secorvo
security consulting

Secorvo Security News

Juli 2016

Wir täuschen uns vielleicht

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“ (Volkszählungsurteil vom 15.12.1983). Wie wahr. Man stelle sich vor, ein Gesprächspartner kenne alle irgendwo über uns gespeicherten Daten: Die bargeldlosen Zahlungen mit Datum/Uhrzeit, die Bewegungsmuster, die das Navi übermittelt, die Schlüsselworte, nach denen wir gegoogelt und die Webseiten, die wir je besucht haben. Wir trösten uns damit, dass diese Daten ohne Weiteres nicht zugänglich sind. Und täuschen uns vielleicht.

Unseren Namen erfährt man über die Fahrzeughalterauskunft, die Adresse über das Einwohnermeldeamt und die Teilnahme an einer Sportveranstaltung über die Ergebnislisten im Internet. Wir trösten uns damit, dass selbst öffentlich zugängliche Daten in der Regel nur mit höherem Aufwand zu erfahren sind, den wohl kaum jemand auf sich nimmt. Und täuschen uns vielleicht.

Denn es gibt Menschen, die sich den Aufwand leisten – um zum Beispiel (Privat-)Insolvenzen über eine App in Google Maps sichtbar zu machen. Oder um zu zeigen, welcher Arzt unseres Vertrauens Zahlungen von Pharmaunternehmen erhält. Diese Apps ließen sich rechtskonform aufwerten, indem man die Vorstandstätigkeiten in Vereinen, die veröffentlichungspflichtigen Leitungsfunktionen in Unternehmen, die Jahresgehälter und Pensionsverpflichtungen von AG-Vorständen und Aufsichtsräten sowie die von ihnen verkauften Aktien ergänzte. Dazu die Einblendung eines aktuellen Fotos aus Facebook, die Angabe des Hochzeitstags aus der Bestellung des Aufgebots und Verweise auf die nächsten Verwandten z. B. aus einer Online-Traueranzeige. Wir trösten uns damit, dass der Gesetzgeber dem schon einen Riegel vorschieben wird. Und täuschen uns vielleicht.

Inhalt

secorvo
security consulting

Security News

Malware Virenschutz

Wie erneut ein aktueller Fall vom 28.06.2016 zeigt (siehe SSN 5/2014), verstecken sich auch in Virenschutzprodukten (diesmal: Symantec) Schwachstellen. Virenschutzsoftware muss man daher inzwischen auch als eine potentielle Gefährdung ansehen, zumal Angreifer über solche Schwachstellen privilegierte Rechte erhalten. Hinzu kommt, dass neue Schadprogramme erst mit mehreren Tagen Verzögerung erkannt und Heuristiken von geschickten Angreifern umgangen werden.

Werden Datenträger konsequent auf Viren geprüft und erfolgt die Datenübermittlung über zentrale Content Filter, sollte man daher darüber nachdenken, auf Fat-Clients und Servern ganz auf Virenschutz zu verzichten.

Wem die Virenfreiheit von Systemen zu bestimmten Zeitpunkten wichtig ist, sollte einen (schreibgeschützten und Firmware-signierten) „Virenschutz-Stick" z. B. mit dem vom heise-Verlag veröffentlichten Desinfec't verwenden, um damit stichprobenhafte Prüfungen durchzuführen.

Ganz klein gelandet

Am 17.06.2016 hat das zweite Gesetz zur Änderung des Telemediengesetzes den Bundesrat passiert. Die Änderungen nach fast 12-monatigem Gesetzgebungsverfahren und noch längerer Vordiskussion umfassen eine WLAN-Definition und § 8 Abs. 3, der klarstellt, dass Anbieter öffentlicher WLANs dem Haftungsprivileg für Access-Provider unterfallen. Ein geplanter Abs. 4, der auch Unterlassungsansprüche ausschließen sollte, wurde nicht aufgenommen.

Hotels und Anbieter von Gäste-WLANs oder Hotspots müssen nun keine Erklärungen ihrer Nutzer mehr einholen und auch keinen verschlüsselten Zugang anbieten. Abmahnungen wegen Rechtsverletzungen der Nutzer können den Anbieter jedoch weiter treffen, denn nach bisheriger Rechtsprechung sind diese vom Haftungsprivileg nicht umfasst. Dem steht nur die unverbindliche Gesetzesbegründung entgegen. Unsicherheit wird weiter die Frage schaffen, was ein zur Unterlassung verpflichteter Anbieter denn tun soll, um erneute Rechtsverstöße über sein WLAN zu verhindern.

