secorvo
security consulting

Secorvo Security News

November 2014

Über den Wolken

Die Berichterstattung über den NSA-Untersuchungsausschuss wird immer mehr zur Realsatire. Schon über die parteipolitischen Zänkereien um die Befragung von Edward Snowden konnte man nur noch den Kopf schütteln. Als der Ausschuss schließlich um ein informelles Treffen in Russland bat, erteilte Snowden dem Vorhaben über seinen Anwalt eine Absage.

Einer der Höhepunkte der Ausschussarbeit war die Befragung der Datenschutzbeauftragten des BND im Oktober. Frau „Dr. F." konnte ihren offenbar reichlich angestauten Frust darüber loswerden, dass die BND-Führung ihre datenschutzrechtlichen Einschätzungen zwar zur Kenntnis nahm, ansonsten aber weitgehend ignorierte. Da wurde selbst die Peinlichkeit eines US-Spions in den Reihen des BND zur Randnotiz.

Möglicherweise ist aber auch nur Reinhard Meys „Über den Wolken" das Lieblingslied von Gerhard Schindler: Nach seiner Überzeugung ist die Freiheit des BND zumindest dort definitiv grenzenlos – und die Verfassung scheint plötzlich nichtig und klein. Denn die BND-Führung vertritt die Meinung, dass bei der Überwachung von Kommunikation über Satelliten per se kein deutsches Recht gelten kann – schließlich befinden sich diese im Weltraum. Die Abhörstation in Bad Aibling sei dabei ohne Bedeutung.

Wie hanebüchen diese Auffassung ist, weiß neben dem gesunden Menschenverstand auch die juristische Fachwelt. Ganz abgesehen davon, dass das Bundesverfassungsgericht dies bereits 1999 ausdrücklich feststellte.

Grundlage für die BND-Arbeit ist das G-10-Gesetz – und dieses ist dringend reformbedürftig. Wir benötigen gesetzliche Regelungen und eine effektive parlamentarische Kontrolle, die die Arbeit der deutschen Geheimdienste aus dem Weltraum zurück auf den Boden demokratischer Tatsachen holen. Und eine Amtsführung, die die verfassungsrechtlichen Grenzen ihrer Tätigkeit respektiert.

Inhalt

Über den Wolken

Security News

Grafikkarten als UKW-Sender

Placebo-Zertifikate

Kampf der Grundrechte

Stuxnet

Blinder Fleck

Secorvo News

Weiterbildung 2015

Zum Nachlesen

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Grafikkarten als UKW-Sender

Wie bekommt man einen isolierten PC dazu, Daten an ein Smartphone zu übermitteln – auch wenn dieser nicht vernetzt ist? Mit dieser Fragestellung haben sich Forscher der israelischen Ben-Gurion Universität beschäftigt und ihre Erkenntnisse am 29.10.2014 auf der Malcon 2014 präsentiert.

Grundidee ihres kuriosen Seitenkanalangriffes ist es, die Grafikkarte derart zu beeinflussen, dass über das Monitorkabel als Antenne ein Signal im UKW-Frequenzbereich ausgesendet wird. Dieses wird vom Smartphone empfangen und von einer zu diesem Zweck entwickelten App „AirHopper" dekodiert.

Auch wenn die Datenrate sehr niedrig ist und die Übermittlung nur über recht kurze Distanzen funktioniert, könnte ein Trojaner auf diesem Weg ausgespähte Kennworte und Daten auf ein Smartphone weiterleiten. In Umgebungen mit sehr hohen Anforderungen an die Vertraulichkeit sollte man daher auf eine angemessene Abschirmung des Raumes achten – und keine Smartphones hineinlassen. Letzteres verbietet sich ohnehin wegen der in PCs und Smartphones verbauten Bluetooth-Chips.

Placebo-Zertifikate

Die US-amerikanische Federal Trade Commission (FTC) hat am 17.11.2014 die Einigung in einem Verfahren gegen TRUSTe, Inc., bekanntgegeben. Dem Anbieter von Gütesiegeln für Online-Dienste wurde vorgeworfen, seit dem kommerziellen Auftreten (ab 2008) bei seinen Kunden nicht für eine entsprechende Änderung der Siegel gesorgt zu haben.

Außerdem habe TRUSTe zwischen 2006 bis 2013 in etwa 1.000 Fällen entgegen der Angaben zu den Siegeln die jährlich erforderliche Rezertifizierung nicht durchgeführt. TRUSTe wurde zur Zahlung von 200.000 USD und zu genauer Rechenschaftslegung über seine Aktivitäten in Bezug auf den *Children's Online Privacy Protection Act* (COPPA) und die Zertifizierung der Einhaltung der *Safe Harbor*-Anforderungen verpflichtet. In diesem Zusammenhang hat die FTC betont, dass sie nicht zögern will, zum Schutz der Verbraucher einzuschreiten, wenn Marktteilnehmer bei Selbstverpflichtungen ihren Versprechungen nicht nachkommen.

