secorvo
security consulting

Secorvo Security News

Februar 2019

Datenschützer auf der Erbse

Es war einmal ein Unternehmer, der wollte einen Datenschützer bestellen. Aber das sollte ein wirklicher Datenschützer sein. Da reiste er in der ganzen Welt herum, um einen solchen zu finden, aber überall fehlte etwas. Datenschützer gab es genug, aber ob es wirkliche Datenschützer waren, konnte er nie herausfinden. Immer war da etwas, was nicht ganz in Ordnung war. Da kam er wieder nach Hause und war ganz traurig.

Eines Tages brach plötzlich der Umsatz des Unternehmens ein, es war ganz entsetzlich. Da klopfte es am Haupteingang, und der Unternehmer ging hin, um aufzumachen. Es war ein Datenschützer, der draußen vor dem Tor stand. Wie hatte ihn der Konjunktureinbruch gebeutelt! Das Wasser lief ihm in die Schuhe hinein und zu Löchern wieder hinaus. Aber er sagte, dass er ein wirklicher Datenschützer sei. ‚Ja, das werden wir schon erfahren!' dachte der CIO, aber er sagte nichts, ging in das Rechenzentrum, löschte alle personenbezogenen Daten und versteckte in einem Verzeichnis eine Geburtstagsliste. Dann nahm er hundert beliebige Dateien, legte sie in demselben Verzeichnis ab und verschob das Verzeichnis in eines von hundert Unterverzeichnissen.

Den ganzen nächsten Tag ließ er den Datenschützer nach Datenschutzverstößen suchen. Am Abend fragte er ihn, wie er das Datenschutzniveau bewerte. „Oh, entsetzlich schlecht!" sagte der Datenschützer. „Ich habe etwas Grässliches entdeckt! Eine Geburtstagsliste ohne Einwilligung. Es ist ganz entsetzlich!" Daran konnte man sehen, dass er ein wirklicher Datenschützer war, da er in einem von hundert Verzeichnissen mit hundert Dateien die Geburtstagsliste entdeckt hatte. So feinfühlig konnte niemand sein außer einem echten Datenschützer. Da bestellte ihn der Unternehmer, denn nun wusste er, dass er einen wirklichen Datenschützer gefunden hatte. Und die Geburtstagsliste kam zur Warnung in einen Schaukasten, wo sie heute noch zu sehen ist, wenn sie niemand gestohlen hat.

Inhalt

secorvo
security consulting

Security News

Encryption – Back to the Roots

Schon bevor 1977 die öffentliche Standardisierung von Verschlüsselungsverfahren mit dem DES Fahrt aufnahm suchten neben den Geheimdiensten auch kommerzielle Unternehmen nach effizienten und zugleich sicheren Algorithmen. So basierte der DES auf der einige Jahre zuvor bei IBM von Horst Feistel entwickelten Chiffre Lucifer, und bei der Wahl des DES-Nachfolgers AES wurde ausdrücklich auch auf eine gute Performance auf einfachsten CPUs geachtet.

Dennoch wäre die Verschlüsselung des kompletten Speichers eines TV-Sticks oder Billig-Handys per AES auch heute noch recht langsam. Daher werden bspw. unter Android Geräte mit einer AES-Leistung unter 50 MB/s nicht verschlüsselt – trotz der seit Version 6 obligatorischen Data Storage Encryption.

Am 07.02.2019 präsentierten Google-Forscher nun unter dem Namen Adiantum einen Algorithmus, mit dem der Datenspeicher eines Geräts ohne AES-Beschleuniger-Hardware etwa fünf Mal schneller verschlüsselt werden kann als per AES. Dazu kombinierten sie die von Daniel Bernstein und anderen unabhängigen Forschern entwickelten Algorithmen ChaCha12, Poly1305 und NH mit AES – zu einem Feistel-Netzwerk. Damit gibt es immer weniger Argumente für Gerätehersteller, den Speicher nicht zu verschlüsseln.

TLS 1.3 auf dem iPhone

Die jüngste Version des TLS-Protokolls – TLS 1.3 – wurde im August 2018 standardisiert. Während die meisten Browserhersteller das neue Protokoll bereits in ihren Produkten nachgerüstet haben, sieht es bei den Betriebssystemplattformen hingegen dürftig aus.

