secorvo
security consulting

Secorvo Security News

November 2013

Potjomkin kehrt zurück

Man schrieb das Jahr 1787. Grigori Alexandrowitsch Potjomkin, Oberbefehlshaber der russischen Armee, Großadmiral der Schwarzmeerflotte, Generalgouverneur von Südrussland und Günstling (möglicherweise sogar heimlicher Ehemann) der Kaiserin Katharina der Großen hatte zahlreiche Siedlungen in Neurussland gegründet, aufgebaut und besiedeln lassen. Anlässlich einer Inspektionsreise in die neuen Provinzen soll er, um seiner Herrscherin zu imponieren, entlang des Wegs bemalte hölzerne Kulissen aufgestellt haben, die beeindruckende Bauwerke – Kirchen, Verwaltungsgebäude, Wehranlagen – vortäuschen sollten.

Unweigerlich blitzt die Erinnerung an diese Geschichte auf, liest man von den neuen Schutzmaßnahmen, die die Helfershelfer der NSA gerade ankündigen – wie die Verschlüsselung von E-Mails bei Microsoft, Google und Yahoo oder *Perfect Forward Secrecy* bei Twitter. Denn keine dieser Maßnahmen verhindert den Datenzugriff eines Nachrichtendienstes direkt über den Anbieter. Zu befürchten ist, dass mit dem wachsenden Laieninteresse an der IT-Sicherheit das allgemeine Tarnen und Täuschen zunimmt. Schon heute erleben wir, dass eine ‚Verschlüsselung' sich bei genauem Hinsehen als Zeichenersetzung oder gar als Kompressionsalgorithmus entpuppt, dass Passworte im Programmcode versteckt oder Remote-Zugänge durch Geheimhaltung der URL geschützt werden. In naher Zukunft könnten sich solcherart kompetenzfreie Implementierungen von Schutzmechanismen seuchenartig verbreiten.

Traurig daran: Auch gut implementierte, wirksame Schutzmaßnahmen werden unter Attrappenverdacht geraten. Wie Potjomkin: Seine Fassaden waren echt, wie nicht nur der inkognito mitreisende österreichische Kaiser Joseph II. später bestätigte. Das Täuschungsgerücht hatte ein Neider am Hofe Katharinas, der Diplomat Georg von Helbig, in die Welt gesetzt. Und es hält sich bis heute hartnäckiger als die Wahrheit.

Inhalt

Security News

TLS-Backdoor

In den vergangenen Wochen wurde mehrfach über die Möglichkeiten der NSA spekuliert, mitgeschnittene, TLS-geschützte Protokolle zu entschlüsseln. Dabei gerieten sowohl der RC4 (siehe SSN 9/2013) als auch die zumeist fehlende *Perfect Forward Secrecy* unter Verdacht. Inzwischen häufen sich die Hinweise, dass die NSA eine dritte Möglichkeit besitzt, die Dan Shumov und Nils Ferguson bereits im August 2007 auf der *Rump Session* der internationalen Kryptografenkonferenz Crypto'07 der IACR beschrieben hatten: Der vom NIST in erster Fassung im Mai 2007 publizierte Standard *Recommendation for Random Number Generation Usind Deterministic Random Bit Generators* (SP 800-90A) enthält einen auf Elliptischen Kurven basierenden Zufallszahlengenerator, der nach einem Blog-Eintrag von Bruce Schneier vom 15.11.2007 offenbar auf Drängen der NSA aufgenommen wurde: der Dual_EC_DRBG.

Im Appendix A des Standards werden drei Generatoren, bestehend aus einer elliptischen Kurve und jeweils zwei festen Kurvenpunkten *P* und *Q* spezifiziert. Der Trick: Ist die mathematische Relation (der diskrete Logarithmus *e*) zwischen diesen beiden Punkten bekannt, so lassen sich aus einem einzigen Output des Generators alle weiteren Zufallszahlen voraussagen. Nachträglich lässt sich *e* nicht berechnen – sollte aber die NSA die Punkte aus einem vorab gewählten *e* konstruiert haben, wäre *e* eine perfekte Backdoor. Das könnte erklären, warum der NIST-Standard empfiehlt, lediglich 16 Bits des Outputs nicht als Teil des Zufallswerts zu verwenden – üblich ist, maximal die Hälfte der Bits zu verwenden. Mit Kenntnis von *e* und einem Zufallswert kann man die fehlenden 16 Bit nämlich leicht durch *Brute Force* (65.536 Varianten) gewinnen. Zwar erlaubt der Standard, *P* und *Q* selbst gemäß ANSI X9.62 zu erzeugen. Für eine Zertifizierung nach FIPS 140-2 sind dann aber eigene Testvektoren erforderlich, die das Zertifikat verzögern – ein Aufwand, der zumindest bei den bisher zertifizierten Produkten gescheut wurde. So ist Dual_EC_DRBG auch in OpenSSL unverändert enthalten (wenn auch nicht als Default).

