secorvo
security consulting

Secorvo Security News

September 2018

Ein bisschen besser

Ende des vergangenen Jahrtausends, genauer am 01.09.1998, wurde Secorvo gegründet. Vier Tage vor Google. Und das fühlt sich ein wenig an wie ein Beleg für das schöne Bonmot von Herbert Hainer (von 2001 bis 2016 CEO bei Adidas) aus einem Interview im Jahr 2003: „Wenn Größe allein entscheidend wäre, würden die Dinosaurier heute noch leben und die Ameisen wären alle tot."

Wie lang uns ein solcher Zeitraum von zwanzig Jahren erscheint, hängt ganz von der Perspektive ab. Vor der (vermutlichen) Unendlichkeit des Universums ist er ein Nichts, für uns Menschen rund ein Viertel der Lebenszeit – und im IT-Bereich eine gefühlte Ewigkeit.

In den vergangenen 20 Jahren haben vor allem Kommunikationstechniken unseren Alltag grundlegend verändert. Die Welt ist dadurch kleiner und schneller geworden. Und dies hat zugleich schleichend – und zumeist unbemerkt – neue Rahmenbedingungen gesetzt. So entwickelt sich insbesondere Vertrauen, das „Schmiermittel" menschlicher Zivilisation, in einer zunehmend virtualisierten Welt aus anderen Zutaten als in zwischenmenschlicher Interaktion. Deutlicher ausgedrückt: Ohne wirksame Sicherheit und verlässlichen Datenschutz ist Vertrauen in technisch vermittelter Kommunikation schlicht unmöglich. Die Ableitung vertrauenswürdiger Sicherheit aus persönlichen Schlüsseln oder Passwörtern und die Umsetzung von Datenschutzanforderungen wie z. B. Löschfristen sind jedoch technisch komplex und organisatorisch anspruchsvoll. Vor allem aber höchst sensibel: Denn Nutzer müssen sich blind darauf verlassen können, dass Software, Hardware und Organisation dies sicherstellen. Davon sind wir leider noch immer ein ganzes Stück entfernt.

Wir hatten das Glück, in den vergangenen 20 Jahren in über 2.500 kleineren und größeren Projekten gemeinsam mit unseren Kunden an der Gestaltung solcher vertrauenswürdiger Prozesse und Datenschutz konformer Lösungen mitzuwirken. Und so, Tag für Tag, die Welt ein kleines bisschen besser zu machen. Vielen Dank dafür.

Inhalt

secorvo
security consulting

Security News

Umfrage ist E-Mail-Werbung

Am 10.07.2018 hat der sechste Zivilsenat des Bundesgerichtshofs entschieden, dass es unzulässig ist, Kunden per E-Mail zur Teilnahme an einer Kundenzufriedenheitsbewertung aufzufordern. Der Kläger hatte über „Amazon Marketplace" bei der Beklagten Waren bestellt. Per E-Mail übersandte die Beklagte die Rechnung, bedankte sich für den Kauf und bat den Kläger an einer Kundenzufriedenheitsumfrage teilzunehmen. Der Bundesgerichtshof teilte die Auffassung des Klägers, dass diese E-Mail eine unaufgeforderte unerlaubte Zusendung von Werbung war, die den Kläger in seinem allgemeinen Persönlichkeitsrecht verletzte.

Der BGH stellte fest, dass eine Zufriedenheitsnachfrage Werbung im Sinne des Art. 13 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) bzw. § 7 Abs. 2 Nr. 3 UWG ist. Dies sei auch dann der Fall, wenn sie zusammen mit einer Rechnung übersandt wird. Die Einwilligung des Nutzers ist folglich Voraussetzung für die Zulässigkeit der (Direkt-)Werbung.

Die Entscheidung des BGH ist richtig, da damit zu rechnen ist, dass sich derartige Fälle durch die Automatisierungsmöglichkeiten häufen werden. Daher überwiegt bei der in solchen Fällen durchzuführenden Interessenabwägung das Interesse des Nutzers, in Ruhe gelassen zu werden, das (wiewohl legitime) Werbeinteresse des Händlers.

