secorvo
security consulting

Secorvo Security News

Juli 2019

Modell und Wirklichkeit

Seit Jahrhunderten erforschen Menschen die Welt. Sie erfanden die Gravitation, den Magnetismus und das Sonnensystem, um damit fallende Äpfel, ausgerichtete Kompassnadeln und kreisende Monde zu erklären und mathematisch zu beschreiben. Stieß dieses Wirklichkeitsmodell (z. B. durch den Nachweis der Konstanz der Lichtgeschwindigkeit) an Erklärbarkeitsgrenzen, wurde es flugs erweitert (Relativitätstheorie). Bis heute wissen wir jedoch nicht, ob es die Welt korrekt beschreibt. Die uneingeschränkte Geltung physikalischer Gesetze ist daher nur in diesem Wirklichkeitsmodell gesichert.

Ganz Ähnliches gilt für technische Lösungen. Sie lösen nie ein Wirklichkeitsproblem, sondern funktionieren nur in einem eingeschränkten Modell: So ist ein Auto nur unter bestimmten Voraussetzungen ein Fortbewegungsmittel – nicht unter Wasser, nicht in der Luft, nicht auf dem Mond (zumindest mit Verbrennungsmotor), und selten ohne Fahrweg oder bei Steigungen von über 30%. Leider vergessen wir das gelegentlich und wundern uns, wenn aus solchen Einschränkungen Risiken erwachsen. So zeigte eine israelische Forschergruppe am 23.06.2019, wie eine Drohne durch Vortäuschung von Verkehrszeichen ein Advanced Driver Assistance System (ADAS) beeinflussen kann. Und wenn das ADAS eines Tesla wie zuletzt am 01.03.2019 die Plane eines querenden LKW nicht als Hindernis erkennt, ist die Ursache höchstwahrscheinlich kein Programmierfehler, sondern eine Beschränkung des zu Grunde liegenden Wirklichkeitsmodells. Diese ergeben sich häufig implizit durch die Wahl einer technischen Komponente – so benötigt eine Bildauswertung Licht und Kontrast, ein Lasersensor nicht.

Dasselbe passiert mit Sicherheitslösungen, die oft versteckte Annahmen über das Angreiferverhalten enthalten. Skimming und Keyless-Go-Angriffe zeigen, dass diese nicht immer realistisch sind. Wir sollten daher von den Naturwissenschaften lernen und beginnen, die Wirklichkeitsmodelle unserer Lösungen präziser zu beschreiben.

Inhalt

secorvo
security consulting

Security News

Was man nicht aufgibt...

Die vor über 12 Jahren für Webserver eingeführten Extended Validation (EV) Zertifikate sollten Anwendern durch besonders gründlich geprüfte Zertifikatsanträge wieder Vertrauen in die durch Hacking-Vorfälle und Schludrigkeit in Verruf gekommene Web-PKI vermitteln. Dazu stellten Browser bei EV-Zertifikaten den geprüften Firmen- oder Organisationsnamen grün hinterlegt neben dem Vorhängeschloss in der Adresszeile dar („grüner Balken").

Doch schon seit iOS 12 (17.09.2018) heben Browser auf Apple-Mobilgeräten den Namen aus EV-Zertifikaten nicht mehr gesondert hervor. Auch Google Chrome wird ab Version 77, die am 10.09.2019 erscheint, die Hervorhebung komplett entfernen – seit Version 69 wird sie nur noch in grau statt grün dargestellt. EV-Zertifikate unterscheiden sich für den Endnutzer nicht mehr von DV- oder OV-Zertifikaten; der Mehrwert entfällt damit für Nutzer dieser Browser.

Diese Entwicklung entspricht der verbreiteten Einschätzung, dass EV-Zertifikate die in sie gesetzten Erwartungen nicht erfüllt haben und kein Plus an Sicherheit bieten. Google setzt stattdessen schon länger auf Certificate Transparency (SSN 6/2019). Auch durch die zunehmende Nutzung von Apps anstelle eines Browsers entfällt die Notwendigkeit der Darstellung von EV-Informationen. Statt EV-Zertifikate besonders zu kennzeichnen schlägt Mozilla mit Firefox Version 70 eine andere Richtung ein und brandmarkt unverschlüsselte HTTP-Webseiten als unsicher. HTTPS wird damit für Webseitenbetreiber endgültig zur Pflicht; die Mehrkosten für EV-Zertifikate kann man sich jedoch sparen.

