secorvo
security consulting

Secorvo Security News

Juni 2017

In der Matrix

Der Wirtschaftsnobelpreisträger Daniel Kahnemann („Schnelles Denken – Langsames Denken“) hat nicht nur dem Bild des rationalen „homo oeconomicus“ den Todesstoß versetzt, sondern deutlich gemacht, dass unsere vermeintlich vernünftigen Entscheidungen allzu oft das Ergebnis „kognitiver Verzerrungen“ sind: Wir schätzen Risiken falsch ein, werden von irrelevanten Relationen abgelenkt und lassen uns durch „Anker“ z. B. bei Käufen auf Preise festlegen.

Zwar sind uns solche Wirkungen grundsätzlich vertraut: Wir kennen den Trick der Lebensmittelläden, neben der Kasse Schokolade in Kinderaugenhöhe zu platzieren. Wir wissen aus Blindtests, dass Marken unser Geschmacksempfinden beeinflussen. Und uns ist klar, dass die „Wird-oft-zusammen-gekauft“-Vorschläge des Online-Shops nicht philanthrop gemeint sind, sondern der Umsatzmaximierung dienen. Dennoch bilden wir uns ein, auf diese Einflüsse souverän zu reagieren – schließlich können wir auch anders entscheiden.

Unter der Oberfläche ist die Technik dank Big Data aber schon viel weiter. Shops lernen, ab welchem prozentualen Preisnachlass wir zugreifen, sie können aus unserem Einkaufsverhalten prognostizieren, wann wir in Spendierlaune sind, und passen ihre Angebote an unsere IT-Umgebung an: Für Mac-Nutzer ist das Leben meist teurer. Google-Remarketing sorgt für individualisierte Online-Anzeigen, die sich aus früheren Seitenbesuchen ableiten – da kann auch mal ein Shop dabei sein, der uns an einen abgebrochenen Kaufvorgang erinnert. Die virtuelle Welt wird bereits für uns zurechtgebastelt.

Und jetzt kommt die Wirklichkeit an die Reihe: Plakatwände, die uns wiedererkennen und die Werbung anpassen oder Läden, die unser Surfverhalten am WLAN-Hotspot auswerten und Preisvergleiche unterbinden, sind nicht mehr fern. Alles anonym, natürlich, und somit kein Datenschutzproblem.

Heimlich, still und unbemerkt sind wir auf dem Weg in die Matrix.

Inhalt

secorvo
security consulting

Security News

Blackout real

Pünktlich zum fünfjährigen Jubiläum des Bestsellers Blackout haben Sicherheitsexperten von ESET am 12.06.2017 die detaillierte Analyse einer Schadsoftware veröffentlicht, die sie „Industroyer" getauft haben. Die Autoren spekulieren, dass die Software für den weitreichenden Stromausfall in Kiew am 17.12.2016 verantwortlich war – die technischen Fähigkeiten dafür besitzt sie offenbar. Die auf 17 Seiten dokumentierten technischen Details machen deutlich, dass es Angreifer gibt, die sich mit viel Know-how und Ressourcen industriellen Zielen widmen. Die dort verbreiteten Protokolle IEC 101 und IEC 104 sind zwei der Angriffspunkte, die über dynamisch aktivierbare Module attackiert werden.

Die erschreckende Vision von Marc Elsberg ist leider wohl (noch immer) näher an der Realität als Mancher es wahrhaben möchte. Für Betreiber von KRITIS-Infrastrukturen ist eine Absicherung nach dem Stand der Technik im Sinne des IT-SiG spätestens jetzt überfällig.

Spyware as a Service

Am 09.06.2017 erschienen erste Berichte zu einer neuen Spyware, die es auf Macs abgesehen hat. Das Besondere daran: Sie wird über das Darknet als Service verkauft. Gegen eine Gebühr von 30 Bitcoins (derzeit etwa 75.000 €) kann man den Service als Franchisenehmer weiterverkaufen. Die Spyware ermöglicht einem Angreifer, Bildschirmfotos, Umgebungsgeräusche und Tastaturanschläge aufzuzeichnen, Browserdaten auszulesen, iCloud-Fotos zu kopieren und die Zwischenablage zu sichern. Seit dem 15.06.2017 erkennen die gängigen Antivirenprogramme die Schadsoftware. Etwa zum gleichen Zeitpunkt erschien mit MacRansom ein Kryptotrojaner „as a Service" für MacOS.

Aufgrund seiner wachsenden Verbreitung zieht MacOS immer mehr Aufmerksamkeit von Hackern und Kriminellen auf sich. „Macs sind sicher" – so einfach ist die Welt mittlerweile nicht mehr.

