secorvo
security consulting

Secorvo Security News

Mai 2019

Kognitive Verzerrungen

Eine der an Einsichten reichste Lektüre der vergangenen Jahre war für mich die Veröffentlichung des Wirtschaftsnobelpreisträgers 2002, Daniel Kahneman: ‚Thinking, fast and slow' (‚Schnelles Denken, langsames Denken', 2011). Darin deckt der Psychologe Wirkmechanismen des menschlichen Denkens auf, die viele Wunderlichkeiten des Homo Rationalis (von ihm „kognitive Verzerrungen" genannt) verständlich machen.

Ein zentraler Mechanismus ist das Denken in Relationen. Wir kennen das von optischen Täuschungen: Identische Objekte erscheinen im Kontext kleinerer bzw. größerer Objekte unterschiedlich groß – selbst wenn wir um ihre gleiche Größe *wissen*, können wir sie nicht gleich groß *sehen*. Diese Relativität durchzieht unser gesamtes Denken. Der Mechanismus wird besonders offensichtlich bei Entscheidungen in Geldfragen: Nicht der absolute Preis, sondern das Verhältnis zu anderen Preisen ähnlicher Güter entscheidet. Das gilt vor allem, wenn eine Ware oder Leistung keinen allgemein anerkannten, „typischen" Preis besitzt: Eine Uhr für 1.400 € erscheint teuer neben einer für 99 €, aber günstig neben einer für 4.500 €.

Umgekehrt fällt es Menschen schwer, den Wert vieler „abstrakter Güter" wie Bildung, Gesundheit oder Freiheit einzuordnen. Damit erscheinen sie „unvergleichbar", denn sie lassen sich vom menschlichen Gehirn nicht in Relation zu anderen Gütern oder Werten setzen. Wie wertvoll ist unsere Privatsphäre? Und wie hoch der Verlust, wenn z. B. unsere E-Mail-Adresse bekannt wird?

Das ändert sich sofort, wenn ihnen ein Preis zugeordnet wird. Und vielleicht wird dies eines Tages das größte Vermächtnis der DSGVO sein: Über die von den Aufsichtsbehörden verhängten Ordnungsgelder erhält unsere Privatsphäre einen Wert, der sie vergleichbar macht. So wissen wir nun: Die Preisgabe von E-Mail-Adressen in einem Verteiler kostet 2.000 €. Fast so viel wie zwei iPhone XS.

Inhalt

secorvo
security consulting

Security News

ZombieLoad und Firmwareschwachstellen

Gleich zwei Mal machte der Chiphersteller Intel im Mai durch Schwachstellen auf sich aufmerksam. Am 14.05.2019 veröffentlichte Intel das Security Advisory INTEL-SA-00213, in dem mehrere kritische Schwachstellen in der Firmware beschrieben werden. Am selben Tag wurde eine neue Schwachstellenkategorie namens Microarchitectural Data Sampling (MDS) bekannt: Wird der Prozess eines Angreifers auf dem gleichen Kern wie ein Opferprozess ausgeführt, so kann der Angreifer Speicherbereiche des Opfers lesen. Im Kontext von Hyper Threading funktionieren derartige Angriffe besonders gut. Die Fallout, RIDL und ZombieLoad genannten Schwachstellen folgen den Schwachstellen Spectre und Meltdown: Schon wiederholt wurden Schwachstellen sowohl in den Intel CPUs als auch in den Management-Technologien (z. B. der Intel Management Engine) entdeckt. Ursache dieser Schwachstellen sind eine immer höhere Komplexität und Leistungsoptimierung auf Kosten der Sicherheit. So bringen moderne Plattformen diverse schlecht oder gar nicht dokumentierte Features mit, die die Angriffsfläche erhöhen. Für die aktuellen Schwachstellen stehen Sicherheitsupdates bereit, die unverzüglich eingespielt werden sollten.

Spyware Hook

Am 14.05.2019 wurde bekannt, dass die israelische Firma NSO Group eine kritische Schwachstelle in WhatsApp nutzte, um Spyware auf iOS- und Android-Smartphones zu installieren. Dazu genügte ein telefonischer Verbindungsversuch, der nicht einmal in der Anrufliste erscheint.