Ein TLS-Client schickt beim initialen *Handshake* eine Zufallszahl – und erzeugt wenig später das *Pre Master Secret*, aus dem der symmetrische Verschlüsselungs-Schlüssel (*Master Secret*) abgeleitet wird, mit demselben Zufallszahlengenerator. Nutzt der TLS-Client den Dual_EC_DRBG, könnte die NSA mit geringem Aufwand aus der ersten Zufallszahl den Schlüssel ableiten. Fatal: Diese Backdoor hebelt auch *Perfect Forward Secrecy* aus. Einziger wirksamer Schutz: Dual_EC_DRBG nicht verwenden.

Schranken der Einwilligung

Bereits am 17.07.2013 hat das Bundesverfassungsgericht in einem nun veröffentlichten Kammerentschluss zu der verbreiteten Versicherungspraxis, umfassende Schweigepflichtentbindungen gegenüber Ärzten, Kranken- und Rentenkassen von den Versicherten zu fordern, Stellung genommen.

Es obliege den Gerichten bei klarer Disparität der Vertragspartner und fehlendem besonderen gesetzlichen Schutz für die Bewahrung der informationellen Selbstbestimmung zu sorgen. Die Schweigepflichtentbindungen seien auf die tatsächlich erforderlichen Informationen zu begrenzen. Soweit dies im Voraus nicht möglich sei, sei ein entsprechendes schrittweises Verfahren zu verwenden. Dem Versicherten könne ein eigenständiges Modifizieren vorformulierter Erklärungen nicht zugemutet werden.

Die Entscheidung ist auf Einwilligungen zwischen ungleich starken Partnern im Allgemeinen übertragbar. Sie bestätigt einmal mehr das Erfordernis, Einwilligungen eng und bestimmt auf das Erforderliche zu begrenzen, will man nicht eine spätere Feststellung deren Nichtigkeit riskieren.

ULD vs. Facebook II

Am 09.10.2013 hob das Schleswig-Holsteinische Verwaltungsgericht mehrere Anordnungen des ULD auf, die von Betreibern von Facebook-Fanseiten deren Deaktivierung aufgrund mangelnden Datenschutzes verlangten (SSN 10/2012). Daraufhin teilte das ULD am 01.11.2013 mit, dass es Berufung gegen das Urteil eingelegt hat.

Gleich, ob einem bei Thilo Weicherts Kampf gegen Facebook eher die Parallele zu Don Quijotes Kampf gegen die Windmühlen oder die zu David gegen Goliat in den Sinn kommt – die Entscheidung des VG Schleswig ist in jedem Fall beachtlich. Denn nach – vermutlich unstreitiger – Auffassung des ULD verstößt Facebook gegen das Telemediengesetz: Durch die Statistik-API Facebook Insights werden Nutzer persönlich erfasst, was nach deutschem Recht einer ausdrücklichen Einwilligung bedarf. Facebook bietet hingegen nicht einmal eine Widerspruchsmöglichkeit.

Das Gericht vertritt die Auffassung, dass Betreiber von Fanseiten keinen Einfluss auf die Datenverarbeitung bei Facebook haben und deswegen für sie auch nicht (mit)verantwortlich sind. Das ist zwar einerseits nachvollziehbar, aber ein ‚Geschmäckle' bleibt: Muss man sich nur die ‚richtigen' Anbieter suchen, um aus der rechtlichen Verantwortung für

einen Internetauftritt zu kommen? Dank dem ULD wird diese Frage jetzt weitere Instanzen beschäftigen.

ForGe

Bereits im September 2013 wurde der *Forensic Test Image Generator* ForGe veröffentlicht. ForGe stellt einen komfortablen Baukasten unter GP-Lizenz bereit, mit dem für unterschiedliche Testfälle Images für NTFS-Dateisysteme automatisiert erzeugt werden können. Unterstützt werden derzeit die Implementierung von *Alternate Data Streams*, Änderungen von Datei-Endungen, Datei-Slack, Merging und Löschung von Dateien. Zusammen mit dem integrierten Zeitlinienmanagement auf Metadatenebene von NTFS kann man damit sehr gut wiederkehrende Prüfungen für Analysewerkzeuge spezifizieren. Zwar existiert mit Forensig^2 seit 2009 ein Forensik-Tool deutscher Herkunft mit ähnlicher Ausrichtung, das allerdings nie allgemein verfügbar war. ForGe beendet damit erstmals die Knappheit datenschutzrechtlich unbedenklicher Testdaten.

Entlastung für Provider

Das OLG Stuttgart hat am 22.10.2013 über die Kostentragung zu einer Abmahnung eines Betreibers einer Blog-Plattform entschieden. Ein Anspruch des Abmahnenden auf Kostenerstattung gegen den Betreiber wegen der urheberrechtswidrigen Fotoverwendung eines Seitennutzers wurde abgelehnt.

