secorvo
security consulting

Secorvo Security News

Februar 2013

Zertifikatsträume

Der Traum von der Zertifizierung von IT-Sicherheit begann vor 43 Jahren: Die am 11.02.1970 publizierten „Security Controls for Computer Systems“, allgemein bekannt als „Ware Report„, waren eine Pioniertat. Fasching ist vorbei, daher soll nicht auf zertifizierte Wetterstationen eingegangen werden: der aktuelle ernste Fall der am 11.01.2013 von der Überwachungsbehörde auf den Boden verordneten Boeing 787 zeigt die Tücken und Grenzen von Zertifizierungsverfahren und wirft die berechtigte Frage auf, warum die FAA die Zertifizierung des Dreamliner auslagerte – ausgerechnet an eine Sparte von Boeing.

Die in „How Certification Systems Fail„ von Murdoch, Bond und Anderson analysierten Beispiele zeigen: das ist kein Einzelfall. So fiel nach der Kompromittierung eines als „Common Criteria evaluated“ beworbenen PIN Entry Device auf, dass der wesentliche Schritt einer Überprüfung durch eine unabhängige Stelle („Common Criteria certified“) fehlte. Und bei einem nach FIPS 140 zertifizierten Gerät wurden nicht alle Software-Komponenten in die Untersuchung einbezogen. Woraus man wesentliche Anforderungen an eine Zertifizierung ableiten kann: Der Prüfgegenstand muss exakt und sinnvoll festgelegt und die Prüfkriterien müssen genau beschrieben sein. Für die Sicherheit im realen Einsatz müssen auch Einsatzumgebung und Betriebsprozesse betrachtet werden. Untersuchungen müssen detailliert dokumentiert und durch eine *unabhängige* Prüfinstanz verifiziert werden. Die Prüfberichte sollten veröffentlicht werden, um Transparenz zu schaffen und die Aussagekraft eines Zertifikats beurteilbar zu machen.

So betrachtet ist das BSI mit Common Criteria (CC) und ISO 27001 auf Basis von IT-Grundschutz auf einem guten Weg. Sofern die externe Prüfbegleitung noch mal überdacht wird klappt es vielleicht auch mit der Anerkennung des Grundschutz-Zertifikats als ISO 27001 *native*.

Inhalt

Zertifikatsträume

Security News

Passworthäufigkeiten

Nebenschauplätze

ZAP 2.0.0

Nicht-Nadel im Nicht-Heuhaufen

TLS = Turn to Latest Standards

Secorvo News

Schau mir in die Augen, Kleines

Security by Design

Zertifiziert

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Passworthäufigkeiten

Die Wahrscheinlichkeitsrechnung gehört nicht zu den Dingen, die dem Menschen in die Wiege gelegt sind, wie ein aktuelles Beispiel illustriert. In einer Prognose für das Jahr 2013 rief Deloitte am 14.01.2013 das Ende des Passwortzeitalters aus: 90 % aller User-Passwörter würden Hacking-Angriffen nicht standhalten. Die Autoren berufen sich auf eine „recent study" – die sich bei einem Blick in die angegebene Quelle als nicht mehr ganz taufrischer Blog-Eintrag von Mark Burnett vom 20.06.2011 entpuppt. Danach hätten 98,1 % der Nutzer aus seiner Sammlung von ca. 6 Mio. User/Password-Paaren eines der 10.000 häufigsten Passworte gewählt. Lädt man Burnetts Liste dieser 10.000 Passwörter mit Häufigkeit herunter, ergibt sich ein anderes Bild: 1,875 Mio. der Accounts verwenden eines der Top-10.000-Passwörter – ein knappes Drittel (gut 31 %). Auch andere Angaben Burnetts lassen sich mit den Zahlen nicht belegen: nicht 71 %, sondern 613.000 User (ca. 10,2 %) wählten eines der Top-500-Passwörter, und nicht 40 %, sondern lediglich 275.000 User (ca. 4,6 %) nutzten ein Top-100-Passwort.

Was lernen wir daraus? Erstens: Traue keiner Quelle, die du nicht selbst geprüft hast. Zweitens: Traue keiner Wahrscheinlichkeitsaussage, die du nicht selbst nachgerechnet hast. Drittens: Wechsle deine Passwörter. Denn moderne Cracker arbeiten mit Wörterbüchern aus „geleakten" Listen echter Passwörter, die sie durch Einfügung von Ziffern, Sonderzeichen und Zeichenersetzungen variieren. 10.000 Passwörter testet ein Cracker wie ophcrack in Millisekunden – da ist eine Trefferwahrscheinlichkeit von 31 % trotz allem ziemlich beängstigend.

Nebenschauplätze

Das Verwaltungsgericht Schleswig-Holstein hat in einem Beschluss vom 14.02.2013 die sofortige Anwendbarbeit eines Bescheides des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein gegen Facebook verneint. Das ULD hatte Facebook aufgefordert mit sofortiger Wirkung pseudonyme Nutzerkonten zuzulassen und gesperrte Konten wieder freizugeben.

