secorvo
security consulting

Secorvo Security News

Januar 2017

Wie wirklich ist die Wirklichkeit?

Vor vierzig Jahren veröffentlichte Paul Watzlawick (1921-2007) sein wegweisendes Werk über die Relativität menschlicher Wahrnehmung. Darin belegt er überzeugend, dass unsere Weltsicht nie objektiv, sondern das Ergebnis von Kommunikation und (subjektiver) Interpretation ist. Neben kulturellen und sozialen Prägungen spielen dabei auch Phänomene wie sich selbst erfüllende Prophezeiungen eine Rolle. So wird unsere Wahrnehmung durch unsere eigene Weltsicht gefiltert: Konforme Erfahrungen werden als Beleg, widersprechende als die Regel bestätigende Ausnahme interpretiert.

Diese Einsicht müsste uns eigentlich skeptisch gegenüber unseren eigenen und tolerant gegenüber den Überzeugungen anderer stimmen. Stattdessen treibt uns eine unerschütterliche Wahrheitssehnsucht dazu, meist wenige Beispiele als Beweis für allgemeine Urteile zu akzeptieren: „Schau' Dir das einmal an. Da sieht man mal wieder, dass ...". Dabei dürfte nicht nur Mathematikern klar sein, dass man die Aussage „Jede Zahl ist eine Primzahl" nicht dadurch beweisen kann, dass man 3, 5, 7 und 11 als Beleg heranzieht.

In der von Blogs, Twitter und Facebook geprägten Meinungsöffentlichkeit finden wir heute unzählige solcher Belege für jedes unserer (Vor-)Urteile, die darüber zu Gewissheiten reifen. Darunter sind auch zahlreiche Falschbehauptungen („4 ist eine Primzahl"), die ebenfalls die eine oder andere Weltsicht zur Wahrheit veredeln. Keine guten Voraussetzungen für Selbstbescheidung und Toleranz.

Da passt es, dass Sprachlog.de am 31.01.2017 „Fake News" zum Anglizismus des Jahres 2016 gekürt hat. Würden wir wenigstens nur solche Behauptungen als „möglicherweise wahr" akzeptieren, deren Herkunft belegt ist, würden es „stille Post" und gezielte Falschmeldungen schwerer haben. Wäre das nicht mal eine wirklich großartige Aufgabe für digitale Signaturen?

Inhalt

secorvo
security consulting

Security News

Datenbank als Geisel

Im vergangenen Jahr machte Ransomware einen Großteil der Neuinfektionen mit Schadsoftware aus. Nach und nach erweiterten die Angreifer ihren Fokus und nahmen Unternehmen (vor allem deren Personalabteilungen) mit individualisierten E-Mails ins Visier. Jüngster Trend: Seit Anfang Januar sind über das Internet erreichbare mongoDB-Datenbanken von Verschlüsselungsangriffen betroffen. Eine neue Angriffswelle vom 12.01.2017 zielt dabei auf Installationen der Suchmaschine Elasticsearch. Die Angreifer verschlüsseln die Datenbankinhalte und fordern Lösegeld in Bitcoins. Nach Analysen des Sicherheitsforschers Niall Merrigan sind ihnen schon zehntausende Installationen zum Opfer gefallen.

Schutz vor den Angriffen bietet das Blockieren des Internet-Zugriffs auf die Datenbank. Außerdem sollten die Empfehlungen der Hersteller zur Zugriffskontrolle und sicheren Konfiguration umgesetzt werden. Und wie bei anderer Ransomware gilt auch hier: Regelmäßige Backups ermöglichen die Wiederherstellung der Daten, falls es doch zu einer Infektion kommen sollte.

Überfällige Regulierung

Die IT-Dienstleister von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten hadern schon lange mit der Strafbarkeit des (in der Praxis nicht auszuschließenden) Einblicks in die von ihnen verarbeiteten geheimen Daten. Nach Jahrzehnten der Rechtsunsicherheit hat sich nun die Bundesregierung mit einem Referentenentwurf vom 15.12.2016 der Überarbeitung des § 203 StGB angenommen.

Die Begründung des Entwurfs belegt (ohne es auszusprechen), dass sich die Mehrheit der Berufsgeheimnisträger seit Jahren durch die Inanspruchnahme von IT-Dienstleistungen strafbar macht. Die Gesetzesänderung sieht nun vor, dass der bisherige Gehilfenkreis um erforderliche Mitwirkende erweitert wird; dem Geheimnisträger fällt die Aufgabe zu, die Mitwirkenden sorgfältig auszuwählen, zu überwachen und zum Schweigen zu verpflichten.