Kritische Infrastrukturen, Teil 2

Das Bundeskabinett hat am 31.05.2017 den Referentenentwurf für den zweiten Korb der Verordnung zur Bestimmung Kritischer Infrastrukturen verabschiedet. Damit wird in Kürze auch für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr feststehen, welche Betreiber den Regelungen für Kritische Infrastrukturen unterfallen.

Die Änderungsverordnung bedarf keiner Zustimmung des Bundesrats, so dass noch im Juni mit einer Veröffentlichung im Bundesgesetzblatt gerechnet werden kann. Die nun erfassten Betreiber haben anschließend ein halbes Jahr Zeit, ihre Kontaktstelle für Meldungen (§ 8b Abs. 3 BSIG) einzurichten und zwei Jahre, um die nach § 8a BSIG geforderten Sicherheitsmaßnahmen umzusetzen.

Die Änderungsverordnung ergänzt zudem die bereits erlassenen Anhänge und Kataloge um Definitionen der Anlagen und passt einige Schwellenwerte an. Auch bei den neuen Sektoren wird die Kritikalität nach Versorgungs- oder Kapazitätsschwellenwerten festgestellt.

Während das Finanz- und Versicherungswesen bereits heute einer vergleichsweise strengen Regulierung in Sachen IT-Sicherheit unterliegt, kommen auf die Gesundheitsbranche und die Transport- und Verkehrsbetriebe vielfach neue Anforderungen zu, die bei den betroffenen Unternehmen und Einrichtungen für erheblichen Beratungs- und Dokumentationsbedarf sorgen werden.

Anonymes Internet 3.0

Wie werden Surfer im Internet identifiziert? Früher (und manchmal noch heute) geschah dies mit Hilfe von Cookies oder der IP-Adresse. Aber auch wer Cookies vermeidet und über mobile Netze surft, kann über weitere Merkmale identifiziert werden. Durch eine Korrelation der über den Browser zugänglichen Informationen wie Browserversion, Betriebssystem oder die installierten Plugins kann ein Benutzer „wiedergefunden" werden.

Wer dies vermeiden möchte, verwendet dedizierte Browser für einen anonymeren Zugang wie den am 07.06.2017 in Version 7.0 veröffentlichten Tor-Browser. Darin wird eine Identifikation des Nutzers durch Härtung des Browsers hinsichtlich der preisgegebenen Informationen erschwert und die Analyse der Internetnutzung durch Verwendung des Tor-Netzwerks verhindert. Wem dieses Maß an Privatheit noch nicht reicht, dem sei nahegelegt, sich die Mitte Juni angekündigte runderneute Version von Tails anzusehen. Tails 3.0 bietet eine - in der Regel von einem USB-Stick gestartete – Plattform an, welche ebenfalls das Tor-Netzwerk und den Tor-Browser nutzt. Durch die Nutzung dieser allgemeinen Plattform und Vermeidung individueller Informationen wird eine persönliche Zuordnung des Nutzers weiter erschwert.

OpenVPN erwischt

Wieder hat es ein Open-Source-Produkt erwischt: Am 21.06.2017 gab Guido Vranken in seinem Blog die Entdeckung von vier schwerwiegenden Sicherheitsschwächen bekannt – die zuvor von zwei un-

abhängigen Sicherheitsaudits nicht entdeckt und durch ein Code-Hardening nicht beseitigt worden waren. Aufdecken konnte er die Fehler durch Fuzzing, eine bereits 1989 entwickelte Analysemethode, der wir inzwischen die Entdeckung zahlreicher Bugs in unterschiedlichsten Anwendungen verdanken. OpenVPN-Nutzer sollten umgehend auf die Versionen 2.3.17 bzw. 2.4.3 wechseln.

Der Fall macht deutlich, dass eine Standardisierung der Methoden zur Code-Auditierung überfällig sind: zu häufig blieben kritische Schwachstellen unentdeckt, obwohl Verfahren zu deren Aufspürung existieren.

Grenzwertiges Marketing

Bereits am 30.05.2017 wurde Amazon ein Patent für ein von Miles J. Ward entwickeltes Verfahren erteilt, mit dem der Einzelhandel einen Internet-Preisvergleich der Kunden über das Laden-WLAN registrieren und unterbinden kann. Zwar muss man in Europa vorläufig nicht mit dem Einsatz dieser Lösung rechnen: Eine Sperrung des Zugriffs auf Vergleichsportale und andere Anbieter über das WLAN-Angebot ist rechtlich zulässig, nicht aber eine Auswertung der WLAN-Nutzung – das wäre ein rechtswidriger Eingriff in das Telekommunikationsgeheimnis.

