secorvo
security consulting

Secorvo Security News

November 2016

Reichtum

Zuerst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.
(Chinesische Weisheit)

Oft beginnt es mit ungenauen Begriffen. Wenn wir „Datenschutz" sagen, meinen wir „Schutz der Persönlichkeitsrechte". Gesprächspartner verstehen aber meist „Schutz der Daten" – und assoziieren unvermeidlich „IT-Sicherheit". Eine wichtige Ursache für das verbreitete Unverständnis, dem Datenschützer begegnen – geschuldet einer irreführenden Bezeichnung.

Schlimmer noch als ungenaue Begriffe sind falsche Metaphern. Das hat viel damit zu tun, dass unser Gehirn „in Bildern denkt": Assoziationen bilden wir nicht in Gestalt abstrakter Begriffe, sondern als visuelle Vorstellungen. Eine starke Veranschaulichung überlagert daher alle denkbaren Bedeutungsnuancen mit unseren damit verbundenen Emotionen und Vorurteilen. Daher sind Metaphern starke argumentative Waffen: Sie fokussieren, vereinfachen und können wahre Bedeutungen sogar überdecken oder verdrängen.

Manchmal jedoch schlägt eine solche argumentative Metapher unerwartet zurück. So sprechen wir seit Jahren von Daten als neuer „Währung", mit denen wir unentgeltliche Leistungen im Internet bezahlen. Der Friedenspreisträger des deutschen Buchhandels von 2014, Jaron Lanier, schlägt sogar vor, dass Nutzer für die Preisgabe ihrer Nutzungsdaten ein Entgelt erhalten. Gar keine schlechte Idee, Daten einen Wert beizumessen, oder? Zweifellos steigt damit ihre Schutzwürdigkeit – wollen wir nicht genau das?

Tatsächlich aber untergräbt die Währungs-Metapher den Wesensgehalt des Datenschutzes. Was macht man mit einer Währung? Man versucht, möglichst viel davon zu akkumulieren. Das Ergebnis ist Reichtum – das Gegenteil von (Daten-) Sparsamkeit (war das nicht die Tugend von Armen und Geizigen?). Kein Wunder, dass Verkehrsminister Dobrint nach „Datenreichtum" ruft – und Datenschützer zurückrudern. Hätten wir bloß diese Metapher verhindert.

Inhalt

secorvo
security consulting

Security News

Attacks are getting better...

... oder wie man mit einer Sonnenbrille zu George Clooney wird: Am 27.10.2016 haben Forscher der Carnegie Mellon University auf der 23rd ACM Conference on Computer and Communications Security vorgestellt, wie sich Gesichtserkennungssysteme in die Irre leiten lassen. In ihrem Vortrag zeigten sie anschaulich, wie sie von theoretischen Überlegungen zu Schwächen in Gesichtserkennungssystemen zu praktischen Angriffen kamen, die die Eignung solcher Systeme als Sicherheitsmaßnahme zweifelhaft erscheinen lassen: Es gelang ihnen – wenn auch unter Laborbedingungen – durch die Verwendung spezieller Brillen Gesichtserkennungssystemen vorzutäuschen, sie seien eine beliebige andere Person, die das System kennt. Mit dem Einsatz von Gesichtserkennungssystemen in Hochsicherheitsbereichen sollte man sich also noch zurückhalten.

AppSec Practice

Am 03.11.2016 veröffentlichte die Firma Veracode eine Studie mit dem Titel *How IT Professionals are approaching AppSec today*. Die Erkenntnisse der Umfrage unter über 300 Verantwortlichen für Softwaresicherheit sind womöglich nicht überraschend, aber dennoch erschreckend: Als Hauptgründe für unzureichende Sicherheit von Softwarelösungen wurden externer und interner Druck sowie die wachsende Komplexität angegeben. Häufig würden Schutzmaßnahmen verwendet, die erwiesenermaßen nicht optimal sind. Dass dies auch praktische Konsequenzen hat, zeigen beispielsweise die im *Verizon 2016 Data Breach Investigation Report* vom 19.05.2016 dokumentierten Fälle.

Leider beschränkt sich der Bericht auf die Problembeschreibung und zeigt keine konkreten Auswege auf. Wir empfehlen die Beachtung konstruktiver Hilfestellungen wie beispielsweise die des OWASP oder aktueller Publikationen wie des CSA-Whitepapers zur Absicherung von IoT-Devices.

