secorvo
security consulting

# Secorvo Security News

**Januar 2018**

## Über Mittel und Zwecke

Er ist nicht nur einer meiner Lieblingsfilme, sondern er zählt zweifellos zu den Meisterwerken der Filmgeschichte: Hitchcocks „Das Fenster zum Hof“. Kürzlich konnte ich ihn das erste Mal im Kino bewundern – und war erneut fasziniert von den zahlreichen Parallelgeschichten, die er aus der Perspektive des Fotografen Jefferies (meisterhaft gespielt von James Stewart) erzählt. Der langweilt sich mit einem gebrochenen Bein in seinem New Yorker Apartment – und beobachtet die Nachbarn im Hinterhof durch sein Teleobjektiv. Dabei meint er, einem Mord auf die Spur gekommen zu sein und bittet seinen Freund Doyle von der Kriminalpolizei um Unterstützung. Nach dieser Szene sah ich den Film diesmal aus einer neuen Perspektive. Denn Doyle stellt seinem Freund zuliebe tatsächlich Ermittlungen an – allein auf der Grundlage vager Vermutungen. Erst als Jefferies ihn bittet, eine heimliche Wohnungsdurchsuchung vorzunehmen, erinnert sich Doyle an die rechtsstaatlichen Grenzen der Polizeiarbeit und verweigert seine Unterstützung – für Datenschützer eine Schlüsselszene. Wie vermutlich bei vielen Zuschauern stößt diese Haltung bei Jefferies auf Unverständnis: Schließlich ist für ihn die Sache klar, steht des von ihm Verdächtigten Schuld außer Frage.

Dabei geht es um eine große Errungenschaft des Rechtsstaats: die Unschuldsvermutung, die Beschränkung der Mittel der Strafverfolgung und eine Strafprozessordnung, die nicht der besseren Ahndung von Verbrechen dient, sondern nach Möglichkeit ausschließen soll, dass es zur Verurteilung von Unschuldigen kommt – und sei es um den Preis, einen Schuldigen davonkommen zu lassen. Diese Beschränkung in der Wahl der Mittel gilt es immer wieder aufs Neue zu verteidigen, damit sie nicht im Eifer der Verbrechensbekämpfung der Aufklärungsrate geopfert wird. Und da gibt eine kürzlich veröffentlichte Zahl zu denken: 310.000 stille SMS setzte der Verfassungsschutz 2017 zur Ortung von Mobilfunkteilnehmern ab. 44% mehr als 2016, 214% mehr als 2015. Sind wir da noch auf Kurs?

## Inhalt

secorvo
security consulting

# Security News

## Bürgerrating

Bereits Ende 2017 berichteten verschiedene Online-medien über Chinas Pläne für ein *Social Credit System*. Das bereits im Aufbau befindliche System für einen Score-Wert aller Bürger kann als Beweis für die Berechtigung der Kernaussagen des vor über 30 Jahren ergangenen Volkszählungsurteils des Bundesverfassungsgerichts dienen. Das wegweisende Urteil, das viele Kernelemente des Datenschutzrechts auf den Punkt gebracht hat, warnt davor, dass ein Bürger, der die Erfassung und Auswertung seines Verhaltens nicht einschätzen kann, in seiner persönlichen Freiheit eingeschränkt wird, und dies auch die Wahrnehmung seiner demokratischen Rechte beschränkt. Chinas Pläne, anhand des Verhaltens auf Shopping-Plattformen, Social-Media-Plattformen und der Nutzung von Finanzdienstleistungen, aber auch anhand des Verhaltens vernetzter Freunde, für jeden seiner Bürger einen Score-Wert zu bilden, stellen die Umsetzung der schlimmsten Befürchtungen der damals urteilenden Richter dar.

Aus europäischer Sicht sollte hieraus ein starkes Argument für die bestehenden Datenschutzprinzipien, für Datensparsamkeit und Transparenz erwachsen. Doch das System zeigt auch, was sich bei vielen Nutzern sozialer Medien bereits abzeichnet: Mit dem Angebot zu erlangender Privilegien, Boni oder vereinfachten Zugängen bei „geeignetem" Score-Wert ist offenbar die Versuchung groß, trotz der offensichtlichen Verhaltenssanktionierung sogar freiwillig an der Bestimmung des Score-Werts teilzunehmen. Vor allem Kritiker des Datenschutzes wären gut beraten, die sich nun entwickelnden Szenarien genau zu beobachten.

