secorvo
security consulting

Secorvo Security News

Juli 2015

… denn sie wissen nicht, was sie tun.

Siebzig Jahre ist es her, dass James Dean in kürzester Zeit die unbekümmerte Ungezügeltheit der Jugend salonfähig machte. Daran konnten auch die Umstände seines frühen Todes nichts ändern. Und sein Vermächtnis wirkt offenbar bis heute fort.

So ist es in den vergangenen 20 Jahren endlich Schritt für Schritt gelungen, Sicherheit als eine wesentliche Eigenschaft eines IT-Systems zu verankern. Kaum ein Anbieter, der sich der Frage der Sicherheit eines neuen IT-Produkts nicht widmen würde – und sei es auf den letzten Metern vor der Produktivschaltung. Das ist das Ergebnis eines mühsamen, oft von unangenehmen (und vermeidbaren) Lernerfahrungen begleiteten Prozesses.

Doch kaum ist es so weit, konterkariert das „Internet der Dinge" diese Entwicklung auf erschreckende Weise: Elektrische Skateboards lassen sich via Bluetooth unter fremde Kontrolle bringen, kontaktlose „Smart-Keys" schalten das Fahrzeug einfach aus, wenn Mitfahrer sie während der Fahrt aus dem Fenster werfen. Ein Automobilhersteller liefert Autos mit Internet-Zugang, die sich während der Fahrt von unberechtigten Dritten steuern und manipulieren lassen – und bittet anschließend seine Kunden, einen Patch über das Internet herunterzuladen und via USB-Stick zu installieren (siehe diese SSN). Schließlich kommt ein 13.000 US$ teures Präzisionsgewehr auf den Markt, bei dem Unberechtigte die Zieleinrichtung via WLAN umkonfigurieren können.

In Fragen der Sicherheit scheint ungezügelte, von Kompetenz unbelastete Produktentwicklung im Internet der Dinge wieder „En Vogue" zu sein – ungeachtet der um ein Vielfaches größeren Gefahren, die dabei für Leben und Gesundheit drohen. Wir können nur hoffen, dass die Lernkurve diesmal steiler und kürzer ausfällt.

Inhalt

secorvo
security consulting

Security News

Mit Daten bezahlen

Was lange von Datenschützern befürchtet wurde, wird nun wahr: Ab 2016 werden unsere Gesundheitsdaten zur Währung. Die Generali plant die Einführung ihres Tarifs „Vitality“ in 2016. Per Smartphone-App können Versicherte Fitnessdaten an Generali übermitteln und werden für einen gesunden Lebensstil mit Rabatten belohnt. Derweil hat Apple am 16.07.2015 ein Verfahren zum Patent angemeldet, mit dem Nutzern eines Smartphones oder Tablets nur dann bestimmte Werbeanzeigen eingeblendet werden, wenn sie sich die beworbenen Produkte oder Dienste auch leisten können. Festgestellt wird das anhand von Bank- oder Prepaid-Guthaben.

Noch sind solche Angebote die Ausnahme, und nur eine Minderheit von freiwilligen „First Movern“ wird sie nutzen. Irgendwann aber wird sich das Blatt wenden. Wer seine Daten dann nicht als Zahlungsmittel einsetzt, wird unter Rechtfertigungsdruck geraten. Mit Freiwilligkeit hat die Datenpreisgabe dann nichts mehr zu tun.

Clipper reloaded

Vor gut 22 Jahren, am 16.04.1993, löste die US-Regierung mit einer Pressemitteilung zum Clipper-Chip eine heftige Debatte über Verschlüsselung aus. Sie plante damals die Einführung einer Telefonie-Verschlüsselung mit einer Zugriffsmöglichkeit für die Strafverfolgungsbehörden. Die öffentliche Diskussion mündete schließlich 1997 in einer öffentlichen Stellungnahme führender Kryptologen mit dem Titel „*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*“, die dazu beitrug, dass in den USA und Europa die Regulierung von Verschlüsselung aufgegeben wurde.

Aber Geschichte wiederholt sich. Begehrlichkeiten von Ermittlungsbehörden, wie sie von FBI-Direktor James B. Comey am 16.10.2014 ausgesprochen wurden, haben eine Kryptodebatte 2.0 losgetreten. Daher haben nun die Autoren der Stellungnahme von 1997 erneut Position bezogen. In ihrem Papier „*Keys Under Doormats*“ vom 06.07.2015 machen sie deutlich, dass Zugriffsmöglichkeiten für Strafverfolgungsbehörden auf verschlüsselte Daten die Fortschritte bei der Sicherheit im Internet konterkarieren: durch höhere Komplexität, zentrale Angriffspunkte und Hintertüren, die von Dritten ausgenutzt werden können. Es ist zu hoffen, dass das Papier den Gegnern offener Kryptografie den Wind genauso aus den Segeln nehmen wird wie die Stellungnahme 19 Jahre zuvor.

