secorvo
security consulting

# Secorvo Security News

**August 2013**

## Macht und Missbrauch

*Die Geschichte lehrt dauernd,*
*aber sie findet keine Schüler.*

*Ingeborg Bachmann (1926-1973)*

Wird Menschen Macht verliehen, so ist dies – sofern man jedem Menschen eine unverletzliche Würde zugesteht – immer zugleich mit der Übertragung großer Verantwortung verbunden. In der Praxis neigen Menschen mit Macht allerdings dazu, deren Wirkungsbereich auszudehnen – und missbrauchen sie nicht selten, wenn auch häufig mit vermeintlich besten Absichten.

Schon früh haben die Staatstheoretiker der Aufklärung erkannt, dass Machtmissbrauch institutionell verhindert werden muss. „Checks and Balances", wie Baron de Montesquieu (1689-1755) sie 1748 in seinem fundamentalen Werk „De L'esprit des Loix" (Vom Geist der Gesetze) forderte, wurden daher zur konstitutionellen Basis moderner Verfassungsstaaten: Gewaltenteilung, Verfassungsgerichte, Untersuchungsausschüsse oder mehrere am Gesetzgebungsprozess beteiligte Kammern (Bundesrat/Bundestag) sind Ausfluss dieses Prinzips.

Aber Machtmissbrauch findet auch im (vermeintlich) Kleinen statt, wenn Kontrollen versagen: Die Erniedrigungen in US-Gefängnissen im Irak entsprangen derselben Geisteshaltung wie die Überwachung der UN und von Ehepartnern durch NSA-Mitarbeiter mit Hilfe von Prism: dem Verlust des Respekts vor der Würde des Anderen und dem Irrglauben, dass verliehene Macht über geltende Regeln erhebt.

Fehlen Kontrollen vollständig und kann man nicht auf die Hilfe Dritter hoffen, bleibt Betroffenen häufig nur der Selbstschutz. Das gilt auch für ein Internet, das zunehmend zu einer – in neuem Sinn „gesetzlosen" – Überwachungsinfrastruktur degeneriert. Wer es bisher eher vertrauensselig nutze, sollte spätestens jetzt beginnen, sich aktiv um den Schutz seiner Daten und Metadaten zu kümmern.

Wie das geht, zeigen wir in diesen SSN – und am 05.09.2013 auf der größten Verschlüsselungsparty Süddeutschlands im Karlsruher ZKM.

## Inhalt

secorvo
security consulting

# Security News

## Kommunikationsdatenschutz

Wer seine Kommunikationsinhalte im Internet vor Dritten schützen will, sollte nach dem TNO-Prinzip ("*Trust No One*!") agieren. In der Praxis bedeutet das den Einsatz von Werkzeugen, die eine Ende-zu-Ende-Verschlüsselung unter Verwendung von als sicher geltenden kryptografischen Verfahren bieten. In der Praxis ist das jedoch oft nicht ganz einfach – vor allem Laien sind daher leicht überfordert.

Dennoch gibt es zahlreiche Lösungen. So stehen seit vielen Jahren mit GnuPG und S/MIME standardisierte, sogar kostenlose Schutzmechanismen für die Verschlüsselung von E-Mails zur Verfügung, die in vielen E-Mail-Clients standardmäßig integriert oder durch Plugins leicht ergänzt werden können. Eine Schritt-für-Schritt-Anleitung bietet zum Beispiel das Unabhängige Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein.

Sogar für Webmail-Lösungen gibt es Javascript basierte Werkzeuge zur Verschlüsselung mit GnuPG wie GPG Javascript Plugins, Mailvelope oder WebPG. Allerdings ist der Einsatz von Javascript Encryption nicht unumstritten – zumindest sollten dafür verbreitete und durch viele Experten getestete Bibliotheken wie bspw. die Stanford Javascript Crypto Library eingesetzt werden.

Aber auch für die inzwischen weit verbreiteten *Instant Messaging*-Dienste wie WhatsApp, Google Chat, iMessage oder Facebook Messaging (sowie weitere Jabber/XMPP basierte Dienste) gibt es Schutzmöglichkeiten. Zum einen lassen sich durch das Off-the-Record-Protokoll (OTR) XMPP-basierte Chats durch Plugins oder den Einsatz von Clients mit direkter OTR-Unterstützung absichern.

Eine sichere Alternative zu asynchronen Messaging Diensten auf iPhone oder Android-Handies bietet die Software Threema. Die App sorgt für eine Ende-zu-Ende-Verschlüsselung unter Verwendung der offenen Krypto-Bibliothek NaCl – ein gutes Beispiel, denn hier wurden kryptografische Verfahren nicht selbst implementiert (was in der Praxis meist dazu führt, dass der Hersteller über zahlreiche Fallstricke stolpert).

## Kommunikationskanalschutz

Zur Absicherung von Kommunikationskanälen im Internet hat sich SSL/TLS durchgesetzt. Web-Angebote sollten heute anbieterseitig bestmöglich mit SSL/TLS geschützt werden; umgekehrt sollte jeder Nutzer darauf achten, diese Protokolle (mit starken kryptografischen Verfahren) zu nutzen.