Last Call für Zertifikate

Am 18.09.2018 erschien das Beta-Release von Chrome 70 – jener Version, die ihre Benutzer nun auch vor den letzten unter der Ägide von Symantec erstellten SSL-Zertifikaten der Marken VeriSign, Thawte, GeoTrust etc. warnt (vgl. SSN 09/2017). Wer noch ein solches „ranziges" Zertifikat einsetzt, sollte schleunigst ein frisches ordern, bevor Mitte Oktober das „stable" Release von Chrome 70 per Update die meisten Anwender erreicht.

Fortschritte bei Facebook

Am 05.06.2018 hat der Europäische Gerichtshof in seinem Urteil zu Facebook Fanpages die gemeinsame Verantwortung von Seitenbetreiber und Facebook für die Datenverarbeitung gegenüber den Nutzern festgestellt. Der Anforderung, eine Vereinbarung zur Verantwortungsabgrenzung nach Art. 26 Abs. 1 und 2 DSGVO vorzulegen, ist Facebook nun nachgekommen. Darin erkennt Facebook die Hauptverantwortung für die Verarbeitung der Nutzungsdaten bei den Seitenaufrufen an und bestimmt Facebook Ireland Ltd. als Verantwortlichen. Das schließt die Gewährleistung der Betroffenenrechte nach Art. 12 ff, 15 bis 22 DSGVO ein. Facebook erklärt sich auch für die Sicherheit der Verarbeitung zuständig (Art. 32 DSGVO). Die Vereinbarung knüpft an die Verwendung von Facebook Insight an. Seitenbetreiber, die im Anwendungsbereich der DSGVO agieren und denen Insight zur Verfügung steht, erkennen die Vereinbarung an. Für die Vereinbarung wird irisches Recht für anwendbar erklärt. Der Seitenbetreiber wird verpflichtet, Kontakte der Aufsichtsbehörden an Facebook zu melden. Für die Angabe einer Rechtsgrundlage seiner Datenverarbeitung, die Erfüllung der nicht näher bestimmten verbleibenden Datenschutzpflichten und die Benennung des Seitenverantwortlichen bleibt der Seitenbetreiber verantwortlich.

Mit der Vereinbarung geht Facebook einen großen Schritt Richtung Rechtssicherheit für Seitenbetreiber. Es ist jedoch noch zu klären, ob die Bestimmung irischen Rechts, die Beschränkung auf Insights-Daten ohne nähere Definition und die Herstellung von Transparenz rechtskonform sind und eine ausreichende Umsetzung darstellen. Für die Seitenbetreiber ist jedoch eine wesentliche Grundlage für die weitere Nutzung des Dienstes geschaffen.

Nicht nur Server soll man härten

Sicherheitsforscher von ESET stellten am 27.09.2018 in ihrem Blog Erkenntnisse über eine neue Art Rootkit vor. Konkret handelt es sich um eine Schadsoftware, die sich in der Firmware (*Unified Extensible Firmware Interface*, UEFI) ihrer Opfer einnistet und von dort ihr Unwesen treibt – unsichtbar für Virenscanner und Anwender.

Ein solch kleines und unscheinbares Rootkit führt uns vor, warum man bei der Härtung von Betriebssystemen nicht nur Server, sondern auch Client-Systeme im Blick haben sollte. Die einfache Aktivierung von *Secure Boot* verhindert zumindest bei diesem speziellen Rootkit eine Infektion. Und das Laden unsignierter Firmware-komponenten beim Systemstart sollte ohnehin generell auf Firmenrechnern verhindert werden.