Derzeit testen die Deutsche Post in rund 100 und Real in 40 Filialen im Rahmen eines Feldversuchs eine vom Fraunhofer-Institut in Erlangen entwickelte Analysesoftware, mit der sich die Inhalte von Werbetafeln über eine Auswertung von Videoaufzeichnungen der Betrachter steuern lassen. Dabei bestimmt die integrierte Gesichtserkennung Alter, Geschlecht und Verweildauer des Kunden.

Die Rechtmäßigkeit dieser Videoanalysen wurde vom Bayerischen Landesamt für Datenschutzaufsicht bestätigt. Auf die Videoüberwachung werde hingewiesen, und die Analyse erhebe keine personenbezogenen Daten.

Die beiden Beispiele zeigen, dass die Grenzen des datenschutzrechtlich Erlaubten nicht nur in der Online-Werbung sondern auch bei Ladenbesuchen zunehmend ausgereizt werden. Bei den Videoanalysen mit Gesichtserkennung treffen dabei durchaus plausible Anonymisierungskonzepte auf das Problem mangelnder Transparenz und Vertrauenswürdigkeit. Dabei wird zweifellos bei den Betroffenen ein Überwachungsdruck erzeugt, dessen datenschutzrechtliche Berücksichtigung allerdings umstritten ist.

Diskrete Anpassung

Weitgehend unbeachtet von der Öffentlichkeit treibt der Gesetzgeber die Anpassung des Datenschutzrechts an die Europäische Datenschutz-Grundverordnung voran. Die jüngsten Änderungen von immerhin 12 Gesetzen verstecken sich in einem am 01.06.2017 verabschiedeten Artikelgesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften.

Darin behandelt werden vor allem Betroffenenrechte in Bezug auf öffentliche Register, bspw. das Handelsregister, das Patent- und Markenregister oder das Register vergriffener Werke, sowie die Verarbeitung von Daten durch die Finanzbehörden (Änderungen der AO). Hier ist besonders die Regelung zur Auftragsdatenverarbeitung von Steuerdaten hervorzuheben: Die hier vorgenommenen strengen Einschränkungen bilden einen Gegensatz zu den Planungen bzgl. der Dienstleister anderer Berufsgeheimnisträger. Beschränkt werden das Auskunftsrecht, Mitteilungspflichten gegenüber dem Betroffenen und Berichtigungsansprüche.

Bei den vorgenommenen Beschränkungen kann sich der Gesetzgeber auf Art. 23 DSGVO stützen. Dieser lässt allerdings Einschränkungen der Betroffenenrechte nur zu spezifischen Zielen im öffentlichen Interesse zu, nicht zur Aufwandsbegrenzung der Behörden. Zudem gibt Abs. 2 Kompensationen vor. Hier hat der Gesetzgeber den Gestaltungsspielraum der DSGVO womöglich überschritten.

Secorvo News

Secorvo Seminare

Nach dem T.I.S.P. ist vor dem T.I.S.P. – gerade erst haben sich zwölf Teilnehmer unseres T.I.S.P.-Seminars erfolgreich auf die Zertifizierung vorbereitet, und schon läuft die Vorbereitung des nächsten T.I.S.P.-Seminars vom **25. bis 29.09.2017**. Die Sommerpause ist die beste Zeit zur Vorbereitung: Nach Ihrer Anmeldung erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ zugesandt. Die letzte Gelegenheit zur T.I.S.P.-Zertifizierung im Jahr 2017 bieten wir Ihnen vom **27.11. bis 01.12.2017**.

Für unser PKI-Seminar vom **06. bis 09.10.2017** gibt es bereits zahlreiche Anmeldungen, daher empfehlen wir allen Interessenten an einem vertieften Einblick in Public Key Infrastrukturen eine baldige Buchung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

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

Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)
August 2017	
06.-09.08.	DFRWS USA 2017 - Digital Forensic Research Workshop (DFRWS, Austin/US)
16.-18.08.	26th USENIX Security Symposium (Usenix, Vancouver/BC)
20.-24.08.	Crypto 2017 (IACR, Santa Barbara/US)

Fundsache

Bereits am 18.11.2016 hat die Group Privacy der Deutschen Telekom eine erste Fassung von konzernweit gültigen „Binding Interpretations" der DSGVO verfasst. Das hilfreiche, gut 100 Seiten starke Dokument ist online zugänglich.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp

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