secorvo
security consulting

Secorvo Security News

November 2017

Panoptikum

Jeremy Bentham (1748-1832), einer der großen Vordenker des Liberalismus und unseres heutigen Rechtsstaatsverständnisses, huldigte einem heute nur schwer nachzuvollziehenden Freiheitsbegriff: Er war überzeugt, dass nur ein mächtiger Staat mit strengen Sanktionen die allein auf ihren Vorteil bedachten Bürger an der rücksichtslosen Durchsetzung ihrer eigenen Interessen hindern könne. Und dass dieser Staat dafür einen umfassenden Überwachungsapparat benötige, damit aus der Erzwingung rechtskonformen Verhaltens echte Freiheit erwachse. Seine Vorstellungen kulminierten in dem Konstruktionsentwurf eines Gefängnisses, bestehend aus einem zentralen Bewachungsturm, um den die Zellen kreisförmig angeordnet und vom Turm aus durch Glaswände einsehbar sind.

Diese von ihm als Panoptikum bezeichnete Konstruktion erlaubte eine Überwachung ohne Wächter: Da der Turm von den Zellen aus nicht einsehbar war, mussten die Gefangenen ständig davon ausgehen, beobachtet zu werden. Mit dem Resultat, dass sie ihr Verhalten automatisch an die vermeintlichen Erwartungen der Überwacher anpassten. So beschreibt es auch Winston Smith in Orwells „1984“: *“You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”*

Benthams Gefängnisse konnten sich nicht durchsetzen. Dafür mutiert unsere Welt gerade zum Panoptikum: Hunderttausende Videokameras auf Straßen, in öffentlichen Gebäuden, Bussen und Bahnen, Kuscheltiere und Kinderuhren mit Mikrofon, HD-Kamera und SIM- oder SD-Karte, Spy-Tools für Smartphones und trackende Navigations-Apps – und natürlich die Kommunikationsfilter der Nachrichtendienste. Orwells Dystopie funktioniert offenbar auch gänzlich ohne „Großen Bruder“. Welchen Preis wir dafür bezahlen, werden wir vor lauter Gewöhnung womöglich nicht einmal bemerken.

Inhalt

secorvo
security consulting

Security News

Übermorgen ist morgen gestern

In den vergangenen Jahren haben sich die öffentlichen Trustcenter, die SSL-Serverzertifikate verkaufen, nicht gerade mit Ruhm bekleckert (u. a. SSN 03/2011, 09/2011 und 09/2017).

Da wäre es doch eine gute Idee, wenn der Browser reagieren könnte, falls ein HTTPS-Server plötzlich ein ganz anderes Zertifikat vorweist als erwartet, dachte man bei Google und entwarf 2011 bis 2015 den HPKP-Standard zum *Public Key Pinning*. Mit dieser HTTP-Header-Erweiterung kann ein Webserver dem Browser mitteilen, wie die Zertifikate aussehen werden, die er in den nächsten Monaten erwarten darf. Bei anderen Zertifikaten blockiert der Browser dann künftig den Zugriff auf die Seite.

Die Krux dabei ist, dass sich im schnelllebigen Internet „erwartet" und „unerwartet" nicht ganz so einfach unterscheiden lassen. Was ist, wenn bspw. der langjährige Zertifikatslieferant plötzlich vom Markt verschwindet? Ein weiteres schlagendes Argument der HPKP-Kritiker ist, dass sich dadurch ein neues Geschäftsfeld für Internet-Erpresser auftut: Wer den Besuchern eines kompromittierten Webservers manipulierte Public Key Pinning Header unterschiebt, könnte einen stolzen Preis für den passenden Private Key verlangen – selbst dann, wenn der Server HPKP eigentlich gar nicht nutzt.

Am 27.10.2017 verkündete Google nun, HPKP in Chrome zum Mai 2018 wieder abschaffen zu wollen – noch bevor Public Key Pinning eine breite Akzeptanz gefunden hat.

