secorvo
security consulting

Secorvo Security News

Juli 2017

EDA-Daten

Ein beliebter Fehler in Kostenrechnungen sind die übersehenen EDA- (oder „Eh-da“-) Kosten: Fixkosten für Personal, Infrastruktur oder bereits verfügbare IT-Systeme. Sie erzeugen keine unmittelbaren Kosten – sind (oder waren) aber natürlich irgendwann einmal fällig. Würde man sie konsequent berücksichtigen, wären zahlreiche Projekte und Maßnahmen erheblich teurer als kalkuliert, und viele davon unwirtschaftlich. Genau deshalb sind sie bei Projektleitern so beliebt wie bei Controllern verhasst: Wer EDA-Kosten geschickt zu verstecken weiß, kann die Durchsetzung eines Lieblingsprojekts mit Wirtschaftlichkeitsargumenten forcieren.

Was dem Controller die EDA-Kosten sind dem Datenschützer die EDA-Daten: Mit jeder neuen Anwendung fallen sie an. Meist sind es Log-Daten, die ursprünglich zur Fehlersuche dienten. Für viele dieser Daten lassen sich zahlreiche andere Nutzungen finden: Verknüpft man Login- und Logout-Zeiten eines Administrators mit seinen Urlaubszeiten, lassen sich Unregelmäßigkeiten entdecken; leitet man aus den E-Mail-Logfiles die Intensität von Kommunikationsbeziehungen ab, kommt man womöglich Insidergeschäften auf die Spur.

Aber die Begehrlichkeiten machen bei Compliance- und Sicherheitsanwendungen nicht halt. Gewöhnt haben wir uns an die Auswertung unseres Online-Verhaltens, auch wenn uns vielleicht nicht klar ist, was diese Spuren alles enthüllen: Schon wenige hundert Likes erlauben Kaufprognosen, die so zuverlässig sind wie die Einschätzung unseres Lebenspartners. Auch Microsoft hat die Möglichkeiten der EDA-Daten entdeckt und bietet in Office 365 einen Dienst zur Analyse des Mitarbeiterverhaltens. Und der Hersteller des Mäh- und Staubsaugerroboters iRobot, Roomba, deutete kürzlich an, er wolle die über Wohnungen und Grundstücke erhobenen Daten verwerten.

Dabei gibt es – anders als bei EDA-Kosten – ein sehr einfaches und probates Mittel gegen EDA-Daten: Löschen.

Inhalt

secorvo
security consulting

Security News

WhatsApp illegal

Das Amtsgericht Bad Hersfeld hat sich in einem unterhaltsamen Sorgerechtsbeschluss vom 20.03. 2017 detailliert zur Legalität der Nutzung von WhatsApp geäußert und die Eltern zum Einholen von Einwilligungen aller im Adressbuch des Sohnes geführten Personen oder zur Deinstallation verpflichtet. Daneben stellte es eine Pflicht der Eltern zur Aneignung digitaler Kompetenz fest.

Der 12-jährige Sohn hatte vorgetragen, sein Vater habe ihn „auf WhatsApp blockiert". Das Gericht sah sich daraufhin veranlasst, Anordnungen zur Abwehr von Gefahren für das Kind zu treffen. Durch den Upload des Adressbuchs zur – nach den Geschäftsbedingungen – undefinierten weiteren Nutzung durch WhatsApp werde das Recht auf informationelle Selbstbestimmung (!) der geführten Personen verletzt, wodurch der Sohn möglichen Abmahnungen und Unterlassungsbegehren nach § 823 BGB ausgesetzt sein könne. Eine genauere Betrachtung der Rechtsgrundlagen des BDSG und der Verantwortlichkeiten erfolgte allerdings nicht.