Für die Web-Browser Firefox und Chrome gibt es beispielsweise das nützliche Plugin HTTPS Everywhere, das automatisch für einen bestmöglichen Schutz durch SSL/TLS sorgt. Aber auch beim Zugriff des E-Mail-Clients auf das Postfach sollte die Nutzung von SSL/TLS selbstverständlich sein – dazu müssen im Client die entsprechenden Protokolle (IMAP4/TLS oder POP3/TLS, SMTP/TLS) und Ports (993 oder 995, 465) ausgewählt werden.

Bei der Nutzung von SSL/TLS sollte man zudem auf die Verwendung von „Perfect Forward Secrecy“ (PFS) achten. Dabei handeln Client und Server für jede Verbindung einen neuen symmetrischen Schlüssel aus, der von beiden Seiten nach Verbindungsende gelöscht wird und den ein Angreifer aufgrund des Verfahrens zur Aushandlung auch nicht später gewinnen kann. PFS erfordert die Verwendung einer Ciphersuite, die „Ephemeral Diffie-Hellman“ (TLS-DHE oder TLS-ECDHA) verwendet – spezifiziert bereits im Januar 1999 in TLS 1.0 (RFC 2246).

Als Achillesferse von SSL/TLS hat sich in den vergangenen Jahren der Umgang mit Zertifikaten erwiesen – nur wenn Nutzer sich auf deren Authentizität verlassen können ist der Aufbau vertrauenswürdiger verschlüsselter Kommunikationskanäle mit SSL/TLS möglich.

## Verbindungsdatenschutz

Der Schutz von bei der Nutzung von Webdiensten anfallenden Verbindungsdaten erfordert die Verwendung von Anonymisierungsdiensten wie Tor, I2P, JAP oder spezieller VPN-Lösungen. Dabei wird durch kryptografische Verfahren und hintereinander geschaltete Server verschleiert, welche Endsysteme eine Kommunikationsverbindung nutzen. Zum gleichzeitigen Schutz der Kommunikationsinhalten sollten Anonymisierungsdienste grundsätzlich zusammen mit Ende-zu-Ende-Verschlüsselungslösungen eingesetzt werden.

Zu beachten ist allerdings, dass Sender und Empfänger nur auf Netzwerkebene anonymisiert werden – gibt der Browser (über die Metadaten) oder der Benutzer selbst in der Anwendung seine Identität preis, ist der Dienst nutzlos.

## Metadatenschutz

Beim Surfen im Internet fallen – neben den Verbindungsdaten - viele weitere Metadaten, wie z. B. die besuchte Webseite, der verwendete Browser oder die Verweildauer an, auch bei der Nutzung von Anonymisierungsdiensten. Die Auswertung dieser Metadaten wird auch als *Tracking* bezeichnet. Wer sich ein Bild davon verschaffen möchte, welche Daten er mit einem einfachen Webseitenaufruf an wen übermittelt, sollte sich mal bei Panopticlick der *Electronic Frontier Foundation* (EFF) umsehen oder das Firefox-Plugin Collusion installieren.

Das Verwischen von Spuren beim Surfen ist heute eine echte Sisyphos-Arbeit. Eine gute Hilfestellung liefern dabei die Anregungen des „*Surveillance Self-Defense-Project*“ der EFF. Ein gewisses Maß an Kontrolle über die versendeten Metadaten behält man durch eine kontrollierte Verwaltung der Cookies, eine selektive Steuerung von Javascript und die eingeschränkte Übermittlung weiterer Daten mit Hilfe geeigneter Plugins wie z. B. NoScript, CookieManager oder RefControl.

### Clouddatenschutz

Der beste Schutz von Daten in der Cloud ist – die eigene Cloud. Diesem Credo folgt das Projekt mit dem sprechenden Namen ownCloud: Es ermöglicht die Installation einer eigenen Cloud zur Speicherung von Daten oder zur Synchronisation von Kalenderdaten.

Alternativ sollte man bei der Verwendung fremder Cloud-Dienste seine Daten grundsätzlich verschlüsseln. Die Verschlüsselung muss dazu auf dem Client stattfinden, und auch nur der Client sollte sich im Besitz der notwendigen Schlüssel befinden („*Trust No One*“). Ein Werkzeug, das einen solchen Ansatz realisiert, ist BoxCryptor, das plattformübergreifend für verbreitete Cloud-Anbieter zur Verfügung steht.

Statt dessen kann man auch verschlüsselte Datencontainer in der Cloud ablegen. Dieses Verfahren erlaubt zwar kein so komfortables Arbeiten, bietet aber ein hohes Schutzniveau. Das freie Programm TrueCrypt ermöglicht die Anlage und Nutzung solcher Datencontainer – nicht nur in der Cloud, sondern auch auf der eigenen Festplatte, dem USB-Stick oder als sicherer Backup-Container.