Apple kündigte am 29.01.2019 als erster Mobilplattformbetreiber an, dass die kommende Version 12.2 des Mobilbetriebssystems iOS TLS 1.3 unterstützen wird. Apps, Browser und E-Mail-Clients können dann ohne weiteres Zutun Verbindungen mit dem neuen Protokoll aufbauen, sofern die Gegenstelle dieses ebenfalls anbietet. Von Google und Microsoft fehlt bisher die Ankündigung, wann mit einer Unterstützung von TLS 1.3 durch das Betriebssystem gerechnet werden kann.

Im Februar 2019 hatte TLS 1.3 auf den Servern der populärsten 150.000 Webseiten bereits eine Verbreitung von über 11,6% – beachtlich für ein Protokoll, das seit gerade einmal sechs Monaten standardisiert ist. Derweil mehren sich die Stimmen, ältere Protokollversionen abzuschalten. So wollen Mozilla, Google, Apple und Microsoft die Unterstützung für TLS 1.0 und TLS 1.1 in ihren Browsern ab März 2020 einstellen. Webseitenbetreiber sollten bis dahin sicherstellen, dass ihre Webserver mindestens TLS 1.2 beherrschen.

Grundschutz-Kompendium 2019

Am 18.02.2019 veröffentlichte das BSI eine überarbeitete Version des IT-Grundschutz-Kompendiums. Anders als die Ergänzungslieferungen zu den IT-Grundschutz-Katalogen wird die Version nun als „Edition" mit der jeweiligen Jahreszahl bezeichnet. Einige Bausteine wurden ergänzt und zum Teil Überarbeitungen der Inhalte der „Edition 2018" vorgenommen. Gut gefallen hat uns, dass auch geringfügige Änderungen explizit ausgewiesen sind, so dass man mit wenig Aufwand Änderungsbedarf an ggf. bereits durchgeführten IT-Grundschutz-Checks erkennen kann. Die klare Unterscheidung nach Bausteinen (= Soll-Anforderungen) und Umsetzungshinweisen (= Möglichkeiten zur Erfüllung der Anforderungen) wurde beibehalten. Auch mit der zweiten Ausgabe des Kompendiums ist damit aus unserer Sicht die 2017 begonnene Modernisierung des IT-Grundschutzes gelungen.

Datenkrake mit App-Zertifikaten

Zwar ist es unter Apples iOS, anders als in Googles offenem Android-Ökosystem, nicht ohne weiteres möglich, Apps aus anderen Quellen als dem offiziellen App Store zu installieren. Eine Ausnahme macht Apple jedoch: Unternehmen, die am Apple Developer Enterprise Program teilnehmen, können mit Hilfe eines speziell für sie ausgestellten Unternehmenszertifikats eigene In-House-Apps signieren und auf den iOS-Geräten ihrer Mitarbeiter installieren. Genau solch ein Unternehmenszertifikat hat Facebook nun missbraucht, um eine datenschutzrechtlich höchst bedenkliche Marktforschungs-App unter dem Titel „Facebook Research" am App Store vorbei an iOS-Nutzer zu verteilen. Damit nicht genug: Die App erfordert die Installation eines Root-Zertifikats im Trust Store des Geräts, so dass Facebook sogar verschlüsselte Kommunikation mitlesen konnte.

„Wir bessern uns" war wenige Tage vor Bekanntwerden dieses neuerlichen Skandals die Kernaussage des öffentlichen Auftritts von Facebook-Vizechefin Sheryl Sandberg Ende Januar in München. Schon kurz darauf musste jedoch Apple einschreiten und widerrief unverzüglich das Unternehmens-Zertifikat von Facebook. Damit waren nicht nur Facebooks „Research App" sondern auch sämtliche Facebook-internen Apps nicht mehr lauffähig. Inzwischen darf Facebook seine eigenen Apps

wieder signieren, die zukünftig hoffentlich innerhalb des Unternehmens bleiben und nicht erneut dazu genutzt werden, Nutzer im Namen der „Marktforschung“ auszuspionieren.