TeleTrusT Innovationspreis 2017

Auf dem mit rund 200 Teilnehmern sehr gut besuchten (und sehr empfehlenswerten) T.I.S.P. Community Meeting wurde am 14.11.2017 der TeleTrusT Innovationspreis 2017 an die PointBlank Security/Steen Harbach AG für eine smarte und einfallsreiche IoT-Lösung verliehen.

Man könnte meinen, der Begriff IoT-Security sei ein Widerspruch in sich, da es doch das Ziel der Hersteller (und oft auch der Nutzer) ist, Steuerungen für Alltagsgegenstände möglichst günstig zu realisieren und an das Internet anzubinden. Sicherheitsaspekte müssen dabei in der Regel zurückstehen – sie kosten Ressourcen und erfordern Know-how. Genau in diese Bresche springt die prämierte Lösung: Ein winziger Hardware-Chip ertüchtigt IoT-Geräte mit aktuellen Kryptofunktionen, der Authentisierung von Kommunikationspartnern und einer TLS-Absicherung der Kommunikationsverbindungen.

Der Chip wird in die Kommunikation eingeschleift und ermöglicht trotz der geringen Rechenleistung Kyptofunktionen auf Augenhöhe mit aktuellen PC-Systemen. Laut Herstellerangaben konnte z. B. der TLS-Handshake durch den sehr schlanken Code von ursprünglich mehreren Minuten auf 300 Millisekunden reduziert werden. Ein vielversprechender Ansatz, um einfache IoT-Geräte mit State-of-the-Art-Security-Mechanismen auszustatten. Security Made in Germany eben.

OWASP Top 10 – 2017

Seit inzwischen 13 Jahren veröffentlicht das OWASP regelmäßig die 10 wichtigsten Risiken bei Webanwendungen. Die am 20.11.2017 veröffentlichte finale Version der OWASP Top 10 2017 basiert zum ersten Mal auf Daten der Community. Erschreckend ist die große inhaltliche Übereinstimmung mit der ersten Version der OWASP TOP 10 aus dem Jahr 2004. Offensichtlich ist das Thema Sicherheit trotz vieler Bemühungen noch immer nur in Teilbereichen der Softwareentwicklung angekommen.

Sehr häufig werden die OWASP Top 10 als Standard missverstanden. Tatsächlich sind die Top 10 ein Awareness-Dokument. Für andere Zwecke bieten OWASP und auch andere Organisationen geeignetere Hilfestellungen, wie die Sicherheitsspickzettel für Entwickler, die Top 10 für Entwickler, den Application Security Verification Standard, den Testing Guide und vieles mehr.

Happy Birthday Privacy Shield

Das EU-U.S. Privacy Shield regelt seit 2016 den transatlantischen Datenverkehr personenbezogener Daten in die USA. Es ersetzte das vom Europäischen Gerichtshof für nichtig erklärte Safe-Harbor-Abkommen. Die Effizienz und Effektivität des Privacy Shield muss jährlich von der Europäischen Kommission überprüft werden. In dem am 18.10.2017 publizierten ersten Jahresbericht wurde dessen Wirksamkeit grundsätzlich bestätigt. Jedoch wurden konkrete Maßnahmen zur Verbesserung identifiziert, z. B. hinsichtlich der Kontrolle zertifizierter U.S.-Unternehmen oder der ausstehenden Ernennung eines Privacy-Shield-Ombudsmanns.

Die geforderte Umsetzung der Privacy-Shield-Vorgaben wird genau überwacht und teilweise kontrovers diskutiert. So wird beispielsweise moniert, dass EU-Datenschutzbeauftragte durch die Europäische Kommission ungenügend zur jährlichen Überprüfung einbezogen wurden, weshalb diese nun an einem eigenen Bericht arbeiten.

Inwieweit sich die Resultate mit denjenigen der Europäischen Kommission decken, bleibt abzuwarten. Falls die datenschutzrechtlichen Bedenken nicht ausgeräumt werden können, wird es zu einem wichtigen Indikator für die künftige Datenschutzausrichtung der Europäischen Kommission, wie diesem Umstand Rechnung getragen wird. Denn europäische Datenschutzbeauftragte zeigten und zeigen sich noch immer unzufrieden mit dem vom Privacy Shield vorgegebenen Datenschutzniveau.