Nach Auffassung des Gerichts hafte der Hosting-Provider, der nach Erhalt der Abmahnung das fragliche Bild sofort entfernt habe, weder auf Schadensersatz, noch als Störer auf Unterlassung. Erst nach unterbliebener Handlung entstehe die Störereigenschaft. Aus demselben Grund könne von dem Host-Provider auch keine Unterlassungserklärung verlangt werden, da er nicht zur Untersuchung der Blogbeiträge verpflichtet sei.

Durch die Entscheidung wird die Rechtssicherheit für Provider von Internetdiensten gesteigert. Sie bedeutet aber auch, dass für ein sicheres Vermeiden von Ansprüchen ein schnelles Handeln ohne Klärung der Vorwurfsberechtigung erforderlich ist.

Secorvo News

T.I.S.P. Community Meeting

Zum siebten Mal fand am 04.-05.11.2013 in Berlin das T.I.S.P. Community Meeting statt. 100 T.I.S.P.-Absolventen waren angereist, um mit Kollegen aus allen Branchen aktuelle Fragestellungen der Informationssicherheit zu diskutieren und Erfahrungen auszutauschen. Schwerpunktthemen waren Security by Design, Risiko-Management und die Umstellung auf IPv6. Das nächste T.I.S.P. Community Meeting wird am 03.-04.11.2014 wieder in Berlin stattfinden. Wem zur Teilnahme (nur) noch das T.I.S.P.-Zertifikat fehlt, dem bietet Secorvo College am **24.-28.03.2014** die nächste Möglichkeit, es zu erwerben.

Weiterbildung 2014

Für die frühzeitige Planung Ihrer Weiterbildungsmaßnahmen 2014 empfehlen wir einen Blick in das Seminarangebot von Secorvo College. Soll es ein Update zu aktuellen Themen der Informationssicherheit sein? Oder umfassende Informationen zum Aufbau und dem Betrieb einer PKI? Oder aber eine Zertifizierung zur Dokumentation Ihrer Qualifikation, wie z. B. der T.I.S.P., der CPSSE oder der T.E.S.S.? Gerne sind wir für Sie da.

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

Anti-Prism-Party 2. Staffel

Mehr als 600 Besucher nahmen an der größten Verschlüsselungsparty Süddeutschlands unter dem Motto „Karlsruhe schützt sich selbst“ am 05.09.2013 im ZKM | Karlsruhe teil. Nach diesem großen Erfolg startet das neue KA-IT-Si-Jahr am 12.02.2014 mit der Anti-Prism-Party 2. Staffel, wieder im ZKM. Ab 18 Uhr werden unsere Experten in kompakten 10-minütigen Kurzvorträgen live vorführen, wie aktuelle und überwiegend kostenlose Schutzmechanismen für Smartphone, Browser und E-Mail-Client installiert, konfiguriert und genutzt werden. Auch für Besucher der 1. Staffel werden spannende neue Themen darunter sein.

Im Anschluss öffnet das Kryptologikum im ZKM seine Pforten. Neben Führungen durch die Ausstellung gibt es auch diesmal die Möglichkeit, sich an verschiedenen Stationen Schutzmechanismen von Karlsruher Sicherheitsexperten vorführen und erklären zu lassen. Aktuelle Informationen zur Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter (damit auch die NSA informiert ist).

Teamverstärkung

Erneut hat das Secorvo-Team Zuwachs bekommen: Seit dem 01.11.2013 unterstützt uns Dr. Yun Ding. Sie ist Diplom-Informatikerin mit über 16 Jahren Berufserfahrung; ein gutes Drittel dieser Zeit war sie verantwortlich für die Entwicklung von Schutzmechanismen wie z. B. kryptografischen Modulen, IT-Lösungen im Gesundheitswesen und Security-Architekturen für Smartphones.

Veranstaltungshinweise

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

Dezember 2013	
02.-03.12.	IsSec/ZertiFA 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
10.-11.12.	2. DFN Workshop Datenschutz (DFN-CERT Services GmbH, Hamburg)
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
17.-19.01.	ShmooCon 2014 (The Shmoo Group, Washington/US)
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)
Februar 2014	
04.-06.02.	Cloudzone 2014 (Karlsruher Messe- und Kongress-GmbH, Karlsruhe)
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
18.-19.02.	21. DFN Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)

Fundsache

Das BSI hat am 26.11.2013 eine Studie zur Sicherheit industrieller Steuerungssysteme (kurz: ICS) veröffentlicht. Sie umfasst eine wertvolle Gegenüberstellung relevanter Industrie- und Sicherheits-Standards und konkrete Vorschläge für die Durchführung von Sicherheitsaudits.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Michael Knopp, Christoph Schäfer, 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