## HSMs jenseits der Donnerkuppel

„Zwei gehen rein, einer kommt raus" heißt es des Öfteren bei Firmenübernahmen wie derjenigen von Gemalto durch Thales, die am 17.12.2017 angekündigt wurde. Betroffen davon sind auch die beiden auf dem überschaubaren Markt für Hardware Security Module (HSMs) weit verbreiteten Produktreihen nShield/nCipher und Safenet/Luna, die ihrerseits durch vorherige Übernahmen im Portfolio der beiden Anbieter gelandet waren. Falls nicht noch die Kartellbehörden zur Auflage machen, eine der beiden Marken an einen Mitbewerber abzutreten, ist zu erwarten, dass Thales über kurz oder lang nur noch eine HSM-Produktreihe weiterführen wird.

Wer HSMs von Thales oder Gemalto z. B. für den Schutz von langlebigen CA-Schlüsseln einsetzt, sollte sich daher bald Gedanken über den langfristigen Support machen. Es wäre nicht das erste Mal, dass Sicherheitsforscher Nutzern helfen müssen, Schlüssel aus ihrem eigenen HSM zu hacken, um den Lieferanten (in diesem Fall: die Produktlinie) wechseln zu können.

## WPA ... zum Dritten

Am 08.01.2018 kündigte die Wi-Fi Alliance an, im Laufe dieses Jahres einen neuen WLAN-Sicherheitsstandard WPA3 zu etablieren, der WPA und WPA2 ablösen soll. WPA3 soll in mindestens den folgenden vier Punkten Verbesserungen bringen:

- Eine nicht-authentifizierte Mindestverschlüsselung für bislang völlig offene WLAN-Netze wie öffentliche Hotspots
- Ein Verfahren für die WLAN-Security-Konfiguration von IoT-Geräten ohne eigenes Display (wohl ähnlich WPS, aber hoffentlich sicherer)
- Die bekannte Anfälligkeit von WPA2 Personal gegen Offline-Attacken auf schwache WLAN-Passwörter in einmal mitgeschnittenen Handshakes
- Zum Suite-B-Nachfolger CNSA kompatible Kryptoverfahren für „National Security Systems" in den USA

Genaue technische Details sind noch nicht bekannt, aber es darf vermutet werden, dass die Wi-Fi Alliance dieses Mal nicht direkt auf den IEEE 802.11 Standard zurückgreift, sondern u. a. auf RFC 7664 und RFC 8110.

Es lohnt wohl, evtl. geplante Investitionen in eine neue WLAN-Infrastruktur noch etwas zurück zu stellen, bis WPA3-fähige Geräte verfügbar sind – oder zumindest jetzt schon auf entsprechende Upgrade-Fähigkeit zu achten. Die Vorgänger WPA und WPA2 verbreiteten sich jeweils relativ zügig, wenn auch vor dem Hintergrund der Angriffe auf das bereits konzeptionell missratene WEP.

## Komplexitätsklippen

Am 06.01.2018 veröffentlichten Paul Rösler, Christian Mainka und Jörg Schwenk von der Ruhr-Universität in Bochum eine vergleichende Untersuchung über die Sicherheit der Gruppen-Chats der verbreiteten Messenger-Dienste WhatsApp, Signal und Threema. Im Rahmen ihrer Analysen entdeckten die Autoren Schwachstellen in der Ende-zu-Ende-Verschlüsselung von Gruppen-Chats in WhatsApp und Signal, die einem Angreifer erlauben, unautorisiert beliebige Benutzer zu einer bestehenden Gruppe hinzuzufügen. Hierbei nutzen sie das Fehlen einer Authentisierung von *group management messages* aus. Diese Nachrichten werden an alle Gruppenmitglieder gesendet,

woraufhin diese einen Schlüsselaustausch mit dem neuen Mitglied durchführen.

Im Detail unterscheiden sich die Schwachstellen der beiden Messenger jedoch, sodass die Schwachstelle von WhatsApp als schwer wiegender einzustufen ist. Bei WhatsApp gibt es nur einzelne Administratoren, die berechtigt sind, neue Benutzer zu einer Gruppe hinzuzufügen. Hierfür laufen die Nachrichten über die zentralen Server von WhatsApp, um die Berechtigung der Benutzer zu prüfen. Eine Ende-zu-Ende-Verschlüsselung findet dabei nicht statt. Um die Schwachstelle auszunutzen, muss ein Angreifer einen WhatsApp-Server unter seiner Kontrolle haben und zusätzlich die komplexe ID des Chats kennen.

Beide Schwachstellen sind insgesamt diffizil und lassen sich in der Praxis wohl eher nicht ausnutzen, zumal die Nachricht, dass ein neuer Benutzer hinzugefügt wurde, weiterhin angezeigt wird. Dennoch zeigt die Analyse, wie komplex Ende-zu-Ende-Kommunikation in Gruppen sein kann. Gerade die Schnittstellen zwischen kryptografischen Protokollen und Management sind hierbei kritisch.