Wesentlicher Streitpunkt der vorläufigen Entscheidung war die Zuständigkeit des ULD und die Anwendbarkeit des deutschen Datenschutz- und Telemediengesetzes. Maßgeblich ist hierfür, ob die deutsche Niederlassung von Facebook die personenbezogenen Daten, die bei der Account-Nutzung erzeugt werden, verarbeitet oder ob dies durch die irische Facebook Ltd. geschieht (§ 1 Abs. 5 BDSG, Art. 4 Abs. 1 DSRL). Ist keine von beiden Stellen verantwortlich, gilt das deutsche Recht gegenüber Facebook Inc. in den USA. Das Verwaltungsgericht hat – ohne weitere Begründung – angenommen, dass die irische Niederlassung verantwortlich ist, somit sei irisches Datenschutzrecht anwendbar. Bezüglich der deutschen Niederlassung wird festgestellt, dass diese offenkundig nur Akquise- und Marketingaufgaben wahrnimmt.

Die Urteilsbegründung beschränkt sich auf einen Verweis auf die Angabe von Facebook, warum die irische Niederlassung nach den Kriterien der Art. 29 Gruppe tatsächlich relevant für die Datenverarbeitung sei. Hätte dieses Vorgehen Bestand, wäre es außereuropäischen Unternehmen möglich, durch schlichte Erklärung der „Relevanz" einer Niederlassung sich den Staat mit der schwächsten oder säumigsten Harmonisierung des Datenschutzes auszuwählen. Das ULD hat bereits die Fortsetzung des Rechtsstreits angekündigt.

ZAP 2.0.0

Zur Untersuchung von Webanwendungen sind Webproxys ein unerlässliches Werkzeug. Am 30.01.2013 wurde Release 2.0.0 des im Rahmen eines OWASP-Projekts entwickelten Zed Attack Proxy (ZAP) veröffentlicht. In der neuen Version wurden beispielsweise der Spider durch einen AJAX-Spider ergänzt und eine Erkennung von Sessionzuständen eingeführt. Weitere Neuerungen betreffen die API zum ZED, die die Entwicklung von Add-Ons ermöglicht. Diese können aus dem laufenden ZAP heraus online bezogen werden. Zusammen mit der Funktionalität von aktiven Scans rückt der ZAP somit immer mehr in die Nähe von kommerziellen Webanwendungs-Scannern. Noch fehlt eine kontinuierliche Entwicklung und Veröffentlichung von Schwachstellenmustern unter Berücksichtigung gängiger Frameworks; kommerzielle Anbieter werden hier auf absehbare Zeit im Vorteil bleiben. Für einen schnellen Scan ist der ZAP jedoch allemal gut.

Nicht-Nadel im Nicht-Heuhaufen

H. D. Moore, Chief Security Officer von Rapid 7 und einer der Hauptentwickler des Metasploit Frameworks, hat im Januar einen Bericht zu den Schwachstellen im UPnP-Protokoll veröffentlicht. Schockierend ist daran nicht so sehr, dass UPnP unsicher ist oder unsicher eingesetzt wird, sondern die hohe Zahl der exponierten Systeme. Laut Studie haben 81 Mio. Systeme im Internet auf UPnP-Anfragen reagiert; 23 Mio. davon sind mutmaßlich anfällig für einen Angriff, bei dem beliebiger Code auf dem betroffenen System ausgeführt werden kann. Die Studie zeigt auch, dass eine Durchsuchung des Internet nach einer einzelnen Schwachstelle machbar ist – die Nadel im Heuhafen ist nicht mehr schwer zu finden. Gewöhnliche

Suchmaschinen wie Google oder Bing helfen dabei, massenhaft weitere Nadeln – verwundbare Systeme – aufzuspüren. So ließ sich in wenigen Minuten ein ungesicherter Drucker einer größeren Organisation identifizieren, der von jedermann über das Internet „ferngewartet" werden konnte.

Und es geht noch besser: SHODAN und Punkspider sind spezialisierte Suchmaschinen für online verfügbare Systeme und Dienste, die bestimmte Merkmale – wie z. B. Standard-Zugangsdaten oder Schwachstellen – aufweisen. Ein solches Angebot mag empören. Allerdings: wer sich nackt auf die Straße wagt, darf sich nicht über die daraus resultierende Aufmerksamkeit beschweren. Die Härtung von im Internet exponierten Geräten ist unerlässlich, will man Integrität und Verfügbarkeit der eigenen Netze und Systeme nicht gefährden.