Dass der Upload des Adressbuchs unter Vorbehalt undefinierter Nutzungszwecke rechtlich problematisch ist, ist zutreffend und führt zu Recht auch zu entsprechenden Warnungen bzgl. der WhatsApp-Nutzung im Unternehmensumfeld. Die hier verlangte Einwilligung kann dies allerdings mangels Bestimmtheit nicht heilen. Für das private Umfeld ist die Begründung des Amtsgerichts schlicht unzureichend. Als Beleg für die (durchaus vertretbare) Rechtswidrigkeit der WhatsApp-Nutzung ist das Urteil trotz seines klaren Tenors deshalb leider gänzlich ungeeignet.

Trau, schau, wem!

Die NSA hat Ende Juni die Liste ihrer Tools, die im Rahmen des NSA Technology Transfer Program (TTP) der Open Source Community zugänglich gemacht wurden, aktualisiert. Die Liste umfasst mehr als 30 Einträge, darunter WELM, GRASSMARLIN, SHB und LOCKLEVEL.

WELM extrahiert die in Windows Binaries eingebetteten Definitionen für Windows Event-Log-Einträge und konvertiert diese in besser auswertbare Formate wie JSON oder CSV. Um die Topologien von ICS- (*Industrial Control System*) bzw. SCADA- (*Supervisory Control and Data Acquisition*) Netzwerken zu analysieren, kann auf GRASSMARLIN zurückgegriffen werden. SHB (*Secure Host Baseline*) oder LOCKLEVEL beschäftigen sich mit der Härtung von Windows-Betriebssystemen.

Die Tools erfüllen den vorgesehenen Zweck – dennoch ist ein gesundes Misstrauen gegenüber den NSA-Tools zweifellos angebracht.

Schöne neue Arbeitswelt

Microsoft plant Analysetools anzubieten, die es ermöglichen sollen, das Zeitmanagement der Mitarbeiter bspw. bei der E-Mail-Nutzung oder Terminplanung sowie die Ressourcennutzung und Zusammenarbeit zu analysieren und auszuwerten. Workplace Analytics soll als Teil von Office 365 angeboten werden.

Workplace Analytics ist seit dem 05.07.2017 bereits als Add-On für Kunden der O365-Suite verfügbar. Der Deutsche Gewerkschaftsbund hat bereits reagiert und die spätestens durch dieses Angebot eingetretene betriebliche Mitbestimmungspflichtigkeit der O365-Einführung postuliert.

Dass es sich bei diesem Angebot um einen gut überlegten Schritt von Microsoft handelt, darf bezweifelt werden. Mit dem neuen Angebotsbestandteil werden die dem bisherigen Einsatz zugrunde liegenden datenschutzrechtlichen und betriebsverfassungsrechtlichen Erwägungen hinfällig. Unternehmen, die bereits O365 einsetzen, werden ihre Entscheidung nachbessern müssen – mit Blick auf die Mitbestimmung mit ungewissem Ausgang. Aus Datenschutzsicht ist der neue Dienst hinsichtlich der Rechtsgrundlagen und Datenschutzanforderungen kritisch zu prüfen; danach sind mindestens neue Prozesse und Regelungen zum Umgang mit diesem Dienst zu schaffen.

Berufsgeheimnisträger

Am 29.06.2017 hat der Deutsche Bundestag das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen verabschiedet. Das Gesetz beendet die Strafbarkeit der Auslagerung von IT-Dienstleistungen durch Berufsgeheimnisträger, die eintritt, sobald der Dienstleister Einblick in geschützte Daten erhält (§ 203 StGB). Im Ausgleich regelt es Voraussetzungen der Dienstleistereinbindung und das Zeugnisverweigerungsrecht des Dienstleisters (§ 53 StPO-neu).

Die Pflichten des Auftraggebers regelt das Gesetz in Änderungen der einschlägigen Berufsordnungen. Daher profitieren vor allem Ärzte zunächst noch nicht, da hier Landesregelungen angepasst werden müssen. Berufsgeheimnisträger müssen die Möglichkeit des Dienstleisters, auf vertrauliche Daten zuzugreifen, auf das Erforderliche beschränken, den Dienstleister sorgfältig auswählen und in einem schriftlichen Vertrag auf Verschwiegenheit verpflichten.