Poison Pi

Je leistungsfähiger Microcontroller-Boards wie der Raspberry Pi werden, desto mehr eignen sie sich auch als preiswertes Angriffs-Tool. Der amerikanische Sicherheitsforscher Samy Kamkar veröffentlichte am 16.11.2016 ein auf einem 5 US$ teuren Raspberry Pi Zero implementiertes, Streichholzschachtel großes Angriffswerkzeug (PoisonTap), das sich (sogar gegenüber einem mit Passwort gesperrten PC) als lokales USB-Ethernet ausgibt und den gesamten Netzverkehr über den Raspberry Pi umleitet. Als „Man-in-the-Middle" kann es Login-Daten mitschneiden, Schadsoftware unterschieben, Daten abfließen lassen oder verfälschen – mehr als einen freien USB-Anschluss in einem laufenden PC mit offenem Browser benötigt es dafür nicht.

Neben einer regelmäßigen Überprüfung der USB-Anschlüsse am PC kann man Client-seitig wenig tun – ein gestarteter Browser genügt PoisonTap. Webserver-seitig hilft HTTPS *Strict Transport Security* (HSTS, RFC 6797), da es HTTPS-Verbindungen erzwingt, die PoisonTap nur unter Inkaufnahme einer TLS-Fehlermeldung aufbrechen kann.

Engineering Reversed

Der reinen Lehre zufolge sollten für neue Kryptoprotokolle zunächst die genauen Sicherheitsziele festgelegt, dann die Verfahren formal definiert und ihre Sicherheit analysiert werden, bevor man sie implementiert und unter das Volk bringt. Beim Kryptoprotokoll des Messengers Signal ist diese Reihenfolge gehörig durcheinander gekommen: Seine wesentlichen Elemente wurden bereits in den Messenger-Anwendungen von WhatsApp, Facebook & Co. genutzt, bevor eine unabhängige Forschergruppe aus England, Australien und Kanada in einer am 01.11.2016 veröffentlichten Analyse das Protokoll und seine Anforderungen formalisiert und basierend auf einer bereits vor 15 Jahren etablierten formalen Beweismethodik untersucht hat.

Für ihre Analyse mussten die Forscher sogar Details aus dem Open Source Quellcode rekonstruieren. Inzwischen wäre das nicht mehr notwendig, denn zwischen dem 20.10. und 20.11.2016 haben die Signal-Autoren schließlich selbst das Protokoll und die Sicherheitseigenschaften in drei Teilen dokumentiert. Die gute Nachricht für eine Milliarde Messenger-Nutzer: Das Protokoll wurde in der formalen Analyse für gut befunden. Auch, wenn das Vorgehen nicht empfohlen werden kann – ob das Protokoll nach Lehrbuch entworfen wurde, interessierte am Ende niemanden mehr.

Privacy Leaks

Greenpeace und der Spiegel veröffentlichten am 25.11.2016 verschiedene Verhandlungsdokumente des internationalen Abkommens über den freien Handel mit Dienstleistungen (*Trade in Services Agreement* – TiSA). Den vorliegenden Dokumenten nach wird dieses geheim verhandelte Abkommen europäisches Datenschutzrecht tangieren. So fordert das „Non-Paper on data flows", Beschränkungen für den Datenfluss auch personenbezogener Daten nicht zuzulassen, wenn dadurch Dienstleistungsanbieter ungerechtfertigt diskriminiert werden. Immerhin enthält der Entwurf eine Ausnahmeklausel für Maßnahmen zum Datenschutz

(Art. I-9 (c) (ii)), und der Annex zum E-Commerce sieht die Berücksichtigung nationalen Verbraucherschutzrechts vor. Allerdings darf kein Vertragsstaat als Bedingung für den Marktzugang die Nutzung von Rechenzentren im eigenen Territorium verlangen – das beißt sich mit geltendem Datenschutzrecht.

Zwar sind die Entwürfe noch deutlich von einer Endfassung entfernt, doch enthalten die Regelungsvorschläge zahlreiche Konfliktpunkte mit den gerade erst neu erlassenen europaweiten Datenschutzbestimmungen.