TLS = Turn to Latest Standards

SSL, das seit Ende des letzten Jahrtausends eigentlich TLS heißt, ist seit 1995 ein praktisch unverzichtbarer Baustein der Netzwerksicherheit – ein großer Erfolg für die Schöpfer des Protokolls. Im Laufe der Jahre wurden jedoch zahlreiche Angriffe auf TLS entwickelt, die ein am 31.01.2013 veröffentlichtes Papier zusammenfasst. Wie aktuell das Thema ist, zeigt sich daran, dass nur wenige Tage später, am 04.02.2013 eine neue TLS-Attacke („Lucky 13„) bekannt wurde. Wie die 2011 publizierte BEAST-Attacke zielt Lucky 13 auf den CBC-Verschlüsselungsmodus häufig genutzter Cipher-Suites. Auch das BSI hatte Pech, dass Lucky 13 für die Empfehlungen zum sicheren Einsatz von TLS zu spät kam, die am 09.01.2013 als zweiter Teil der TR-02102 erschien. Obwohl TR-02102-2 über Kryptoverfahren hinaus geht und bspw. Angriffe gegen die TLS-Renegotiation berücksichtigt, fehlen wichtige Schutzmaßnahmen wie das Deaktivieren der TLS-Kompression gegen die 2012 veröffentlichte CRIME-Attacke. Eine gute Ergänzung ist daher die SSL/TLS-Best-Practice-Empfehlung des BSI an Unternehmen vom 16.01.2013.

Fast alle bekannten Attacken lassen sich bei Verwendung des seit August 2008 aktuellen TLS 1.2 (und dessen Updates) beherrschen. Nur wird diese Version noch viel zu selten genutzt. Immerhin ist ein Fallback auf das seit 1996 überholte SSL 2.0 seit März 2011 nicht mehr standardkonform. Höchste Zeit, dass Hersteller und Anwender auf den aktuellen Standard umsteigen.

Secorvo News

Schau mir in die Augen, Kleines

Schwächen und Grenzen einer Passwort-Authentifizierung werden spätestens bei der Eingabe eines 12stelligen, alpha-numerischen Passworts mit Sonderzeichen auf einem Tablet-Computer offenkundig. Alternativen sind überfällig - und umstritten. Kannte man biometrische Verfahren zur Authentifizierung früher nur aus Hollywoodfilmen wie „Mission Impossible", so werden neben Fingerabdruckscannern und automatischer Gesichtserkennung auch Retina-Scans bald zum Alltag gehören. Doch welche datenschutzrechtlichen Rahmenbedingungen gelten und welche Risiken birgt eine solche Methode? Diesen Fragen geht Friederike Schellhas-Mende (KIT, Zentrum für Angewandte Rechtswissenschaft) in ihrem Vortrag „Datenschutzkonformes Retina-Scanning" beim nächsten KA-IT-Si Event am **14.03.2013** nach. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Gastgeber an diesem Abend ist das Fraunhofer IOSB in Karlsruhe, seit Anfang des Jahres Unterstützer der KA-IT-Si. Beginn ist um 18.00 Uhr. Wir freuen uns auf Ihre Anmeldung!

Security by Design

Wird Sicherheit von Anfang an bei der Konzeption eines Systems mitbedacht, lässt sie sich auch wirtschaftlich in hoher Qualität implementieren. Vor diesem Hintergrund hat Secorvo in Zusammenarbeit mit KIT und TeleTrusT das Qualifizierungszertifikat T.E.S.S. entwickelt. Mit der Schulung Security Engineering – Sichere Systeme durch Security by Design erwerben Sie die Zulassungsvoraussetzung für die T.E.S.S.-Prüfung. Nächster Termin: 23.-26.09.2013.

Am 15.-19.04.2013 bieten wir die erste diesjährige T.I.S.P.-Schulung an. Nutzen Sie die Möglichkeit, Ihre Qualifikation mit einem Feinschliff zu versehen und zertifizieren zu lassen. Weitere Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Zertifiziert

Am 03.02.2013 wurde das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz an die KomIT URS erteilt. Knapp zwei Jahre dauerte das von der CONNECT Karlsruhe vorbereitete Projekt von der Idee bis zum von Secorvo durchgeführten Audit. Der Aufwand hat sich nach Überzeugung von Frank Wondrak, Vorsitzender der Geschäftsführung KDRS/RZRS, gelohnt: Das Projekt habe konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau erzwungen – wichtige Voraussetzung für den ordnungsgemäßen Betrieb und die Vertrauenswürdigkeit für die Kunden der kommunalen Datenverarbeitung.

Veranstaltungshinweise

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

März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
12.-14.03.	IMF 2013 (Fraunhofer IAO, Nürnberg)
14.03.	Schau' mir in die Augen, Kleines (KA-IT-Si, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	BvD Verbandstag 2013 (BvD e.V., Berlin)
Mai 2013	
14.-16.05	13. Deutscher IT-Sicherheitskongress (BSI, Bonn)
14.05.	Forensik kompakt (Secorvo College, Karlsruhe)
15.-16.05.	14. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2013 (IACR, Athen/GR)

Fundsache

Die vom BSI 2012 initiierte „Allianz für Cybersicherheit„ hat inzwischen zahlreiche Dokumente bereitgestellt, viele davon in einem offenen Download-Bereich. Die Dokumente reichen von Broschüren zur Management-Sensibilisierung (16.10.2012) über aktuelle Einschätzungen zur Sicherheitslage bis zu konkreten Konfigurationsempfehlungen (bspw. zu SSL/TLS, 16.01.2013).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora (Editorial), 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