PKI unter Zeitdruck

Erfolge erschaffen bekanntlich Neider - und finden oft Nachahmer. So veröffentlichte die israelische Firma StartCom Ltd. am 06.06.2016 ihr Produkt StartEncrypt, das viele Ähnlichkeiten mit dem sehr erfolgreichen Projekt LetsEncrypt aufweist. Kurz darauf wurden allerdings gravierende Sicherheitsprobleme aufgedeckt, sodass der Service am 04.07.2016 wieder eingestellt wurde – vorübergehend, wie es heißt, da man aus Zeitdruck nicht ausreichend getestet habe. Ein für ein Sicherheitsunternehmen besonders peinliches Eingeständnis.

Gut gemeint

Die Volksverschlüsselungs-Software, die die Fraunhofer Gesellschaft mit Unterstützung der Deutschen Telekom am 29.06.2016 in der aktuellen Version zum Download bereit gestellt hat, um Ende-zu-Ende E-Mail-Verschlüsselung auf Grundlage von S/MIME und PGP mit kostenlosen Zertifikaten für private Endanwender tauglich zu machen, ist gar keine Verschlüsselungslösung – sie kümmert sich allein um die Erzeugung und Einbindung des Public-Private-Schlüsselpaars.

Keine ganz neue Idee: Schon Anfang der 2000er Jahre hatte TC Trustcenter kostenlose S/MIME- und PGP-Zertifikate für Privatnutzer im Angebot.

Vor allem aber kombiniert sie die Nachteile offener und geschlossener PKIs: den aufwändigen Registrierungsprozess einer jedermann offenstehenden PKI mit der Beschränkung auf „mitspielende" Kommunikationspartner wie bei einer geschlossenen PKI.

Vielleicht sollte man lieber die vereinfachte Benutzerschnittstelle der Open-Source Volksverschlüsselungs-App mit einem Open-Source E-Mail-Client wie bspw. Thunderbird kombinieren – und auf die ebenfalls kostenlosen E-Mail-Zertifikate öffentlicher Trust Center wie Comodo oder StartCom zurückgreifen.

Stand der Technik

In Gesetzten und Verträgen wird von IT-Sicherheitsmaßnahmen häufig die Erfüllung eines „Stands der Technik" gefordert. Doch welche Maßnahmen genügen diesem Kriterium? Dieser Fragestellung hat sich der TeleTrusT-Arbeitskreis Stand der Technik angenommen. Am 26.05.2016 legte er eine "Handreichung zum Stand der Technik" im Sinne des IT-Sicherheitsgesetzes vor, die im Detail aufzeigt, welche Produkte und Technologien als etabliert betrachtet werden können.

Das mit viel Engagement erstellte Dokument bietet eine recht vollständige Aufstellung und erscheint nur in einzelnen Bereichen (wie den konkreten Anforderungen an sichere Softwareentwicklung oder die Sicherheit von Web-Applikationen) ergänzungswürdig, während das Thema „Datendiode" etwas überbewertet erscheint. Dennoch eine klare Leseempfehlung.

Datenschutz-Workaround

Die Europäische Kommission hat am 12.07.2016 ihre hoch umstrittene Angemessenheitsentscheidung (Art. 25 Abs. 6 Datenschutz-Richtlinie) zur Datenübermittlung in die USA auf Basis des sog. *EU-US Privacy Shield* erlassen. Diese Antwort auf die Safe-Harbor-Entscheidung des EuGH besteht aus mehreren Regelungsdokumenten, die die EU-Kommission mit verschiedenen US-Ministerien ausgehandelt hat, darunter Datenverarbeitungsprinzipien, Schiedsverfahren, Betroffenenrechte und ein erläuternder Anhang zur Datenschutz-Rechtslage in den USA. Zentraler Mechanismus ist weiter die freiwillige Selbstzertifizierung der US-Unternehmen, die personenbezogene Daten importieren; sie unterliegt staatlicher Aufsicht und Verstöße sollen sanktioniert werden.

