secorvo
security consulting

Secorvo Security News

Oktober 2014

Der Anforderungs-Zyklus

Es gibt Erkenntnisse, die sich wie Naturgesetze in unserem Weltverständnis eingenistet haben, obwohl sie sich den in den Naturwissenschaften bewährten Beweisverfahren und Modellbildungen entziehen. Dazu zählen das Pareto-Prinzip („80:20-Regel") – und der Hype-Zyklus von Jackie Fenn (Gartner) aus dem Jahr 1995, der den charakteristischen Verlauf der Aufmerksamkeit für ein Thema beschreibt.

Auch in der IT-Sicherheit lässt er sich beobachten. Tatsächlich beschreibt der Zyklus sogar die Entwicklung der Systemanforderungen. Ein Blick auf die fast 40jährige Geschichte der modernen Kryptografie macht das deutlich: Nachdem das RSA-Verfahren von 1978 erste Bekanntheit erlangt hatte, verbreiteten sich Implementierungen wie die Open Source-Software PGP, die viel Wert auf ein vom Anwender kontrolliertes Vertrauensmodell legte (welchen Schlüssel halte ich für authentisch?). Mit der Verabschiedung des ersten deutschen Signaturgesetztes im Jahr 1997, das höchste Sicherheitsvorgaben für Zertifizierungsdiensteanbieter enthielt und von einem zunächst 350 Seiten starken Maßnahmenkatalog des BSI begleitet wurde, erreichte der Anforderungs-Zyklus seinen Höhepunkt.

Es folgte der Absturz. Trotz EU-weit vereinheitlichtem Signaturgesetz konnte keine Anwendung eine nennenswerte Zahl von Anwendern gewinnen; PGP- bzw. S/MIME-Verschlüsselung blieben eine Nerd-Beschäftigung. Sicherheitsexperten, Gesetzgeber und Entwickler hatten übersehen, dass der Aufwand für hohe Sicherheitsanforderungen den Nutzen einer Verschlüsselungslösung reduziert.

Nun haben Edward Snowdens Veröffentlichungen den Ruf nach Verschlüsselung wieder aufleben lassen. Gesucht werden jedoch transparente Lösungen, bei denen die Verschlüsselung automatisch erfolgt – z. B. in einem lokalen „Verschlüsselungs-Proxy", der dem Benutzer Verwaltung und Prüfung öffentlicher Schlüssel abnimmt. Aus Sicherheitssicht vielleicht nicht perfekt. Aber anwendbar.

Inhalt

Der Anforderungs-Zyklus

Security News

Des Pudels SSL-Kern

ULD gegen Facebook

Google-Token

Beweis-Last

Orientierung für Cloud-Nutzer

Secorvo News

Lesestoff

Forschen gegen das Ausforschen

T.I.S.P. und T.E.S.S.

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Des Pudels SSL-Kern

Am 14.10.2014 veröffentlichte das Google Security Team eine neu entdeckte Schwachstelle der SSL/TLS-Protokollfamilie und taufte sie auf den Namen POODLE. Sie ermöglicht einem Man in the Middle-Angreifer zunächst ein Downgrade der Verbindung auf die veraltete Version SSLv3 und anschließend einen Angriff auf dessen Block-Cipher-Modus CBC. Da nur stark veraltete Browser die aktuelle TLS-Version nicht unterstützen und inzwischen alle SSLv3-Cipher-Suites angreifbar sind, sollte SSLv3 in allen Clients und Servern deaktiviert werden.

Ein Blick auf die lange Reihe von Schwachstellen der komplexen SSL/TLS-Suite legt nahe, bei Sicherheitssoftware auch deren Komplexität als grundsätzliches Sicherheitsproblem im Auge zu behalten. Das einfache Design der Crypto-Bibliothek NaCl weist einen Ausweg.

ULD gegen Facebook

Nach Auffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sind Fanpage-Betreiber für die Auswertung des Nutzungsverhaltens der Seitenbesucher durch Facebook verantwortlich. Daher hatte es gegenüber der Wirtschaftsakademie Schleswig-Holstein die Deaktivierung der Fanpage angeordnet, die das Verwaltungsgericht daraufhin in erster Instanz aufhob (siehe SSN 11/2013). Nun ist das ULD am 04.09.2014 in der Berufung beim Schleswig-Holsteinischen Oberverwaltungsgericht (OVG) gescheitert.

