Allerdings bestätigte er gleichzeitig, dass dennoch ein „Überwachungsdruck“ und damit ein Eingriff in das allgemeine Persönlichkeitsrecht vorliegen kann. Folglich kann ein zivilrechtlicher Unterlassungsanspruch gemäß §§ 1004, 823 BGB geltend gemacht und damit die Beseitigung der Kamera-Attrappe verlangt werden.

Anders als Datenschutzaufsichtsbehörden teilweise behaupten sind Attrappen demnach nicht wie echte Kameras zu behandeln. Unzulässig können sie im Einzelfall dennoch sein.

Passworttipps der Spione

Am 08.09.2015 hat der englische Geheimdienst GHCQ Hinweise zum Umgang mit Passwörtern veröffentlicht. Auch wenn man nach den Skandalen um die Geheimdienste einem solchen Dokument erst mal skeptisch gegenüber stehen mag, finden sich dort doch sinnvolle und angemessene, wenn auch nicht sonderlich überraschende Hinweise zum Umgang mit Passwörtern – gut dargestellt auf 13 Seiten. Anscheinend beschäftigen sich einige Mitarbeiter des GHCQ auch mit für die Sicherheit wertvollen Tätigkeiten.

DIN-Norm Löschkonzept

Der zuständige Arbeitskreis des DIN verabschiedete am 10.09.2015 eine weiterentwickelte Fassung der Leitlinie Löschkonzept als DIN-Norm 66398 – passend zur DIN 66399, die die Vernichtung von Datenträgern regelt. Seit Ende 2013 hatten die Deutsche Bahn, DATEV, Blancco, Secorvo und Toll Collect an diesem Projekt gearbeitet (siehe SSN 2/2014 und SSN 1/2015). Die neue DIN 66398 hilft bei der Entwicklung passender Löschkonzepte, insbesondere für personenbezogene Daten. Sie beschreibt die Elemente eines Löschkonzepts und stellt dar, wie mit Hilfe von Löschklassen Löschregeln für unterschiedliche Datenarten festgelegt werden können. Die Norm wird voraussichtlich Ende November im Beuth-Verlag erscheinen; eine englische Übersetzung ist geplant.

Für den Datenschutz ist die neue Norm ein großer Gewinn: Sie kann helfen, das Vollzugsdefizit beim Löschen personenbezogener Daten abzubauen.

Der Geist im iPhone

Am 20.09.2015 gestand die Firma Apple einen erfolgreichen Angriff auf den Appstore ein. Eine bisher unbekannte Anzahl von Apps (FireEye spricht von über 4000) ist durch Verwendung einer modifizierten XCode-Entwicklungsumgebung mit Schadsoftware infiziert worden. Apple arbeitet an der Bereinigung. Der Vorfall zeigt, dass selbst ein stark reguliertes Anwendungsökosystem anfällig für Angriffe sein kann. Dass modifizierte Compiler ein Sicherheitsproblem sein können, hat Ken Thompson schon 1984 in seinem berühmten Artikel „Reflections on Trusting Trust“ angesprochen. Sollten Software-Entwicklungswerkzeuge zum Einfallstor für Schadsoftware werden, wird dies die Entwicklung sicherer Software vor ganz neue Herausforderungen stellen.

Finger in die Wunde

Die Auftragsdatenverarbeitung (ADV) ist eines der wichtigsten Instrumente des Datenschutzes, wenn es um das Outsourcing der Verarbeitung personenbezogener Daten geht. Braucht man hierfür normalerweise einen Erlaubnistatbestand, ermöglicht es die gesetzliche Fiktion der ADV, diese durch einen Vertrag zu ersetzen. Dadurch wird der Auftragnehmer datenschutzrechtlich zum Teil des Auftrag-

gebers (verantwortliche Stelle), sodass keine – erlaubnispflichtige – Datenübermittlung an einen Dritten vorliegt.

Mit einer Pressemitteilung vom 20.08.2015 und einem Bußgeldbescheid in fünfstelliger Höhe legte das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) den Finger tief in die Wunde der praktischen Umsetzung: Oft machen es sich Auftraggeber allzu leicht und verwenden ADV-Vertragsmuster aus dem Internet, ohne dass diese auf den konkreten Fall angepasst werden. So sollte man beispielsweise mit einem Aktenvernichtungsunternehmen keine Rückgabe der Datenträger nach Erfüllung des Auftrags vereinbaren.