Die Entscheidungsbegründung geht nur auf Basis der US-Darstellungen auf die Überwachungs- und Rechtsschutzpraxis ein; eine vom EuGH geforderte eigenständige Prüfung der objektiven Rechtslage ist kaum erkennbar. Auch der Privacy Shield dürfte daher vor dem EuGH landen und der Prüfung mit hoher Wahrscheinlichkeit nicht standhalten. Wer als Rechtsgrundlage seines Datenverkehrs in die USA gerade erst Verträge mit Standardvertragsklauseln abgeschlossen hat, sollte es erst einmal dabei belassen. Allerdings werden auch diese Gegenstand eines EuGH-Verfahrens.

Lawful Access

Wie ein Damokles-Schwert schwebte seit zwei Jahren ein Gerichtsverfahren vor einem New Yorker Bezirksgericht über den US-amerikanischen Cloud-Anbietern: Die US-Regierung hatte im Rahmen eines Drogenermittlungsverfahrens eine Verfügung gegen Microsoft erwirkt, um an Daten eines E-Mail-Accounts zu gelangen, die im Microsoft-Rechenzentrum in Irland gespeichert sind. Microsoft wehrte sich mit allen juristischen Mitteln. Unterstützung erfuhren sie dabei nicht nur von anderen IT-Giganten wie AT&T, Apple, Cisco und Verizon und Bürgerrechtsorganisationen wie der Electronic Frontier Foundation (EFF) als Amicus Curiae – auch die irische Regierung schaltete sich ein. Die umstrittene Verfügung wurde nun am 14.07.2016 durch ein Bundesberufungsgericht aufgehoben. Der Stored Communications Act (SCA) von 1986, auf den sie gestützt wurde, sei im Gegenteil dazu da, Daten vor dem Zugriff des Staates zu schützen, und dies gelte auch für ausländische Server eines US-Unternehmens.

Der Microsoft-Chefjurist Brad Smith äußerte sich frenetisch. Gewonnen ist jedoch lediglich ein Kampf in der großen Schlacht um die Datenhoheit. Eine große Hürde für amerikanische SaaS-Anbieter ist aus dem Weg geräumt – aber FBI & Co. werden zweifellos weiter nach kreativen juristischen Wegen für den Datenzugriff suchen.

Secorvo News

Spätsommerseminar

Unser rundum erneuertes Seminar „IT-Sicherheit heute“ (**27.–29.09.2016**) erfreut sich großer Nachfrage – damit sind interessante Diskussionen und ein lebhafter Erfahrungsaustausch schon garantiert. Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz oder der Datenschutz-Grundverordnung der EU bis zu einem „Hacking Day“ mit WebGoat-Workshop.

Schnell Entschlossene bekommen noch einen Platz (Programm und Online-Anmeldung).

Penetrationstests

Das Angebot von Penetrationstests erfordert eine ständige Weiterentwicklung, da sich Angriffsmethoden und Tools permanent verändern. Daher haben sich unsere Pentester der renommierten OSCP-Zertifizierung unterzogen, unseren Pentest-Werkzeugkasten weiter ausgebaut sowie typische Leistungspakete (wie die Untersuchung von Webanwendungen, der DMZ-Systeme oder des WLAN-Zugangs) geschnürt, die den Leistungsumfang transparenter machen.

Durch standardisierte Arbeitsabläufe und die Ergänzung von Einzelanalysen konnten wir die Aussagekraft unserer Berichte weiter verbessern – was den Mehrwert der Penetrationstests nochmal deutlich erhöht. Eine Übersicht unseres Pentest-Leistungsangebots finden Sie in unserem neuen Produktflyer.

Encryption as a Service (EaaS)

Wie real ist die Gefahr, sich mit einer Ransomware zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche Schutzmaßnahmen helfen dagegen?

Auf diese Fragen gibt auf dem nächsten KA-IT-Si-Event am **22.09.2016** der Vortrag von Tobias Häcker (Leitwerk AG) Antworten. Er wirft einen Blick hinter die Kulissen moderner Ransomware, beleuchtet deren Funktionsweise und stellt Abwehrmaßnahmen vor. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" – mit Blick über die Dächer von Karlsruhe. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

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

August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.-07.10.	Java Security (Secorvo, Karlsruhe)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, 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