Kartellamt macht Datenschutzaufsicht

Das Bundeskartellamt schützt als unabhängige Bundesbehörde den Wettbewerb in Deutschland. In dieser Funktion hat es sich nun in die Verarbeitung von Nutzerdaten bei Facebook eingeschaltet, da Facebook eine marktbeherrschende Stellung unter sozialen Netzwerken in Deutschland innehabe. Es unterliege daher auch dem Verbot der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung nach § 19 Abs. 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), insbesondere, da der Umgang mit personenbezogenen Daten für die Stellung des Unternehmens im Wettbewerb maßgeblich ist.

Bislang war die Nutzung von Facebook nur möglich, wenn einer weitreichenden Sammlung von Daten auch außerhalb der Facebook-Seite mit Zuordnung zum Nutzeraccount zugestimmt wurde. Diese Drittquellen umfassen sowohl zum Facebook-Konzern zugehörige Gesellschaften (z. B. WhatsApp, Instagram) als auch bei der Nutzung von Apps und Drittwebseiten anfallende Daten, z. B. Facebook Business Tools wie der „Like“-Button.

Ein Zusammenführen dieser Daten ist nach der Entscheidung des Kartellamts nur zulässig, wenn der Nutzer darin (freiwillig) einwilligt – was außerdem bereits aus Art. 7 Abs. 4 DSGVO folgt.

Dieser Entscheid muss als Präzedenzfall für Online-Medien angesehen werden: Der Datenverarbeitung sind sowohl datenschutzrechtliche als auch kartellrechtliche Grenzen gesetzt.

Steinige Anpassung

Nach der Stellungnahme des Bundesrats vom 19.10.2018 hat der Bundestag das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (2. DSAnpUG EU) am 08./09.11.2018 an verschiedene Ausschüsse überwiesen. Eine endgültige Fassung gibt es daher weiterhin nicht. Der gegenwärtige Entwurf der Bundesregierung ändert in 155 Artikeln auf 553 Seiten 154 Gesetze. Dementsprechend unübersichtlich ist das Anpassungsvorhaben, zumal nun weitere Änderungsvorschläge der Ausschüsse zu berücksichtigen sind. Darunter auch – vom Bundesrat abgelehnte – Vorschläge zu einer Lockerung der Bestellpflicht von Datenschutzbeauftragten.

Angepasst werden Datenschutzregelungen in den Sozialgesetzbüchern und in Gesetzen über Dateien und Register, zahlreiche medizinrechtliche Bestimmungen, zahlreiche Gesetze des besonderen Verwaltungsrechts, das BSI-Gesetz und das Strafgesetzbuch. Vielfach werden dabei die Betroffenenrechte aus Art. 12-22 DSGVO nach Art. 23 DSGVO eingeschränkt. Nicht berücksichtigt werden bisher das Telekommunikations- und das Telemediengesetz, deren Status damit bis zur Verabschiedung der europäischen ePrivacy-Verordnung weiter unklar bleibt.

Eine öffentliche Diskussion zu den Vorschlägen blieb bislang weitgehend aus. Die zahlreichen Anpassungen werden die Rechtslage jedenfalls nicht einfacher machen, zumal die speziellen Einschränkungen der DSGVO-Pflichten Zweifel an der Reichweite der Öffnungsklauseln nach sich ziehen werden.

Secorvo News

Weiterer Black Belt

Unser Penetrationstester Michael Knöppler ist jetzt ebenfalls Träger eines „Black Belt“: Anfang Januar bestand er die OSCP-„Gürtelprüfung“ – eine weitere fachliche Verstärkung unseres Pentest-Teams.

Nächste Seminare

Wir freuen uns auf Ihre Teilnahme am kommenden PKI- (**18.–21.03.2019**) oder T.I.S.P.-Seminar (**25.–29.03.2019**) – die vollständigen Programme und eine Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Kaltblütig.

Zum Schutz von Daten vor unberechtigtem Zugriff ermöglichen Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen angeschalteten oder „schlafenden“ (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung zeigen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Veranstaltungshinweise

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

März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jannis Pinter, Christian Titze

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