Die damit öffentlich gewordenen TRUSTe-Verfehlungen zeigen deutlich, dass im Bereich der Online-Dienste Gütesiegel derzeit mehr schaden als nutzen. Hinter dem Vertrauen, das Nutzer und Geschäftspartner dem Siegel entgegenbringen, steht häufig wenig oder nicht nachvollziehbare Substanz. Dieses (blinde) Vertrauen hält Nutzer oder Anwender jedoch von eigenen Vorsichtsmaßnahmen und Kontrollen ab. Anstelle eines Sicherheitszuwachses führen derartige „halbseidene" Siegel eher zum Gegenteil.

Kampf der Grundrechte

Nachdem die Lehrerbewertungsportale bereits 2009 „dran" waren, hat der Bundesgerichtshof (BGH) sich nun mit einem Internetportal zur Ärztebewertung beschäftigt. In seiner am 06.11.2014 veröffentlichten Urteilsbegründung bewertet der BGH die Meinungs- und Informationsfreiheit der Portalnutzer und deren Interesse an einem Austausch über ärztliche Leistungen höher als das Recht auf informationelle Selbstbestimmung und die Berufsfreiheit des klagenden Arztes.

Dabei hat der BGH die Beeinträchtigung der Ärzte durch die Auffindbarkeit der Bewertungen mit Suchmaschinen, die Gefahr anonymer Wertungen ohne wahren Sachverhaltsbezug, die aufgezwungene Vergleichssituation mit anderen Ärzten und die Wettbewerbskonsequenzen als durchaus substantiell angesehen. Im Gegensatz zu dem in diesem Punkt ähnlichen EuGH-Urteil zu Suchmaschinen orientiert sich der BGH aber eher an der Dogmatik der Meinungs- und Informationsfreiheit. Danach ist das entscheidende Kriterium, dass die Bewertungen sich auf die Sozialsphäre des Arztes (das Arbeitsleben) beschränken.

Der Konflikt zwischen informationeller Selbstbestimmung und Informationsfreiheit in einem wenig vergessenden und jedermann zugänglichen Internet beginnt sich gerade erst zu entfalten. Für den Informationsaustausch in sozialen Netzwerken steht er im Grunde noch bevor; Suchmaschinen und Bewertungsportale sind da erst der Anfang. In den Argumentationen stoßen unterschiedliche Grundwerte aufeinander (Kontrolle des Einzelnen über die eigenen Daten gegenüber gesellschaftlichem Informationsinteresse). Für die Bedeutung und Grenzen des Datenschutzes ist dies eine wesentliche und wegweisende, aber keineswegs einfache Auseinandersetzung.

Stuxnet

Am 11.11.2014 veröffentlichte das Kaspersky Lab neue Erkenntnisse zum Verlauf der Stuxnet-Angriffe auf Irans Atomprogramm 2009 bis 2010. Einfallstor waren demnach nicht USB-Sticks (SSN 10/2010), sondern Dienstleister. Alle besaßen Expertise in der Automatisierungstechnik (SCADA) im iranischen Energiesektor. Alle wurden mehrfach infiziert oder konnten ihre Systeme nie von Stuxnet

reinigen. Das erste Opfersystem wurde wenige Stunden nach der Kompilation von Stuxnet am 22.06.2009 infiziert. Der zunächst vermutete Infektionsweg USB-Gerät erscheint damit unwahrscheinlich. Das System gehörte der Foolad Technic Engineering Co. Über die Behpajooh Co. Elec & Comp. wurde auch Irans größter Stahlproduzent Mobarakeh Steel Company angesteckt. Von dort breitete sich eine Infektionslawine bis in ferne russische Niederlassungen aus. Infiziert wurden auch die Neda Industrial Group, Teilnehmer der US-Sanktionsliste und die Control-Gostar Jahed Company. Der fünfte Dienstleister, Partner im Iranischen Atomprogramm, wurde von drei Systemen aus gleichzeitig angegriffen, was E-Mail als Infektionsweg unwahrscheinlich macht. Letztlich fand der Schadcode über die dauerinfizierten iranischen Dienstleister seinen Weg zum Ziel.

Was bleibt ist die Erkenntnis, dass Vertrauensbildung mit Dienstleistern nicht zum laxen Umgang bei der (IT-) Sicherheit verleiten sollte. Die strikte Kontrolle von Fernzugriffen und eingebrachten Daten sowie vertragliche Regelungen zur Mindestsicherheit mit Dienstleistern bleiben auch dann sinnvolle Maßnahmen, wenn man sich mit seinem Dienstleister gut versteht.