Orientierungssuche

Die Übermittlung personenbezogener Daten ins außereuropäische Ausland beschäftigt derzeit die Datenschutz-Aufsichtsbehörden: Die Behörden der Länder Bayern, Berlin, Bremen, Hamburg, Niedersachsen, NRW, Rheinland-Pfalz, Saarland und Sachsen-Anhalt haben am 03.11.2016 in Pressemitteilungen bekannt gegeben, 500 zufällig ausgewählte Unternehmen verbindlich zur Beantwortung eines diesbezüglichen Fragebogens auffordern zu wollen. Darin wird u. a. nach Übermittlungen in die USA und weitere Drittstaaten, nach der Rechtsgrundlage (u. a. auch Safe Harbor), nach der Überprüfung der tatsächlichen Privacy-Shield-Unterwerfung und nach typischen Auslagerungen oder Cloud-Diensten mit außereuropäischem Bezug gefragt. Zum weiteren Vorgehen machten die Aufsichtsbehörden hingegen keine Angaben.

Nun ist wenig gegen Versuche der Aufsichtsbehörden einzuwenden, einen Überblick über die Praxis der Datenübermittlung zu gewinnen. Dass den Unternehmen bei den Angaben zahlreich Gelegenheit gegeben wird, sich diverser Datenschutzverstöße selbst zu bezichtigen, hinterlässt jedoch einen schlechten Beigeschmack – während die Aufsichtsbehörden an anderer Stelle ihre Unsicherheit bei der Beurteilung der derzeitigen Rechtslage betonen.

Secorvo News

ISMS-Verstärkung

Angesichts der wachsenden Bedeutung, die Unternehmen inzwischen dem systematischen Umgang mit Informationssicherheit beimessen, haben wir uns um Verstärkung bemüht: Seit dem 01.11.2016 zählt Fabian Ebner zum Secorvo-Team. Er bringt neben praktischer Erfahrung einen Bachelor-Abschluss in Unternehmens- und IT-Sicherheit mit – und damit ein breites Grundlagenwissen über alle Gebiete der Informationssicherheit hinweg.

Ebenfalls im November hat Stefan Gora die Qualifikation eines ISO 27001:2013-Lead-Auditors erlangt – als vierter im Secorvo-Team.

IT-Sicherheit in der Produktion

Am **08.12.2016** führen wir in Kooperation mit der Innovationsallianz Karlsruhe unsere letzte KA-IT-Si-Veranstaltung in diesem Jahr zum Thema „IT-Sicherheit in der Produktion“ durch.

Als besonderes „Schmankerl“ starten wir diesmal mit einer Führung durch das IT-Sicherheitslabor des Fraunhofer IOSB. Im Anschluss zeigt das Fraunhofer ISI das wachsende Gefährdungspotential durch Industrie 4.0 und stellt Handlungsvorschläge zur Verbesserung der IT-Sicherheit vor. Das IOSB präsentiert das „Smart Factory Web“, eine Verbindung von Modellfabriken in Südkorea und Deutschland.

Schließlich gewährt die Firma HOMAG einen Einblick in das nationale Referenzprojekt zur IT-Sicherheit für „Industrie 4.0“. Im Anschluss an die Fachvorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.

24 Krypto-Rätsel

Am 1. Dezember beginnt unser diesjähriges Adventsrätsel „Krypto im Advent“ für Schülerinnen und Schüler der Klassen 3-9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Verschlüsselung und Geheimsprachen. Diesmal gilt es, drei Spione zu stoppen, die es auf die Weihnachtsgeschenke abgesehen haben... Wer alle Aufgaben richtig beantwortet, kann einen der zahlreichen, von unseren Sponsoren beigesteuerten Preise gewinnen.

Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

Dezember 2016	
08.12.	IT-Sicherheit in der Produktion (KA-IT-Si, Innovationsallianz, Karlsruhe)
16.12.	Sicherheit oder Datenschutz: Ein falscher Gegensatz? (GFT, ZKM, GI Karlsruhe)
Januar 2017	
13.-15.01.	ShmooCon 2017 (The Shmoo Group, Washington/US)
16.-18.01.	Omnisecure 2017 (in TIME berlin, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, Californien, US)
Februar 2017	
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
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)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Christoph Schäfer

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