Ferngesteuert in den Graben

Chris Valasek und Charlie Miller sorgten am 21.07.2015 mit der Veröffentlichung eines Hacks, den sie auf der diesjährigen BlackHat vorstellen werden, bei Autofahrern für Gänsehaut: Es gelang ihnen, mittels einer Schwachstelle im Uconnect-Bordsystem über das Internet direkt auf Fahrzeuge verschiedener Marken des Konzerns Fiat-Chrysler (unter anderen Jeep, Fiat und Alfa Romeo) zuzugreifen. So konnten sie bei einem gekaperten Jeep Cherokee nicht nur die Bordelektronik (Klimaanlage, Radio) fernsteuern, sondern bekamen auch sicherheitskritische Komponenten unter ihre Kontrolle: Sie konnten Hupen, Bremsen deaktivieren und in die Lenkung eingreifen. Auch beim Umgang mit der Schwachstelle schwächelte Chrysler – und bot über die Uconnect-Webseite ein Executable zum Download für die Installation via USB-Stick an.

Die Schwachstelle ist kein Einzelfall, wie Valasek und Miller bereits 2014 in einer 100seitigen Studie belegten. Sie beweist aber überdeutlich, dass durch die für die Vernetzung von Auto und Smartphone erforderliche Anbindung an das Internet neue Bedrohungen entstehen – und sich auch traditionelle Industriezweige ernsthaft mit Security Engineering befassen sollten.

Sozialadäquanz als Erlaubnistatbestand?

Schon in den SSN 3/2015 berichteten wir über die geplante Neufassung von § 2 BORA (Berufsordnung der Rechtsanwälte), die das Outsourcing bei Berufsgeheimnisträgern legalisieren sollte. Der Bundesjustizminister hatte den Beschluss mit Verweis auf die mangelnde Regelungsbefugnis am 04.03.2015 aufgehoben. Auf Intervention der Bundesrechtsanwaltskammer wurde die Aufhebung am 31.03.2015 wieder rückgängig gemacht und die Neuregelung trat am 01.07.2015 in Kraft.

Damit ist die Inanspruchnahme von Leistungen Dritter nun auch bei Gefahr einer möglichen Offenbarung von geheimen Inhalten zulässig, wenn sie „objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)“. Bisher machte sich ein Berufsgeheimnisträger durch unbefugte Offenbarungen strafbar, wenn er bspw. externe IT-Dienstleistungen in Anspruch nahm, bei denen er mit eigenen Mitteln einen unberechtigten Zugriff auf die Daten kaum verhindern konnte.

Bei allem Verständnis für das Dilemma: Die Argumentation der Rechtsanwaltskammer ist angesichts des hohen Schutzgutes gefährlich. Soll ein ungenügender Schutz, der üblich wird, künftig als Legitimationsgrundlage taugen?

Weisungsfreiheit externer DSBs

Das Landesarbeitsgericht Düsseldorf hat in einem jüngst veröffentlichten Urteil vom 04.03.2015 wichtige Standpunkte zur Stellung eines in einem Drittunternehmen angestellten, persönlich bestellten externen Datenschutzbeauftragten ausgeführt. Darunter sind für externe Datenschutzbeauftragte die folgenden Aussagen besonders interessant:

Die arbeitsvertragliche Weisungsgebundenheit des zum externen DSB persönlich bestellten Unternehmensmitarbeiters steht der Weisungsfreiheit gegenüber der verantwortlichen Stelle nicht entgegen. Auch das Benachteiligungsverbot betrifft nur das Vertragsverhältnis zur verantwortlichen Stelle. Eine persönliche Bestellung darf allerdings dem Angestellten eines dritten Unternehmens nicht aufgedrängt werden, es sei denn, dies ist Teil der arbeitsvertraglichen Leistung.

Tatsächlich ist die BDSG-konforme Bestellung eines externen Datenschutzbeauftragten unter Experten umstritten. Durch diese Entscheidung wird die Bestellung von Angestellten aufgewertet – ein bislang eher kritisch betrachteter Weg. Zu empfehlen ist er wegen des Auseinanderfallens von Bestellung und Leistungsvertrag dennoch nicht.