Kunden der auf Cyberwarfare spezialisierten Firma sind – eigenen Angaben zufolge – Regierungen und deren Sicherheitsbehörden, die damit Terrorismus bekämpfen. In jüngster Vergangenheit wurden Angriffswerkzeuge der NSO Group aber auch gegen Menschenrechtsaktivisten, Journalisten und mindestens einen Anwalt eingesetzt. Meldungen über ähnliche Angriffe, die ebenfalls in Verbindung zur NSO Group stehen, gab es bereits im August 2018.

Aber ganz unabhängig vom Geschäftsmodell des Unternehmens bleibt zu fragen, was von einem Unternehmen zu halten ist, dass entdeckte Sicherheitslücken zu eigenen Geschäftszwecken geheim hält – und damit wissentlich Milliarden Endgeräte weiter potentiellen Angriffen aussetzt.

Log-Password-Leaks

Passwörter sollen nur mit einer geeigneten Hash-Funktion und einem individuellen Salt geschützt gespeichert werden – das ist Best Practice, wie man u. a. beim NIST nachlesen kann. Auch Facebook, GitHub, Google und Twitter wissen das. Trotzdem hatten alle vier Unternehmen in jüngerer Vergangenheit Schwierigkeiten, das beim Umgang mit Nutzerpasswörtern zu beherzigen, wie zuletzt am 21.05.2019 von Google gemeldet: So wurden die eingegebenen Passwörter als „Beifang“ in Log-Dateien des Anbieters protokolliert. Bei Facebook hatten mehr als 20.000 Facebook-Mitarbeiter Zugriff auf diese Protokolle.

Zur Fehlerbehebung ist das Protokollieren von Anfragen äußerst nützlich, aber Passwörter haben darin nichts verloren und dürfen niemals im Klartext gespeichert werden. Dem Endnutzer bleibt nur darauf zu vertrauen, dass die Anbieter in dieser Hinsicht keine Fehler machen. Weil das aber ganz offensichtlich selbst bei großen Anbietern keine Selbstverständlichkeit ist, sollten Endnutzer für jeden Dienst ein anderes Passwort verwenden. Und gegen Vergessen hilft ein Passwortmanager.

Angreifbare Altlasten

Eine Standardinstallation von Windows 10 umfasst neben dem Edge-Browser noch heute den immer weniger gepflegten Internet Explorer (IE). Eine am 28.03.2019 veröffentlichte XXE-Schwachstelle beim Umgang mit MHTML-Dateien (*.mht) erlaubt es Angreifern, über eine manipulierte MHTML-Seite Dateien vom System des Opfers zu laden.

Aus dem Internet heruntergeladene Dateien werden unter Windows mit dem so genannten „Mark of the Web“ (MOTW) versehen – einem speziellen Attribut, welches eine Datei als nicht vertrauenswürdig einstuft und die weitere Verarbeitung einschränkt. Dadurch würde der Angriff normalerweise verhindert, doch der Mechanismus funktioniert nicht ordnungsgemäß beim Download mit Edge, da dieser die Zugriffsberechtigungen der heruntergeladenen Datei durch ein nicht dokumentiertes Sicherheits-Feature so verändert, dass niedrig privilegierte Prozesse wie die des IE die Dateiattribute nicht mehr lesen können. Anstatt die Datei in einem solchen Fall als „nicht vertrauenswürdig“ einzustufen, macht der IE das Gegenteil.

Offizielle Patches für diese Probleme gibt es bisher nicht und Microsoft kündigte lediglich an, dass eine Lösung in einer zukünftigen Version des Internet Explorers „in Erwägung gezogen“ werde. Bis dahin kann man sich vor solchen Angriffen nur schützen, indem man MHTML-Dateien standardmäßig mit einem anderen Programm als dem IE öffnet (z. B. einem Texteditor) oder den Internet Explorer deaktiviert. Alternativ hilft auch der Drittpartei-Patch von 0patch (ohne Gewähr).

secorvo
security consulting

Automatisieren statt Aufpassen

Anfang Mai konnten Firefox-Anwender weltweit keine Add-ons mehr ausführen, weil deren Code-Signatur als ungültig erkannt wurde: Das Zertifikat einer Intermediate-CA im Zertifikatspfad der Code-Signing-Zertifikate für Add-on Entwickler war am 04.05.2019 abgelaufen. Die Mozilla-Entwickler hatten als Validierungszeitpunkt den Termin gewählt, an dem das betreffende Add-on geladen wird – und nicht den Zeitpunkt, zu dem die Code-Signatur angebracht wurde. Microsofts Authenticode Code-Signaturverfahren nutzt dazu korrekter Weise Timestamps.