Angst beflügelt den eilenden Fuß

Am 18.07.2019 schlug eine Schwachstellenmeldung Wellen: Fach- und Allgemeinpresse berichteten über eine kritische Sicherheitslücke im VLC Media Player, die einem Angreifer das entfernte Ausführen von Code ermöglichen würde. Untermauert wurde die Kritikalität durch einen CVSSv3 Score von 9.8. Losgetreten hatte sie CERT-Bund, die im BSI angesiedelte zentrale Anlaufstelle für Computersicherheitsvorfälle, nachdem MITRE den Schwachstellen-Identifier CVE-2019-13615 zugewiesen hatte. Wie sich herausstellte, handelte es sich gar nicht um eine Schwachstelle in VLC, sondern um eine in der von VLC verwendeten Bibliothek „libEBML", die bereits am 20.04.2018 mit Version 1.3.6 behoben worden war. VLC wird schon seit dem 29.05.2018 (Version 3.0.3) mit einer korrigierten „libEBML" ausgeliefert. Der Entdecker der Schwachstelle hatte eine Ubuntu-Version verwendet, die keine aktuelle Version der Bibliothek bereitstellte (deren Maintainer das Problem schnell behoben).

Ein Sicherheitsforscher, der eine nicht aktuelle Software analysiert, zwei offizielle Institutionen (MITRE und CERT-Bund), die ohne gründliche Prüfung eine kritische Schwachstelle anerkennen, Medien, die ohne tiefere Recherche voneinander abschreiben und die Community einer Linux-Distribution, die Sicherheitsaktualisierungen nicht zeitnah verfügbar gemacht hat – ein gefährlicher Cocktail, der Unternehmen vermeidbare Aufwände beschert hat.

Selbst die Änderung der Kritikalität der Schwachstelle ist nur schwer nachvollziehbar: Allein das NIST pflegt in der NVD eine umfängliche Änderungshistorie. CERT-Bund beschreibt die Änderungen vollkommen unzureichend und MITRE führt erst gar keine Historie. Und die Moral: Trau' keiner Nachricht, die Du nicht selbst überprüft hast...

Die Geister, die ich rief...

Das deutsche Vorratsspeicherungsgesetz ist nach den Urteilen des EuGH und der deutschen Obergerichte derzeit ausgesetzt und wird es auch noch auf absehbare Zeit bleiben. Allerdings hat sich der Europarat am 27.05.2019 für eine Vorratsdatenspeicherung zum Zwecke der Kriminalitätsbekämpfung ausgesprochen. Offenbar speichern Internet- und Telefonanbieter jedoch trotz der einschlägigen Rechtsprechung über Monate hinweg nicht abrechnungsrelevante Daten ihrer Kunden.

Um den Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 Grundgesetz zu gewährleisten, muss diese Art von Vorratsdatenspeicherung unterbunden werden. Wie wichtig das ist, zeigt ein aktueller Vorfall aus Dänemark: Das dänische Justizministerium gab am 02.07.2019 bekannt, dass ein IT-Fehler bei der Vorratsdatenspeicherung möglicherweise dazu geführt hat, dass Unschuldige verurteilt und Täter fälschlich freigesprochen wurden. Insgesamt müssen 10.700 Fälle von der inzwischen eingesetzten Expertenkommission überprüft werden.

Freiheit und Gerechtigkeit können auch unter die Räder einer gefährlichen Mixtur aus unkritischem Glauben von Strafverfolgern an die Verlässlichkeit technischer Nachweise und vorauseilendem Gehorsam bei Telekommunikationsanbietern hinsichtlich der, rechtsstaatliche Grenzen überdehnenden, Speicherung von Verbindungsdaten geraten.

Was lange währt...