Bezüglich der Verantwortung der Fanpage-Betreiber kommt das OVG zu demselben Ergebnis wie die Vorinstanz: Fanpage-Betreiber seien zwar eigene Dienste-Anbieter; anders als bei einem Website-Betreiber, der Trackingcode in seine Seite einbettet, bestehe aber keinerlei Kontakt zu der Datenerhebung durch Facebook. Die Grundsätze der Störerhaftung kämen daher nicht zur Anwendung.

Zwar lässt das Urteil die Frage offen, ob das deutsche Datenschutzrecht anwendbar ist und die Datenverarbeitung durch Facebook dagegen verstößt. Entgegen den Verlautbarungen des ULD ist es jedoch überzeugend begründet. Für die Revision wird das ULD sich eine bessere Begründung für die Verantwortlichkeit der Seitenbetreiber einfallen lassen müssen. So einleuchtend und richtig die Forderung auch ist, dass ein Diensteanbieter nicht völlig von der Verantwortung für illegale Datenverarbeitungen seiner Dienstleister entbunden werden darf – sie muss sich auch mit rechtlichen Zurechnungsnormen begründen lassen.

Google-Token

Für die Anmeldung bei Google-Diensten wird schon länger die Zwei-Faktor-Authentisierung „2sv“ angeboten (siehe Editorial SSN 01/2013). Dabei wird ein Einmalpasswort als zweiter Faktor per SMS verschickt. Geklaute Login-Daten können so nicht dauerhaft genutzt werden; Angriffsmöglichkeiten durch Phishing bestehen aber nach wie vor. Und nicht jeder will Google seine Handy-Nummer anvertrauen – auch wenn diese Zurückhaltung in Zeiten von WhatsApp etwas hilflos anmuten mag.

Eine vielversprechende Alternative stellt der von Google am 21.10.2014 vorgestellte USB-Token „Security Key“ dar, der bereits ab sechs Euro erhältlich ist. Er unterstützt das PKI-basierte, von der Fast IDentity Online (FIDO-) Allianz spezifizierte Universal Second Factor Protocol (U2F). Neben Google gehören der Allianz Größen wie MasterCard, Microsoft, Nok Nok, NXP, Visa und Paypal an.

Leider ist das Verfahren eher für PC und Laptop gedacht als für das Anstecken an ein Smartphone. Auch ist zu hoffen, dass die Zahl der Allianz-Mitglieder steigt, damit man gute Authentisierung nicht irgendwann mit einem dicken Token-Schlüsselbund bezahlen muss.

Beweis-Last

Die Frage der Beweislastverteilung bei tatsächlichen oder vorgeblichen Hacking-Angriffen und Phishing-Attacken gewinnt zunehmend an Bedeutung. Das LG Coburg hat am 29.04.2014 den Streit über die Verbindlichkeit eines Ebay-Angebots zugunsten des Käufers entschieden, der einen Porsche Carrera sehr günstig erworben hatte. Der Ebay-Anbieter argumentierte, das Angebot sei nach einer Phishing-Attacke ohne seine Mitwirkung erstellt worden; der Porsche hätte gar nicht zum Verkauf gestanden.

Das LG Coburg sah den Beklagten für die unbefugte Account-Nutzung in der Beweispflicht. Einen Nachweis für die Phishing-Attacke konnte dieser jedoch nicht erbringen und die behauptete Anzeige bei der Polizei nicht belegen.

Das Urteil folgt dem Trend (siehe SSN 09/2014), das Risiko von Angriffen faktisch den System-Nutzern aufzubürden. Allerdings sind Phishing-Attacken und Hacking-Angriffe für Privatnutzer meist nur schwer nachweisbar; daher wäre wenigstens regelmäßig zu hinterfragen, ob das verwendete Authentifizierungssystem überhaupt geeignet ist, ein Handeln des Account-Inhabers hinreichend sicher zu belegen.

Orientierung für Cloud-Nutzer

Am 09.10.2014 veröffentlichten die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis die Version 2.0 ihrer „Orientierungshilfe Cloud Computing". Die Broschüre geht darauf ein, dass nicht alles, was technisch möglich, auch rechtlich zulässig ist. Es erläutert ausführlich die rechtlichen Rahmenbedingungen der Cloud-Nutzung, vor allem bei Anbietern mit Sitz außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR).