Der insgesamt sehr zu begrüßende Entwurf benötigt sicher noch die eine oder andere Anpassung: So ist der Einsatz von Unterauftragnehmern nicht in § 203 StGB, wohl aber in der geplanten Rechtsanwaltsordnung erwähnt. Auch die Beauftragung einer juristischen Person scheint bezüglich der zu verpflichtenden Personen noch nicht zu Ende gedacht. Wenig überzeugend ist es auch, die korrespondierenden Zeugnisverweigerungsrechte erst in einem gesonderten Gesetz regeln zu wollen. Schließlich könnte das Kriterium der Erforderlichkeit erneut für Rechtsunsicherheit sorgen.

Volatility 2.6

Das Forensik-Framework Volatility ist nach 14 Monaten kontinuierlicher Weiterentwicklung seit dem 27.12.2016 nun als Release 2.6 verfügbar. Das bewährte Werkzeug für die Speicherforensik der Betriebssysteme Windows, Linux, Android und iOS hat viele neue und sinnvolle Funktionen für den Praktiker erhalten. Dazu zählen insbesondere die Unterstützung der aktuellen Versionen von Windows 10, Windows Server 2016 und KASLR Linux, deren neue Kernelstrukturen es schon längere Zeit deutlich erschwerten, spezifische Informationen aus dem Hauptspeicher zu analysieren.

Der standardisierte Funktionsumfang ist ebenfalls stark angewachsen. Inzwischen umfasst er 111 Windows-, 77 Mac- und 71 Linux-Plugins. Gerade für Mac und Linux sind viele Plugins mit den Schwerpunkten Prozesse und Dateien hinzugekommen, mit denen in der Analyse deutlich mehr Einsichten verfügbar sind als zuvor. Für Windows wurde in zahlreichen *dump-Plugins eine "--memory"-Option ergänzt, die es ermöglicht, auch die umliegenden Adressbereiche ausgeführter Prozesse automatisiert zu extrahieren. Das vereinfacht die Lokalisierung aktiven Schadcodes, der sich häufig außerhalb des eigentlichen Prozess-Adressraums befindet.

Die Standardausstattung an Plugins wird durch das Community-Repository fast verdoppelt, und dank ausgiebiger Tests konnte die Robustheit des Werkzeugs erneut gesteigert werden.

Der letzte Vorhang

Bereits am 21.12.2016 hat der EuGH ein neues Urteil zur Vorratsdatenspeicherung gefällt. Nachdem die Richtlinie zur Vorratsdatenspeicherung am 08.04.2014 für nichtig erklärt worden war, wurden jetzt auch die Schranken für nationale Regelungen geklärt. Die Entscheidung misst die allgemeine und unterschiedslose Vorratsdatenspeicherung von Telekommunikationsdaten an Art. 15 der ePrivacy-Richtlinie und an den Artikeln 7 (Achtung des Privatlebens), 8 (Schutz personenbezogener Daten) und 11 (Meinungsfreiheit) der Europäischen Grundrechtecharta. Im Ergebnis wiegen nach Überzeugung des Gerichtshofs die Grundrechte schwerer als Überwachungs- und Ermittlungsinteressen.

Eine Vorratsdatenspeicherung soll wegen des damit erzeugten Eindrucks einer ständigen Überwachung nur bei einem konkreten Bezug zwischen gespeicherten Daten und dem Überwachungsziel möglich sein. Eine allgemeine und unterschiedslose Vorrats-

datenspeicherung sei hingegen nicht zu rechtfertigen. Der Zugriff auf Vorratsdaten darf nur auf Grundlage eines gerichtlichen Beschlusses ermöglicht werden, die Speicherung ist auf das absolut Notwendige zu beschränken. Mit diesem Urteil wird auch die deutsche Neuauflage vom Dezember 2015 hinfällig, denn inhaltliche Beschränkungen der Vorratsdaten sind darin nicht vorgesehen.

Noch eine Verordnung

Die EU-Kommission hat am 10.01.2017 einen weiteren, die Datenschutz-Grundverordnung ergänzenden Verordnungsentwurf „Regulation on Privacy and Electronic Communication" veröffentlicht. Er soll u. a. die e-Privacy-Richtlinie (RL 2002/58/EG) ersetzen und Widerspruchsfreiheit mit der neuen Regelungslage herstellen und ist Teil der Digital Single Market Strategy.