Insbesondere mangelt es häufig an konkret vereinbarten technischen und organisatorischen (Sicherheits-) Maßnahmen (TOM) – stattdessen werden nur allgemeine Floskeln angeführt oder eine Ankreuz-Liste beigefügt, die meist nur geringe Aussagekraft besitzt. Eine individuelle Vereinbarung und Prüfung der Auftragnehmer ist aber unumgänglich, um als Auftraggeber den gesetzlichen Aufsichts- und Kontrollpflichten zu genügen.

Datenschutzniveau der USA

Wir erinnern uns: Der österreichische Datenschutz-Aktivist Max Schrems hatte gegen die irische Datenschutzaufsichtsbehörde wegen der Speicherung der Daten europäischer Facebook-Nutzer in den USA und die damit einhergehende Überwachung durch US-Behörden vor dem irischen High Court geklagt. Dieser hatte unter Berufung auf die Safe Harbor-Entscheidung der EU-Kommission die Prüfung der Beschwerde abgelehnt. Im daraufhin von Max Schrems eingeleiteten Verfahren gegen den irischen Data Protection Commissioner hat der EuGH nun nach Ansicht des Generalanwalts zu prüfen, ob die Kommissionsentscheidung die nationalen Aufsichtsbehörden an eigenen Maßnahmen und Prüfungen hindert und ob unter Anwendung der Safe-Harbor-Grundsätze von einem angemessenen Datenschutzniveau in den USA ausgegangen werden kann. Angesichts der nicht bestrittenen massiven und nicht zielgerichteten Überwachungspraxis sowie des fehlenden gerichtlichen Rechtsschutzes wird letzteres von Generalanwalt Bot in seinen Schlussanträgen vom 23.09.2015 verneint.

Folgt man dieser Begründung steht jedoch nicht nur das Safe-Harbor-Abkommen auf dem Prüfstand, sondern indirekt auch die Wirksamkeit der Standardvertragsklauseln. Denn die staatliche Überwachungspraxis kann auch durch diese nicht ausgeschlossen werden. Bezogen auf deutsche Unternehmen wäre die Folge, dass Datenübermittlungen in die USA nur noch mit Genehmigung der Aufsichtsbehörden, mit Einwilligung des Betroffenen oder in den Ausnahmefällen aus § 4c Abs. 1 BDSG zulässig blieben. Für die betroffenen Unternehmen würde das zu gravierenden Problemen führen, da ein Großteil der Datenverarbeitungen mit US-Unternehmen faktisch rechtswidrig wären.

Secorvo News

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade (Karlsruher Institut für Technologie) und Dirk Fox (Secorvo) 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 zur Führung – eine Anmeldung zur Veranstaltung ist nicht erforderlich. Führung und Vortragsveranstaltung finden auf Einladung des ZKM Karlsruhe in Zusammenarbeit mit dem KIT und der KA-IT-Si 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.

Softwaresicherheit

Sicherheitsrelevante Schwachstellen in Software lassen sich durch systematisches Vorgehen bei der Softwareentwicklung vermeiden. Mit zwei Seminaren führen wir in die Sichere Softwareentwicklung (CPSSE, **16.–19.11.2015**) und das System Security Engineering (T.E.S.S., **09.–11.11.2015**) ein und bieten Ihnen anschließend die Möglichkeit, sich als *Certified Professional for Secure Software Engineering* (CPSSE) bzw. als *TeleTrusT Engineer for System Security* (T.E.S.S.) zu zertifizieren.

Alle weiteren Seminarangebote und den Seminarkalender für 2016 finden Sie jetzt auf unserer Webseite.

Veranstaltungshinweise

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

Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)
08.10.	Eine kurze Geschichte der Überwachung (KA-IT-Si, Karlsruhe)
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
20.-23.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association)
November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-11.11.	ISSE 2015 (TeleTrusT e.V./eema, Berlin)
10.-13.11.	T.E.S.S. - Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
23.-27.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Das BSI hat eine FAQ zum IT-Sicherheitsgesetz veröffentlicht, in der der Geltungsbereich des Gesetzes präzisiert und die Verpflichtungen der betroffenen Unternehmen zusammengefasst werden.

Impressum

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

ISSN 1613-4311

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

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