### Zugangsdatenschutz

Zu guter Letzt bleibt noch die Absicherung der Zugangsdaten – vulgo: Passworte – zu genutzten Web-Diensten. Angesichts der heute verfügbaren Werkzeuge und Rechenkapazität zum Knacken von Passwörtern sind vor allem zwei Dinge wichtig: Passwörter müssen eine hohe Qualität besitzen und sollten auf keinen Fall mehrfach verwendet werden. Die daraus erwachsenden Anforderungen an Passwörter und den Umgang damit können Menschen kaum noch leisten.

Abhilfe bieten „Passwort-Tresore“, die diese mit kryptografischen Mitteln absichern. Ein Beispiel hierfür ist die *Open Source*-Lösung KeePass, die auch plattformübergreifend verfügbar ist. Für Passwörter von Webdiensten empfiehlt sich die Nutzung von PwdHash zur Ableitung von Passwörtern in Abhängigkeit von der besuchten URL aus einem Master-Passwort – dieser Ansatz schützt zugleich vor Phishing.

## Secorvo News

### Karlsruhe schützt sich selbst

Ganz gleich ob elektronische Nachrichten, Internet-Recherchen oder Einträge in Sozialen Netzwerken: stehen die Server im Ausland, bedienen sich, wie wir nun wissen, nationale Geheimdienste nach Bedarf an den Datensammlungen.

Diesen Zugriffen muss man nicht tatenlos zusehen, denn viele der Daten müssten gar nicht erst anfallen. Schließlich gibt es Schutzmechanismen zuhauf – und viele davon sogar kostenlos. Häufig scheitert der Selbstschutz aber an unzureichenden Kenntnissen der Nutzer oder der (vermeintlichen) Komplexität der Hilfsprogramme.

Um diesem Mangel abzuhelfen lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL), dem CyberForum und dem ZKM | Zentrum für Kunst und Medientechnologie (ZKM) zur ersten Karlsruher "Anti-Prism-Party" am **05.09.2013** ab 18 Uhr ins ZKM ein (Eintritt frei).

Dort werden Karlsruher IT-Sicherheitsexperten vorführen, wie leicht man sich schützen kann – von der Verschlüsselung von E-Mails bis zum anonymen Surfen im Web ist für jeden etwas dabei. Für die musikalische Untermalung der größten Verschlüsselungsparty Süddeutschlands sorgen ab 20.00 Uhr die vom Karlsruher FEST bekannten Curbside Prophets.

### Wie ich lernte, Malware zu lieben

Die Verbreitung von Malware nimmt stetig zu und täglich kommen neue Arten von Viren, Würmern und Trojanern hinzu. Auch die Infektionswege ändern sich ständig – auch aufgrund des immer besseren Sicherheitsbewusstseins der Benutzer und der besseren Erkennungsraten und größeren Verbreitung von Antivirensoftware.

Dr. Matthias Schmidt (1&1 Internet AG) gibt mit seinem Vortrag „Dr. Seltsam, oder wie ich lernte, Malware zu lieben“ beim nächsten KA-IT-Si-Event am **19.09.2013** ab 18 Uhr im Panoramasaal der IHK Karlsruhe einen Einblick in die Arbeitsweise von moderner Malware. Anhand praktischer Beispiele werden neue Infektionswege aufgezeigt und mobile Malware beleuchtet, die sprunghaft an Zuwachs gewinnt.

Wir freuen uns auf Ihre Anmeldung!

## Veranstaltungshinweise

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

| September 2013 | |
|---|---|
| 02.-06.09. | SecSE 2013 (SINTEF, Regensburg) |
| 05.09. | Anti-Prism-Party, (KA-IT-Si, ZKM Karlsruhe) |
| 16.-20.09. | T.I.S.P.-Schulung (Secorvo College, Karlsruhe) |
| 17.-18.09. | D A CH Security (GI/OCG/BITKOM/TeleTrusT, Nürnberg) |
| 19.09. | Dr. Seltsam, oder wie ich lernte, Malware zu lieben (KA-IT-Si, IHK Karlsruhe) |
| 23.-26.09. | Security Engineering (Secorvo College, Karlsruhe) |
| **Oktober 2013** | |
| 01.10. | Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt) |
| 08.-10.10. | it-sa 2013 (NürnbergMesse GmbH, Nürnberg) |
| 14.-16.10. | 13. IDACON (WEKA-Akademie, Würzburg) |
| 14.-17.10. | CPSSE-Schulung (Secorvo College, Karlsruhe) |
| 21.-25.10. | T.I.S.P.-Schulung (Secorvo College, Karlsruhe) |
| 22.-23.10. | ISSE 2013 (TeleTrusT e.V./eema, Brüssel) |
| 25.-27.10. | FIfF Jahrestagung 2013 (FifF e.V., Siegen) |

## Fundsache

In einem seiner jüngsten Essays, publiziert am 23.08.2013 in Forbes, beschäftigt sich Bruce Schneier mit unserer Risikoaversion. Sein Fazit: Maßnahmen zum Schutz vor von Menschen ausgehenden Risiken verfehlen meist das Ziel – weil Menschen sich anpassen. Gelegentlich verursacht die Schutzmaßnahme selbst sogar höhere Schäden.


## Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian

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