Blinder Fleck

Am 18.11.2014 veröffentlichte Mark Schloesser Erkenntnisse der Rapid7 Labs über Schwachstellen in digitalen Videorecordern der Firma Hikvision – gleich mit Metasploit-Exploit. Die betroffenen Geräte sind weltweit für die digitale Videoüberwachung im Einsatz – ein Scan fand über 150.000 im Internet erreichbare Geräte. Neben einem Trivialpasswort für den Admin-Zugang zeigt der Bericht drei aktuelle Firmware-Schwachstellen, die durch Pufferüberlauf (das „Cross-Site-Scripting“ der 80er Jahre des vergangenen Jahrhunderts) einem Angreifer die volle Kontrolle über das Gerät ermöglichen. Ähnliche Schwachstellen zeigen die IP-Kameras desselben Herstellers.

Für Angreifer sind dies Einfallstore ins Intranet eines Unternehmens. Fremdgenutzt wird bereits die Rechenpower der Geräte, um Bitcoins zu minen. Und Einbrecher könnten aus der Ferne Beweisfotos ihrer Taten verschwinden lassen. Seit September ist der Hersteller informiert; Patches sind bisher nicht verfügbar.

Überwachungstechnik mit Fernzugriff wird gern genutzt, um Routinearbeit auszulagern. Sobald aber IP-Technik mit dem Intranet verbunden wird, muss sie sicher administriert werden (Standardfehler: Default-Passwort). Sie muss patchfähig sein und sollte daher von einem Hersteller stammen, von dem bekannt ist, dass er Patches liefert. Diese Aspekte müssen Gegenstand der Beschaffungsentscheidung sein. Ein sicherer Internet-Fernzugriff erfordert weitere Maßnahmen wie einen VPN-Zugang oder eine Firewall.

Secorvo News

Weiterbildung 2015

Auch im kommenden Jahr werfen wir mit dem dreitägigen Seminar IT-Sicherheit heute einen vertiefenden Blick auf aktuellen Angriffe, neue Bedrohungen und mögliche Schutzmechanismen. Der erste Termin ist der 03.-05.03.2015.

Mit dem anerkannten Expertenzertifikat TeleTrusT Information Security Professional (T.I.S.P.) können Sie Ihre Erfahrungen und Kenntnisse in der IT-Sicherheit dokumentieren und sichtbar machen. Die nächste Schulung (mit anschließender Zertifikatsprüfung) findet vom 09. bis 13.03.2015 statt.

Sie suchen ein Seminar, das Ihnen das Thema PKI praxisnah und produktunabhängig vermittelt? Seit über 15 Jahren führen wir PKI-Projekte durch – und haben aus unseren Erfahrungen und Einsichten das Seminar PKI – Grundlagen, Vertiefung, Realisierung entwickelt, das inzwischen mehr als 350 Teilnehmer besucht haben (Termin: 21.-24.04.2015).

Sollen Sie in Zukunft Ihren Datenschutzbeauftragten in seinen Aufgaben unterstützen und ihm zuarbeiten? Die Schulung Geprüfter Datenschutzkoordinator im Unternehmen bereitet Sie auf zwei intensiven Seminartagen darauf vor (28.-29.04.2015). Nach bestandener Prüfung erhalten Sie ein Zertifikat vom TÜV Rheinland.

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

Zum Nachlesen

Im Dezemberheft der iX (12/2014, S. 64-71) erschien ein ausführlicher Beitrag der Secorvo-Experten André Domnick, Dr. Safuat Hamdy und Kai Jendrian zur systematischen Überprüfung der Sicherheit von Anwendungen.

Wer mehr von Secorvo lesen möchte, dem sei „das Buch“ empfohlen – „Zentrale Bausteine der Informationssicherheit“, erschienen Mitte 2014 in zweiter, aktualisierter und deutlich erweiterter Auflage, zugleich Begleitbuch des T.I.S.P.-Seminars. Je nach Präferenz als Hardcover oder E-Book (pdf) eine wunderbare, 720seitige Lektüre für den Lesesessel vor dem vorweihnachtlichen Kaminfeuer.

Veranstaltungshinweise

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

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)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Der am 21.10.2014 veröffentlichte Melani-Halbjahresbericht 2014/1 zur Informationssicherheitslage in der Schweiz und international stellt unterhaltsam und lesenswert aktuelle Informationen zu bekannt gewordenen Angriffen, Entwicklungen und Hintergründen vor.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer (Editorial)

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