Noch blamabler ist, dass das Intermediate-CA-Zertifikat ohne eine rechtzeitige Erneuerung ablaufen konnte – zumal Mozilla das gleiche Malheur bereits drei Jahre zuvor unterlaufen ist. Dabei sollte die Erneuerung von Zertifikaten und CRLs wo immer möglich automatisiert und der Gültigkeitsstatus aktiv überwacht werden. Besser Aufpassen war noch nie eine gute Empfehlung.

Arbeitszeiterfassung und Leistungskontrolle

Mit Urteil C-55/18 vom 14.05.2019 verpflichtet der EuGH Arbeitgeber, die tägliche Arbeitszeit der Arbeitnehmer zu messen. Was der einen (insbesondere Gewerkschaften und Co.) Freud, da nun endlich die geleisteten Überstunden erfasst werden, ist der anderen Leid: Die Arbeitgeber fürchten einen Rückfall in Stechuhrzeiten, den Wegfall flexibler Arbeitszeitmodelle und Schwierigkeiten im Hinblick auf die Ruhezeiten. Datenschutzrechtlich stellt die Einführung von Systemen zur Zeiterfassung kein großes Problem dar: § 26 BDSG bietet dafür die notwendige Rechtsgrundlage.

Zugleich erwägen viele Unternehmen, Client-Monitoring-Systeme einzuführen, mit denen oft auch eine sehr einschneidende Kontrolle insbesondere der Arbeitnehmerleistung möglich ist. Da solche Systeme häufig automatisiert Entscheidungen treffen, wird nicht nur die Rechtsgrundlage des § 26 BDSG verlassen, sondern auch der Anwendungsbereich des Art. 22 DSGVO mit weitreichenden datenschutzrechtlichen Konsequenzen eröffnet. So müssen die Arbeitnehmer mindestens in die Verarbeitung einwilligen – ein stacheliges Unterfangen, da die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis regelmäßig in Frage steht.

Damit ist klar, dass die EuGH-Entscheidung keineswegs als Freibrief für die Einführung von Leistungskontrollen missverstanden werden darf.

Secorvo News

Neu: Der PKI-Blog

Wer sich seit über fünfunddreißig Jahren mit Public Key Infrastrukturen (PKI) beschäftigt, hat einiges erlebt: Von den ersten RSA-Implementierungen auf PCs und Smartcards über das „Web of Trust" von Phil Zimmermans „Pretty Good Privacy" bis zur gesetzlichen Regulierung von „elektronischen Signaturen" und den manchmal bizarren Auswüchsen bei der praktischen Umsetzung. Inzwischen sind PKIs das Rückgrat vieler Sicherheitsmechanismen – und daher bei Fehlern auch gelegentlich Ursache weit reichender Sicherheitsprobleme. Seit Kurzem gewährt der Secorvo-PKI-Experte Hans-Joachim Knobloch einen Einblick in seine Erfahrungen und Erlebnisse rund um PKIs – in seinem eigenen PKI-Blog. Lesenswert.

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist „digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom „Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema „Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit" konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets') gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
06.06.	Wie souverän ist der Souverän? (KA-IT-Si, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (University of Minnesota, Stockholm/SWE)

Fundsache

Der am 09.04.2019 veröffentlichte Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS) hätte besser acht Tage früher erschienen sollen: Streicht man von den kompakten neun Seiten die Formalia (Deckblatt, Adressangabe, Vorwort, Inhaltsverzeichnis, Beschreibung, Literaturverzeichnis, Abkürzungsverzeichnis) und die überflüssige Grafik, bleibt nur Seite sechs übrig. Und es ginge noch kompakter: "Mindeststandard: Wenn TLS verwendet wird, dann müssen die Vorgaben aus BSI TR-02102-2 eingehalten werden." Aha.

Impressum

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

ISSN 1613-4311

Autoren: André Domnick, Fabian Ebner, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, 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