Nach über sechsmonatiger Beta-Phase wurde am 28.06.2019 Version 2.1 der Burp Suite veröffentlicht. Als Proxy zwischen Web-Browser und -Server erlaubt sie das Mitschneiden, Analysieren und Mani-

pulieren von HTTP-Verkehr – ein unverzichtbares Werkzeug für Sicherheitsexperten und Web-Entwickler. Die lang erwartete Runderneuerung enthält sowohl in der (kostenfreien) Community- als auch in der Professional-Edition zahlreiche Verbesserungen: Der neue Crawler und die neue Scanning-Engine vereinfachen zusammen mit der dynamischen JavaScript-Analyse insbesondere automatisierte Tests. Auch das User Interface wurde an einigen Stellen stark überarbeitet – so wurden ein neues Dashboard und ein alternatives dunkles Farbschema integriert. HTTP-Antworten werden nun dank einer neuen Rendering-Ansicht unter Berücksichtigung von Stylesheets dargestellt. Die Burp Suite kann jetzt auch über eine REST-API aus anderen Anwendungen angesprochen werden, um beispielsweise Scans zu initiieren. Schließlich wurde auch die Performance verbessert.

Stets ist die Sprache kecker als die Tat

Datenschutzaufsichtsbehörden, Datenschutzkonferenz, Europäischer Datenschutzausschuss und Datenschutzverbände überschütten Unternehmen, Datenschutzbeauftragte und Verantwortliche derzeit mit Hinweisen, Orientierungshilfen und Stellungnahmen. Dabei hapert es aber gelegentlich an der inhaltlichen Konsistenz. Zwei aktuelle Beispiele:

Die Argumentation der Stellungnahme des HDBI vom 09.07.2019 zur Unzulässigkeit des Einsatzes von Office 365 in Schulen lässt sich durchaus auf Arbeitgeber übertragen. Als Lösung wird auf on-premise Angebote verwiesen. Zwar haben Rechtsbedenken gegen Office 365 durch das Ende der Deutschland-Cloud (SSN 3/2019) und eine niederländische Prüfung vom 07.11.2018 (SSN 4/2019), die erhebliche Datenschutzrisiken benennt (Zugriff auf personenbezogene Daten auf Grundlage des US Cloud Acts und ungeklärte Verwendung von Telemetrie-Daten durch Microsoft), neue Nahrung erhalten. Eine grundsätzliche Rechtswidrigkeit wurde bisher jedoch nicht festgestellt – und erscheint auch vor dem Hintergrund der geltenden EU-US Privacy Shield Vereinbarung juristisch fragwürdig.

Die neuen FAQ der bayerischen Landesdatenschutzaufsicht enthalten einen informationellen Rundumschlag – und verblüffen mit der Aussage, dass einerseits Google Maps, Google Fonts und allgemeine Captchas, sofern in der Datenschutzerklärung darüber informiert wird, in Webseiten eingebunden werden dürfen, andererseits aber ein rechtmäßiger Einsatz von Google Recaptcha eine Darlegung der Nutzerdatenverarbeitung durch Google erfordert. Die Zulässigkeit von Facebook Fanpages (SSN 4/2019) wird uneingeschränkt verneint.

Die Beispiele hinterlassen den Eindruck, dass die Aufsichtsbehörden sich mit einer eindeutigen Positionierung insbesondere zu amerikanischen Cloud-Angeboten schwer tun – und gelegentlich liebgewonnene Feindbilder die Argumentation überlagern.

Secorvo News

Easy – Certificates ready2go

Auch in internen Netzen wird immer häufiger TLS eingesetzt. Die Einrichtung und Erneuerung von Serverzertifikaten kann inzwischen auch ohne eigene PKI über eine Clientsoftware vorgenommen werden, die kompatibel mit öffentlichen Trustcentern ist. Mit Certificates ready2go, einer Entwicklung von Secorvo, übernimmt ein ACME-Proxy (SSN 3/2019) die Domain-Validierung und ermöglicht so auch Servern im gesicherten internen Netz den vollautomatisierten Bezug und die Erneuerung von Zertifikaten, beispielsweise von Let's Encrypt. Mit dem zugehörigen Dashboard Easy behalten Sie dabei den Überblick über den Status aller Ihrer internen Zertifikate. Zu sehen auf der it-sa 2019.

Nächste Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), gefolgt von T.I.S.P. (**14.–18.10.2019**, schnelle Anmeldung empfohlen) und IT-Sicherheit heute (**22.–24.10.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss an den Vortrag haben Sie – wie gewohnt – Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)

Fundsache

Das NIST hat im Juni einen Entwurf für ein White Paper zur sicheren Softwareentwicklung veröffentlicht. Das White Paper hilft dabei, einen Software Development Life Cycle (SDLC) um Praktiken der sicheren Softwareentwicklung zu ergänzen. Kommentare können noch bis zum 05.08.2019 eingereicht werden.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

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