Die Verordnung zielt auf elektronische Kommunikationsdienste, Verzeichnisdienste und auch auf Software-Provider, die elektronische Kommunikationsdienste bedienen, sowie auf das Direkt-Marketing mittels elektronischer Kommunikation und auf Dienstleister, die Daten von Endgeräten sammeln. Sie soll als spezielle Regulierung der Datenschutz-Grundverordnung vorgehen.

Darin wird die Verwendung von Verkehrs- und Nutzungsdaten (außerhalb von technischen und Abrechnungszwecken) weitgehend auf Einwilligungen gestützt. Enthalten sind weiter umfangreiche Informationspflichten, Regelungen für Verzeichnisdiensteanbieter sowie Einwilligungserfordernisse bei Verwendung personenbezogener Daten und Regelungen zum Direkt-Marketing, die den bisherigen § 7 UWG berühren. Die Sanktionen lehnen sich an die Datenschutz-Grundverordnung an.

Gelten soll die Verordnung ab dem 25.05.2018. Sie führt zu tiefgreifenden Änderungen des deutschen Telemedienrechts und enthält eine Reihe neuer Bestimmungen. Für einen sorgfältigen Gesetzgebungsprozess erscheint der Zeitplan ambitioniert.

Secorvo News

Enkeltrick für Fortgeschrittene

Seit einem guten Jahr gehören auch deutsche Unternehmen zu den Opfern der als „CFO Fraud" oder „Fake President Fraud" bekannt gewordenen Social-Engineering-Angriffe. Dabei erhalten gezielt ausgewählte Mitarbeiter mittelständischer oder großer Unternehmen E-Mails und Anrufe, die vermeintlich von der Unternehmensleitung stammen oder von ihr initiiert wurden. Unter der Vortäuschung streng vertraulicher Akquisitionen werden die Mitarbeiter dazu gebracht, große Zahlungen unter Umgehung interner Prozesse auszulösen.

Auf der Jahresauftaktveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) berichten Dr. Boris Hemkemeier und Ronny Wolf von der Commerzbank AG am **02.02.2017** über diese und andere aktuelle Cybercrimeangriffe gegen Unternehmen und zeigen, wie man sich dagegen schützen kann.

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

Ihr Weg zum Zertifikat

In Kürze fällt die „magische Marke" der 1.000 Informationssicherheitsexperten, die ihre Kenntnisse und Erfahrungen mit einem T.I.S.P.-Zertifikat gekrönt haben. Falls auch Sie diesem wachsenden Kreis von Experten angehören möchten, bieten wir Ihnen vom **06. bis 10.03.2017** die Gelegenheit, Ihre Kenntnisse und Erfahrungen zertifizieren zu lassen. Das einwöchige T.I.S.P.-Seminar und das von uns verfasste Begleitbuch bereiten Sie gründlich auf die Prüfung vor.

Auch Absolventen einer T.I.S.P.-Zertifizierung kommen im März auf ihre Kosten: Vom **14. bis 16.03.2017** bietet Ihnen das Seminar „IT-Sicherheit heute" die Gelegenheit, Ihre für die Rezertifizierung erforderliche fachliche Weiterbildung nachzuweisen.

Entwickler und Systemdesigner bereitet das Seminar T.P.S.S.E. (vormals CPSSE) vom **27. bis 30.03. 2017** systematisch auf die Prüfung als zertifizierter Professional für sicheres Software-Engineering vor. Hier erlernen Sie die konkrete Umsetzung von Security by Design in der Praxis. Weitere Seminarangebote und die Möglichkeit zur Anmeldung finden Sie unter www.secorvo.de/seminare.

Save the Date

Informationssicherheit und Datenschutz erfreuen sich seit Jahren wachsender Aufmerksamkeit. Inzwischen fordern Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen in den Mittelpunkt des Interesses.

Was aber bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich der? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Diesen Fragen widmet sich die diesjährige **Secorvention** am **30. und 31.05.2017**. Das Programm finden Sie in Kürze auf unseren Webseiten.

Veranstaltungshinweise

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

Februar 2017	
02.02.	Wenn der Vorstand zweimal klingelt ... (KA-IT-Si, Karlsruhe)
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
15.-16.02.	27. Smart Card Workshop (Fraunhofer SIT, Darmstadt)
März 2017	
06.-10.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Jochen Schlichting.

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