Vor dem Hintergrund der NSA-Affäre erklären die Datenschutz-Aufsichtsbehörden, dass sie sich vorbehalten, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen und zu prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind, solange der Zugriff ausländischer Nachrichtendienste nicht begrenzt wird.

Hunde, die bellen, beißen oft nicht: Die Verträge mit den relevanten Dienstleistern sind in der Regel nicht genehmigungspflichtig. Und die nebulöse Hoffnung auf eine „Begrenzung der Zugriffe ausländischer Geheimdienste" bleibt vage – und wäre, falls sie denn kommen sollte, wohl kaum überprüfbar. Davon abgesehen gibt das Dokument einen guten Überblick über die derzeitige Rechtslage.

Secorvo News

Lesestoff

Im Oktober erschien das Sonderheft 4/2014 iX Kompakt zum Thema „Security" – ein lesenswertes Kompendium mit 27 Beiträgen zu aktuellen Fragen der IT-Sicherheit. Zwei der Beiträge hat Secorvo beigesteuert: Einen Ansatz zur pragmatischen und effektiven Umsetzung von IT-Grundschutz in kleinen und mittleren Unternehmen von Kai Jendrian und Stefan Gora, und die Vorstellung eines strukturierten Vorgehens beim Testen der Sicherheit von Apps mit Hilfe von Threat Modeling von Dr. Yun Ding und Jörg Völker.

Bereits im August erschien ein Aufsatz von Kai Jendrian in Heft 8/2014 der DuD über den neu gefassten Standard ISO/IEC 27001:2013 – verfügbar zum Download auf unseren Webseiten.

Forschen gegen das Ausforschen

Abseits vom Katz-und-Maus-Spiel zwischen Angreifern und IT-Sicherheitsbeauftragten beschäftigt sich die IT-Sicherheits-Forschung mit Fragen von Übermorgen: Können wir Sicherheit beweisen? Wie können wir Vertrauen in der Cloud erzeugen? Welche Sicherheitsgarantien kann uns Technik liefern?

Auf der kommenden KA-IT-Si-Veranstaltung am **27.11.2014** werfen wir in zwei Vorträgen einen Blick in das Karlsruher Zukunftslabor der IT-Sicherheit und werden Lösungsansätze kennenlernen, die den Status des Laborversuchs bereits hinter sich haben. Gastgeber ist diesmal das Karlsruher „House of Living Labs" des Forschungszentrums Informatik. Für die ersten 25 schnell Entschlossenen bieten wir eine Führung durch dieses Zukunftslabor: vom intelligenten Stromzähler über Roboterkonzepte von morgen bis zum selbstfahrenden Auto mit Straßenverkehrszulassung (Führungsbeginn: 17 Uhr, Dauer: ca. 1 Stunde; Anmeldung unter www.ka-it-si.de).

Im Anschluss an die Veranstaltung haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking".

T.I.S.P. und T.E.S.S.

Vom 10. bis 14.11.2014 können Sie sich Ihre Kompetenz im Bereich Informationssicherheit mit dem Zertifikat „TeleTrusT Information Security Professional (T.I.S.P.)" bestätigen lassen (noch zwei freie Plätze). Nächster Termin des Zertifizierungsseminars im kommenden Jahr ist der 09. bis 13.03.2015. Als Teilnehmer des Seminars erhalten Sie die im August 2014 erschienene zweite, erweiterte Auflage des 700 Seiten starken Begleitbuchs „Zentrale Bausteine der Informationssicherheit" vorab zugesandt.

Die Komplexität von informationstechnischen Systemen wird zunehmend zum Sicherheitsrisiko. Dass und wie es dennoch möglich ist, komplexe Systeme sicher zu konzipieren und zu realisieren, ist Thema der viertägigen Zertifikatsschulung „T.E.S.S. – Sichere Systeme dank System Security Engineering" vom 17. bis 20.11.2014, die Sie durch die Teilnahme an der T.E.S.S.-Prüfung mit einem T.E.S.S.-Zertifikat abschließen können. Die Schulung zeigt, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (noch vier freie Plätze).

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/college.

Veranstaltungshinweise

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

November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.12.	German OWASP Day 2014 (OWASP Germany, Hamburg)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)
Januar 2015	
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)

Fundsache

Wer Videoüberwachung einsetzen will, muss einen Vielzahl gesetzlicher Vorschriften beachten. Wie das nach Auffassung der Aufsichtsbehörden richtig geht, zeigt die aktuelle Broschüre des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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