Forensik inside

Seit dem 21.11.2017 liegen die Ergebnisse des diesjährigen Volatility Plugin Contest der Volatility Foundation vor, bei dem einige interessante und hilfreiche Erweiterungen prämiert wurden.

Besonders hervorzuheben ist darunter das Plugin SqliteFind, mit dem nun der Hauptspeicher nach jeglichen vorhandenen Table-Definitionen des „sqlite_master table" logisch und automatisiert durchsucht werden kann. In einem zweiten Schritt können dann spezifische Tables zeilenweise als Row ausgelesen werden.

Da SQLite inzwischen von sehr vielen Programmen genutzt wird und es immer seltener bei einer forensischen Analyse zu Beginn bekannt ist, wo ggf. wichtige Datenspuren vorhanden sind, schließt dieses Plugin einen wirklich blinden Fleck bei der forensischen Datenaufbereitung.

Secorvo News

Vom Rack zum RZ

In vielen Unternehmen ist die IT-Infrastruktur über die Jahre gewachsen – und manchmal sieht man ihr das auch an: Der Serverraum war eigentlich nie als Serverraum gedacht, und es sind eher die Erfordernisse des Tagesgeschäfts, die den Ausbau prägen, als eine systematische Planung. Der Sicherheit und Wartbarkeit der Infrastruktur kommt das selten zugute.

Wie aus dem gewachsenen Serverraum ein kleines Rechenzentrum werden kann, das heutigen Sicherheits- und Verfügbarkeitserwartungen genügt, zeigt Marco Müller (DC-Datacenter-Group GmbH) bei unserem kommenden KA-IT-Si-Event am **07.12.2017**, diesmal in den Räumen des Cyber-Forum. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „**Buffet-Networking**" (zur Anmeldung).

24 Verschlüsselungsrätsel

Am 01.12.2017 beginnt unser Adventsrätsel „Krypto im Advent" für Schülerinnen und Schüler der Klassen 3 bis 9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Kryptologie. Diesmal gilt es, die drei Spione innerhalb von 24 Tagen davon abzuhalten, die Weihnachtsfeier der Agenten zu entlarven...

Wer alle Aufgaben richtig beantwortet, kann einen der zahlreichen, von unseren Sponsoren beigesteuerten Preise gewinnen. Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

www.krypto-im-advent.de

Who watches the watchmen?

Merken Sie sich schon einmal die Abschlussveranstaltung der Traumfabrik-Filmreihe „BIG BROTHER: Surveillance Cinema" am **27.02.2018** (18-21 Uhr) im Karlsruher Filmtheater Schauburg vor – einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit dem Zentrum für Angewandte Kulturwissenschaft (ZAK) am KIT. Wir zeigen den Film „The Circle" (OmU) und diskutieren anschließend mit **Dr. Stefan Brink** (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), **Beate Bube** (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und **Thomas Rüttler** (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe) – eine Anmeldung ist nicht erforderlich.

Secorvo Seminare

Im kommenden Jahr bieten wir Ihnen wieder zahlreiche Gelegenheiten, Ihre Kenntnisse in der IT- und Informationssicherheit aufzufrischen, zu vertiefen und zu zertifizieren. Das nächste T.I.S.P.-Seminar findet **vom 16. bis 20.04.2018** statt – nach Ihrer Anmeldung erhalten Sie zur Vorbereitung ein Exemplar des T.I.S.P.-Begleitbuchs.

Veranstaltungshinweise

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

Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)
Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Mozilla wartet in diesem Jahr mit einem besonderen Weihnachtsgeschenk auf: Auf einer ansprechend gestalteten Webseite bewertet es die (US-amerikanischen) technischen „Must-Haves“ dieser Geschenkesaison nach einer einfachen Privacy-Taxonomie: Kann es mich ausspionieren? Was weiß es über mich? Und: Was kann passieren, wenn etwas schiefgeht?

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Sarah Niederer, 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