secorvo
security consulting

# Secorvo Security News

**März 2016**

## Rettungsleck

Vor einigen Jahren nahmen wir an einer Wildwasser-Fahrt im Schlauchboot teil. Als mein Blick bei der Einweisung auf die Boote fiel, staunte ich nicht schlecht: im Boden klaffte jeweils ein großes Loch. „Damit das Wasser herauslaufen kann“, erläuterte uns der Bootsführer grinsend. Kaum im Wasser klärte sich das vermeintliche Wunder: Der Auftrieb der Luftkammern hielt das Boot so weit über der Wasseroberfläche, dass das hereinschwappende Wasser tatsächlich durch das Loch ablief – ohne Loch hätte das Boot tief und schwerfällig im Wasser gelegen.

An dieses Erlebnis musste ich am 09.03.2016 denken, als ein Verschlüsselungstrojaner unter Verwendung der Ransomware EDA2 die Runde machte. Dessen Autor Utku Sen hatte eine Entschlüsselungs-Hintertür in EDA2 eingebaut, die eine Rekonstruktion der Schlüssel ermöglichte – etwa 700 Betroffene kamen daher ohne Lösegeldzahlung wieder an ihre unerwünscht verschlüsselten Daten.

Das klingt nach einem guten Argument für das FBI, das derzeit von Apple den Einbau von Entschlüsselungs-Hintertüren in iPhones fordert. Aber wie beim Loch im Wildwasser-Schlauchboot gilt auch hier: Nicht jede Speziallösung eignet sich als generelles Konzept. Denn nachweislich ist ein Loch im Rumpf normalerweise kein wirksamer Sinkschutz.

Ein Verschlüsselungsverfahren ist nur dann ein sicheres Verfahren, wenn es keine Hintertür besitzt. Solche Verschlüsselungsverfahren sind bei einem Ransomware-Angriff zweifellos unerfreulich – sie sind jedoch nicht die Ursache des Problems. Auch die „Klick-nicht-auf-den-Anhang“-Empfehlung nimmt allein den Auslöser ins Visier. Der Schaden von Ransomware ist hingegen meist deshalb so groß, weil die betroffenen Benutzer Schreibrechte auf zu vielen Daten besitzen – und die zugehörigen Backups zu alt sind für eine verlustarme Wiederherstellung. Hier stecken die eigentlichen Hausaufgaben.

## Inhalt

secorvo
security consulting

# Security News

## DROWN-Angriff: ein SSL-Krimi

Der von einer Gruppe von Sicherheitsexperten am 01.03.2016 publizierte jüngste Angriff auf TLS/SSL (DROWN – *Decrypting RSA using Obsolete and Weakened eNcryption*) liest sich wie ein Krimi: Eine Gemengelage aus Crypto War-Relikten, Protokoll-Designfehlern, fehlerhafter Konfiguration und Bugs. Er basiert auf der verbreiteten, aber irrigen Annahme, dass es ungefährlich sei, wenn ein Server das „ausgestorbene" Protokoll SSLv2 nicht deaktiviert. Anfang März 2016 unterstützten allein sechs Millionen HTTPS-Server SSLv2. Anfällig für DROWN sind weitere Millionen Server, die andere SSL-basierte Protokolle nutzen oder mit einem SSLv2 unterstützenden Server das Zertifikat teilen.

DROWN nutzt die schwachen Export-Chiffren von SSLv2 aus den 90er Jahren mit nur 40 bit langen symmetrischen Schlüsseln (RC2 bzw. RC4) für einen *Chosen-Ciphertext*-Angriff, um den Sitzungsschlüssel einer mitgeschnittenen TLS-Verbindung zu berechnen und damit die Daten nachträglich zu entschlüsseln. Kryptographisch basiert DROWN auf dem *Padding Oracle*-Angriff von Daniel Bleichenbacher aus dem Jahr 1989.

Um einen HTTPS-Server vor DROWN zu schützen, reicht das Entfernen der Export-Chiffren in der Serverkonfiguration nicht aus: Es müssen SSLv2 serverseitig deaktiviert und aktuelle TLS/SSL-Bibliotheken (z. B. für OpenSSL) eingespielt werden.

Zum Testen der Verwundbarkeit eines HTTPS-Servers bietet die Webseite „The DROWN Attack" ein Check Tool und eine wunderbare FAQ.

## Quadratur des Kreises

Nach erfolgloser Abmahnung hat die Verbraucherzentrale Nordrhein-Westfalen am 29.02.2016 Microsoft vor dem LG München I (AZ. 12 O 909/16) auf Unterlassung verklagt. Grund ist die nach Auffassung der Verbraucherzentrale schwer verständliche und unklare Datenschutzerklärung zu Windows 10, auf deren Grundlage jeder Windows-Nutzer in zahlreiche Datenübertragungen einwilligen soll.