### Big brother is watching

Der am 15.01.2018 in der Frankfurter Allgemeine erschienene Beitrag zu WeChat sollte aus Datenschutzsicht zu Vorsicht mahnen. Hinter der Entwicklung des Kurznachrichtendienst WeChat, der mittlerweile sehr viel mehr kann als Nachrichten auszutauschen und z. B. das Buchen von Reisen und Tickets, das Begleichen von Rechnungen, Arztterminvereinbarungen oder Geldtransfers ermöglicht, steht die chinesische Firma Tencent. Mittlerweile wird die App (überwiegend in China) von knapp einer Milliarde Menschen genutzt.

Durch die geografische Angebotserweiterung soll nun der Vorstoß in neue Weltmärkte gelingen. Seit 2017 ist die App auch aus Deutschland offiziell im App Store downloadbar. Obwohl die Messaging App von TrustArc (ehemals TRUSTe) zertifiziert ist und ein „Höchstmaß an Kontrolle über die Privatsphäre“ verspricht, raten wir – zumindest aus Datenschutzsicht – dringend vor einer Installation ab. Es sei denn, man möchte, dass alle Daten an den chinesischen Staat geliefert werden und diesem zur Datenauswertung zur Verfügung stehen.

## Secorvo News

### Weiterbildung 2018

Die Secorvo-Seminare starten in diesem Jahr mit einem Vorbereitungsseminar für sichere Softwareentwicklung und der Zertifizierung als T.P.S.S.E. (**12.–15.03.2018**), gefolgt von IT-Sicherheit heute (**20.–22.03.2018**). Im April bieten wir Ihnen die nächste Gelegenheit, sich als T.I.S.P. zu zertifizieren (**16.–20.04.2018**).

Die aktuellen Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

### DSMSready2go

Eine der wichtigen Änderungen, die die europäische Datenschutz-Grundverordnung mit sich bringt, sind die erweiterten Dokumentationspflichten. Damit wird, davon sind wir überzeugt, der Datenschutz zukünftig den Aufbau von Managementsystemen erfordern, wie wir sie bereits aus der Informationssicherheit, insbesondere der ISO/IEC-Standard-Familie 2700x kennen.

Um diesen Prozess zu unterstützen hat Secorvo ein Datenschutz-Management-System auf der Grundlage eines Confluence CMS entwickelt, das Vorlagen, Prozesse, Richtlinien, Verfahrensverzeichnis und eine Methode zur Datenschutzfolgenabschätzung für die DSGVO-konforme Umsetzung des Datenschutzes in KMU bereitstellt – angelehnt an das erfolgreiche ISMSready2go. Nehmen Sie bei Interesse gerne Kontakt mit uns auf.

### Who watches the watchmen?

Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger“ zu machen. Doch was, wenn die Kontrolleure sich der Kontrolle entziehen – oder gar unkontrollierbar werden?

Zusammen mit dem ZAK (Zentrum für Angewandte Kulturwissenschaft und Studium Generale des KIT) lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg. Bei dieser Abschlussveranstaltung der Traumfabrik „BIG BROTHER – Surveillance Cinema“ wird der Film „THE CIRCLE“ von James Ponsoldt gezeigt. Die Einführung in den Film übernimmt Wolfgang Petroll, der bereits durch die gesamte Filmreihe führte. Im Anschluss an den Film findet eine Diskussion 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) statt. Anschließend können Sie den Abend im persönlichen Austausch beim „Buffet-Networking“ ausklingen lassen (zur Anmeldung).

## Veranstaltungshinweise

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

| | |
|---|---|
| **Februar 2018** | |
| 01.02. | Wie ich lernte, die Blockchain zu lieben (KA-IT-Si, Karlsruhe) |
| 21.-22.02. | 28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt) |
| 27.02. | Who watches the watchmen? (KA-IT-Si, Karlsruhe) |
| 27.-28.02. | 25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg) |
| **März 2018** | |
| 12.-15.03. | T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe) |
| 20.-22.03. | IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe) |
| 21.-23.03. | DFRWS EU Conference (DFRWS, Florenz/IT) |
| **April 2018** | |
| 10.-11.04. | Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden) |
| 16.-20.04. | T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe) |
| 23.-26.04. | PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe) |
| 24.-26.04. | 3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK) |
| 29.04.-03.05. | Eurocrypt 2018 (IACR, Tel Aviv/ISR) |


## Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Michael Knopp. Sarah Niederer.

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