Einjährige Hackerin

Am 18.07.2015 gelang einem einjährigen Mädchen ein unfreiwilliger Hack des VW Passat ihrer Mutter: Es warf auf der A1 den Schlüsselbund mitsamt dem Smart-Key des Passat aus dem Fenster. Sofort schaltete sich der Motor aus – die Mutter konnte den Wagen glücklicherweise noch unfallfrei auf den Standstreifen lenken.

Offenbar ist der Hersteller hier bei der Bedrohungsanalyse zu kurz gesprungen. Bequemlichkeit sollte besser nicht vor Sicherheit gehen, schon gar nicht, wenn dadurch Leib und Leben in Gefahr geraten können. Auch bei Automobilzulieferern sollte man besser Security Engineering praktizieren.

Side-Channel in der Cloud

Auf der diesjährigen Recon stellte Sophia D'Antoine am 19.06.2015 einen sehr interessanten Side-Channel Angriff auf virtuelle Maschinen (VM) vor. VMs nutzen Hardware-Ressourcen gemeinsam; die virtuellen Instanzen und die darauf verarbeiteten Daten werden über einen Hypervisor getrennt. D'Antoines Angriff liest über den gemeinsamen Zugriff zweier VMs auf die Level-3-Caches des Prozessors Daten der VMs untereinander aus. Yuval Yarom und Katrina Falkner zeigten bereits am 05.07.2013 in „aFLUSH+Reload: A High Resolution, Low Noise, L3 Cache Side-Channel Attack", wie von einer Angreifer-VM aus z. B. auf den privaten PGP-Schlüssel in einer zweiten VM zugegriffen werden kann.

Wer vertrauliche Daten in der Cloud verarbeitet sollte nicht nur seinen Provider, sondern auch seine unmittelbaren Nachbarn auf Vertrauenswürdigkeit prüfen: Auch Hardware sollte man besser nicht unbesehen mit jedermann teilen.

Secorvo News

Secure Coding

Kaum ein Angriff, der zu seiner Durchführung nicht auf eine Software-Schwachstelle angewiesen wäre. Daher gilt: Wer das Übel an der Wurzel packen möchte, muss dafür sorgen, dass Software sicherer wird. Seit einigen Jahren engagiert sich Secorvo deshalb für sichere Software-Entwicklung und unterstützt Unternehmen mit entsprechenden Trainings.

Neben dem Seminar „Certified Professional for Secure Software Engineering" (CPSSE) sind daraus nun zwei Seminare speziell für Softwareentwickler entstanden: Für Java- und für C/C#-Entwickler bietet Secorvo College ab Oktober zwei Schulungen, die vermitteln, wie Sicherheit „programmiert" werden kann. Java Security findet statt am 13.-16.10.2015, und Secure Coding C/C# bieten wir an am 01.-03.12.2015.

T.I.S.P., PKI und aktuelle Fragen

Ende September (21.-25.09.2015) und Ende November (23.-27.11.2015) können Sie Ihre Kenntnisse und Erfahrungen mit dem T.I.S.P.-Zertifikat krönen – beim „Seminar zum Buch".

Schon einige hundert Teilnehmer haben sich mit unserem laufend aktualisierten Hands-on-Seminar „PKI – Grundlagen, Vertiefung, Realisierung" mit CAs, CRLs und OCSP vertraut gemacht. Die nächste Gelegenheit für die Teilnahme an diesem PKI-Steilkurs bietet sich Ihnen am 20.-23.10.2015 (schnelle Buchung empfohlen).

Mit der Neuauflage unseres Seminars IT-Sicherheit heute – das Schlaglicht auf die Informationssicherheit setzen wir auf aktuelle Themen mit hoher Relevanz für die Praxis – und auf eine Kombination auf konzentrierter Wissensvermittlung, Erfahrungsaustausch und Diskussion. Nächster Termin: 29.09.-01.10.2015.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/seminare.

Veranstaltungshinweise

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

August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D·A·CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)

Fundsache

Am 23.07.2015 veröffentlichte Google die Ergebnisse der Studie *Comparing Expert and Non-Expert Security Practices*. Die Befragung von über 500 Experten und Laien zeigt Aufklärungsbedarf: Während Experten Software-Updates für die wichtigste Maßnahme halten, setzen Laien auf Antivirus-Software – bei Experten nicht unter den fünf wichtigsten.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, 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