Die Datenschutzerklärung von Microsoft differenziert nach Diensten und verlinkt jeweils auf unterschiedliche Informationsquellen. Dabei ist für den Nutzer kaum zu erkennen, welche Datenkategorien zu welchen Zwecken unter welchen Umständen erhoben und verarbeitet werden. Andererseits handelt es sich bei Windows 10 um ein komplexes System von verschiedensten Diensten und Funktionen; sämtliche hierbei anfallenden Datenerhebungen in einer kurzen, hervorgehobenen Erklärung darzustellen und dabei alle einwilligungsrelevanten Informationen zu vermitteln dürfte der Quadratur des Kreises gleichkommen.

Auch wenn ein gesteigerter Sanktionsdruck bezüglich der Verarbeitungstransparenz wünschenswert ist, so ist in diesem konkreten Fall jedoch auch zu hoffen, dass er nicht zum Auftakt einer Abmahnwelle wird, die auf konfligierenden Gesetzesanforderungen fußt und auch bemühte Anbieter erfasst.

## Hackers Contest

Im Rahmen der von TippingPoint im Jahr 2005 gegründeten Zero Day Initiative, die Security-Forscher mit Preisgeldern für gefundene Schwachstellen belohnt, fand am 16. und 17.03.2016 der Pwn2Own-Contest 2016 in Vancouver statt. Dabei lobten HP und Trend Micro hohe Preise für diejenigen aus, denen es gelingen sollte, Systeme über die aktuellen Versionen von Google Chrome, Microsoft Edge, Adobe Flash oder Apple Safari mittels *Zero Day Exploits* zu übernehmen. Die Teilnehmer deckten insgesamt 21 kritische Sicherheitslücken auf – und reisten mit Prämien in Höhe von insgesamt 460.000 $ ab. Allein 145.000 $ strich der erfolgreichste Teilnehmer, der Südkoreaner Jung Hoon Lee ein: Ihm gelang die Übernahme von Google Chrome in weniger als zwei Minuten. Schon im vergangenen Jahr war er als Sieger aus dem Contest hervorgegangen und mit einer Gesamtprämie in Höhe von 225.000 $ zurückgekehrt.

Der Wettbewerb zeigt den Herstellern jährlich die Grenzen ihrer Softwareentwicklung auf – und macht eindrucksvoll deutlich, dass es, allen Anstrengungen zum Trotz, mit deren Qualität noch längst nicht zum Besten bestellt ist.

## No-Spy-Klausel

Am 16.03.2016 hat der IT-Planungsrat – das zentrale Gremium zur Koordination der Informationstechnik zwischen Bund und Ländern nach Art. 91c GG – in ihre Standard-Beschaffungsverträge die Zusicherung des Auftragnehmers aufgenommen, dass erworbene Hardware „frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Hardware, anderer Hardware und/oder Software oder von Daten gefährden". Eine entsprechende Formulierung hatte der IT-Planungsrat bereits am 16.07.2015 in die Vertragsbedingungen für die Beschaffung und Pflege von Standardsoftware aufgenommen.

Ein wichtiger Schritt um Softwarehersteller dazu zu bewegen, Sicherheitsaspekten eine höhere Priorität einzuräumen.

## Datenschutz via Kartellrecht

Am 02.03.2016 teilte das Bundeskartellamt mit, dass ein Verfahren gegen Facebook Inc., Facebook Ltd. und Facebook Germany GmbH wegen „Konditionenmissbrauchs" eingeleitet wurde: Es bestehe ein Anfangsverdacht, dass Facebook seine marktbeherrschende Stellung auf dem Gebiet der sozialen Netzwerke zur Durchsetzung rechtswidriger Datenschutzklauseln verwendet. Anlass ist die Einwilligung in die Datenverarbeitung bei der Nutzerregistrierung, die sich auf die als Fragenkatalog gestalteten Datenschutzrichtlinien bezieht. Darin wird nur sehr ungenau beschrieben, welche Daten in welchem Umfang verarbeitet und an Dritte weitergegeben werden.

Das Kartellamt kann nach eigener Auffassung selbständig datenschutzrechtliche Verstöße feststellen und Anordnungen zur Beseitigung oder Bußgelder von bis zu 10% des Jahresumsatzes verhängen.

Ob es tatsächlich zu einem Bußgeld kommt und dieses auch einen anschließenden Rechtsstreit übersteht, ist noch eine offene Frage. Im Erfolgsfall ist der Ansatz jedoch angesichts der Sanktionsmöglichkeiten des Kartellamtes (§ 32 ff GWB) ein starkes Druckmittel, Transparenz und die Einhaltung von Datenschutzgrenzen bei großen, internationalen Anbietern zu erzwingen. Voraussetzung dafür ist jedoch eine sorgfältige Marktdefinition, um deren marktbeherrschende Stellung bei bestimmten Angeboten nachzuweisen.