Die Strafbarkeit der Geheimnisoffenbarung wird auf die mitwirkenden Personen erstreckt; das Versäumen der Verpflichtung wird ebenfalls unter Strafe gestellt. Das Erfordernis von Auftragsdatenverarbeitungen bleibt unberührt.

Das Gesetz schafft eine überfällige Rechtsgrundlage vor allem für die zahlreichen IT-Dienstleistungen, deren Berufsgeheimnisträger bedürfen; diesbezüglich kann es nur begrüßt werden (SSN 1/2017). Der Schutz der Geheimnisse wird jedoch unweigerlich erheblich geschwächt.

Ende der Störerhaftung

Mit dem Dritten Gesetz zur Änderung des Telemediengesetzes hat der Bundestag nach der zaghaften Einschränkung vom 21.07.2016 nun in § 8 Abs. 1 TMG-neu die Haftung auf Schadensersatz oder auf Unterlassung von WLAN-Anbietern für rechtswidriges Nutzerverhalten ausgeschlossen. Das Gesetz wurde am 30.06.2017 verabschiedet, der Bundesrat muss nicht mehr zustimmen.

Mit der Abschaffung reagiert der Gesetzgeber auf das EuGH-Urteil zur WLAN-Haftung vom 15.09.2016. Für WLAN-Anbieter wird durch den Ausschluss der Störerhaftung ein wesentliches Rechtshindernis beseitigt, sodass Internetanschlüsse nun ohne Identifizierungserfordernisse oder Belehrungen der Nutzer Dritten zur Verfügung gestellt werden können. § 7 TMG-neu ermöglicht den Rechteinhabern allerdings, von den Anbietern Sperrungen von Inhalten zu verlangen. Die Kosten einer solchen Anordnung können jedoch nicht mehr dem Anbieter auferlegt werden.

Der Abmahnindustrie wird durch die Neuregelung weiter Boden entzogen. Für Anbieter und Internetnutzer handelt es sich trotz der verbliebenen Sperrthematik um eine lange erwartete gute Nachricht.

Secorvo News

SSN-Jubiläum

Am 04.07.2002 erschien die erste Ausgabe der Secorvo Security News. Seit nunmehr 15 Jahren versorgen wir Sie monatlich mit Hintergrundinformationen und Einschätzungen zu den (nach unserer Bewertung) wichtigsten Security-Ereignissen des jeweiligen Monats. 180 Ausgaben mit insgesamt 720 Seiten – trotz der von uns angestrebten inhaltlichen „Verdichtung“ ein kolossales Werk.

Wir danken Ihnen für Ihre Lese-Treue, mit der Sie dazu beigetragen haben, dass die SSN heute zu den wichtigsten Informationsquellen zur IT- und Informationssicherheit in Deutschland zählen.

Frisches aus der Hackerküche

Nach der Sommerpause werden Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) beim KA-IT-Si-Event am **21.09.2017** zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Anschließend stellen Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

Im Anschluss an die Vorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Secorvo-Publikationen

Webanwendungen sind eines der beliebtesten Einfallstore von Angreifern. Systematische Analysen und Penetrationstests können oft das Schlimmste verhüten. Wie man dabei vorgehen sollte, stellt Dr. Safuat Hamdy in Ausgabe 04/2017 der iX vor.

Und wer bloggen möchte, aber die Sicherheitsrisiken dynamischer Content-Management-Systeme (CMS) scheut, findet in Ausgabe 08/2017 der iX hilfreiche Hinweise von Kai Jendrian auf Alternativen.

Secorvo-Seminare

Die Sommerpause ist eine perfekte Gelegenheit zur Vorbereitung auf Ihre T.I.S.P.-Zertifizierung: Nach Ihrer Anmeldung für das T.I.S.P.-Seminar vom **27.11. bis 01.12.2017** erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ von uns.

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.

Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

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

Veranstaltungshinweise

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

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)
September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landes-zentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
26.-28.09.	Future Security 2017 (Fraunhofer VVS, Nürnberg)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, 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