# Secorvo News

## CfP T.I.S.P. Community Meeting

In Frankfurt treffen sich vom **10. bis 11.11.2016** 150 IT-Sicherheitsexperten der deutschen Wirtschaft zum Erfahrungsaustausch beim 10. *T.I.S.P. Community Meeting*. Noch bis zum 18.04.2016 können Vortragsvorschläge eingereicht werden.

## PKI für Praktiker

Unsere PKI-Schulung vom **19. bis 22.04.2016** bündelt die Expertise und Erfahrung aus 19 Jahren aktiver Gestaltung von Public Key-Infrastrukturen. Hier die Einschätzung eines der über 300 Teilnehmer: „*Das PKI-Seminar bei Secorvo hat mir durch seine thematische Breite bei gleichzeitig gut durchdachter Struktur alle notwendigen Kenntnisse und Werkzeuge an die Hand gegeben, die mich in die Lage versetzen, auch künftigen PKI-Anforderungen unserer Organisation zu begegnen.*" Wir freuen uns, Sie auf dem Seminar zu begrüßen (Anmeldung).

## CPSSE-Zertifikat

Auf unserer Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe lernen Sie, wie Sie bereits bei der Code-Entwicklung Schwachstellen gezielt vermeiden. Dazu eine Teilnehmerstimme: „*Ich kann das Seminar nur weiterempfehlen. Hervorheben möchte ich neben der Kompetenz der Vortragenden die angenehme und inspirierende Atmosphäre und die dadurch ermöglichten Diskussionen, die wesentlich zum Verständnis der Problematik beitragen und motivieren, sich weiter mit dem Thema auseinanderzusetzen.*" Wir freuen uns auf Ihre Anmeldung.

## T.I.S.P.-Zertifikat

Vom **06. bis 10.06.2016** gibt Ihnen die Schulung zum T.I.S.P. einen umfassenden und themenübergreifenden Überblick über die aktuell wichtigsten Gebiete der Informationssicherheit. Mit der anschließenden Prüfung können Sie das anerkannte T.I.S.P.-Zertifikat erwerben und damit Ihr Expertenwissen dokumentieren.

## Anti-Prism-Party #4

Zum Abschluss der Ausstellung „Global Control and Censorship" des ZKM | Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) und dem CyberForum e.V. am **Freitag, 29.04.2016 ab 16 Uhr** zur 4. Staffel der Anti-Prism-Party (Eintritt frei).

Dort zeigen Experten, wie Sie sich vor Ausspähung im Internet schützen können. Es gibt Live-Vorführungen zu den Themen „Sicheres Surfen", „Sicher kommunizieren" und „Sichere Kommunikation im Karlsruher Public WLAN". Vertiefte IT-Kenntnisse sind nicht erforderlich, um den anschaulichen Vorführungen folgen zu können. Sie können sich von Experten individuell beraten lassen und die Erläuterungen im Workshop „E-Mail-Verschlüsselung" direkt am eigenen Laptop umsetzen. Derweil werden Ihre Kinder in der Spion-Schule von der Pädagogischen Hochschule Karlsruhe zu Verschlüsselungsexperten ausgebildet.

Um 18:30 Uhr schließt die Veranstaltung mit einem offenen Diskussionsforum unter Mitwirkung des Datenschutz-Aktivisten Malte Spitz. Nähere Informationen und das Programm zur 4. Staffel der Karlsruher Anti-Prism-Party finden Sie auf der Webseite www.anti-prism-party.de.

## Veranstaltungshinweise

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

| April 2016 | |
|---|---|
| 04.-07.04. | T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe) |
| 05.04. | Security Sells (CyberForum, Karlsruhe) |
| 11.-14.04. | CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe) |
| 19.-22.04. | PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe) |
| 21.04. | Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe) |
| 27.-28.04. | 17. Datenschutzkongress (EUROFORUM, Berlin) |
| 29.04. | Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe) |
| **Mai 2016** | |
| 30.05.-01.06. | IFIP SEC 2016 (IFIP, Hamburg) |
| **Juni 2016** | |
| 06.-10.06. | T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe) |
| 13.-14.06. | DuD 2016 (Computas, Berlin) |
| 22.06. | 8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe) |

## Fundsache

Das Nationale IT-Lagezentrum des BSI hat angesichts der zunehmenden Verbreitung von Ransomware am 11.03.2016 ein Dokument mit Empfehlungen zur Prävention und Reaktion herausgegeben. Inhaltlich wenig Überraschendes, aber eine gute Zusammenfassung.


## Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Michael Knopp.

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