Überwachungsvideo als Beweis

In einem von Bundesarbeitsgericht am 23.08.2018 entschiedenen Fall hatte ein Arbeitgeber seine Geschäftsräume (hier einem Tabak- und Zeitschriftenhandel mit angeschlossener Lottoannahmestelle) mit einer offenen Videoüberwachung

überwacht, um sein Eigentum vor Straftaten seiner Kunden und seiner Mitarbeiter zu schützen. Nachdem im 3. Quartal 2016 ein Fehlbestand an Tabakwaren festgestellt worden war, wertete der beklagte Arbeitgeber die Videoaufzeichnungen aus und stellte dabei fest, dass die klagende Arbeitnehmerin schon im Februar 2016 vereinnahmte Gelder nicht in die Registrierkasse gelegt hatte. Daraufhin kündigte der Arbeitgeber der Arbeitnehmerin fristlos. Gegen diese Kündigung erhob die Klägerin Kündigungsschutzklage.

Das BAG entschied (auch unter Berücksichtigung der DSGVO), dass, wenn eine offene, rechtmäßige Videoüberwachung stattfindet, die Videoaufzeichnungen als Beweis verwertet werden können. Arbeitgeber seien aufgrund des datenschutzrechtlichen Löschgebots nicht verpflichtet, Videoaufzeichnungen umgehend auszuwerten. Es sei rechtmäßig damit solange zu warten, bis es einen (berechtigten) Anlass zur Auswertung des Bildmaterials gab. Die Prüfung, ob eine rechtmäßige Videoüberwachung gegeben war, muss das Gericht treffen, an welches die Sache zurückverwiesen wurde.

Die Entscheidung des BAG ist vor allem deshalb Aufsehen erregend, weil daraus gefolgert werden kann, dass ein Verstoß gegen die datenschutzrechtlichen Löschregeln kein allgemeines Beweisverwertungsverbot nach sich zieht. Aus datenschutzrechtlicher Sicht bleibt es aber dabei, dass Daten aus einer Videoüberwachung nicht unbegrenzt lange gespeichert werden dürfen. Damit ist ein neues Spannungsfeld zwischen den Grundsätzen des Datenschutzes und den rechtlichen Konsequenzen in anderen Rechtsbereichen bei Datenschutz-Verstößen eröffnet.

Beschränkt einsatzfähig

Nachdem das *besondere elektronische Anwaltspostfach* (beA) Ende 2017 aus Sicherheitssicht eine Bruchlandung hinlegte, gelobten die Verantwortlichen Besserung. Nach der Erstellung eines Sicherheitsgutachtens und Behebung mehrerer festgestellter Schwachstellen ging die Anwendung am 03.09.2018 wieder in Betrieb. Nach wie vor begrenzen jedoch Designansätze die Sicherheit: Zwar erfolgt die Nachrichtenverschlüsselung auf dem Client, die eigentliche Anwendung wird jedoch als Web-Applikation von den Servern des Betreibers ausgeliefert und kommuniziert nur für die kryptografischen Operationen mit der Client-Security-Komponente des Anwenders. Ein Angreifer, der die Web-Anwendung kontrolliert, kann Betreff und Nachrichtentext einsehen sowie weitere Empfänger hinzufügen. Dies wurde im Gutachten als „betriebsverhindernd" eingestuft und sollte somit vor der Inbetriebnahme behoben werden.

Angesichts der nötigen umfangreichen Änderungen an der Anwendungsarchitektur wäre vermutlich eine planmäßige Inbetriebnahme nicht möglich gewesen. Die Bundesrechtsanwaltskammer entschied daher, die Priorität der Schwachstelle herabzustufen: Es sei keine Einsichtnahme in die Anhänge möglich und der Schutzbedarf der Nachrichten sei geringer einzuschätzen. Diese Einschätzung beruht allerdings auf der Annahme, dass Benutzer tatsächlich keine sensiblen Daten in Text oder Betreff integrieren. Besser wäre es gewesen, klarzustellen, dass die technische Lösung nur unter bestimmten Voraussetzungen sicher ist. Das Beispiel zeigt, warum Sicherheit in allen Phasen der Software-Entwicklung Beachtung finden sollte: Denn Fehler in der Anforderungs- oder Design-Phase lassen sich in der Implementierung kaum noch beheben.

Secorvo News

Secorvo@it-sa

Besuchen Sie uns vom 9. bis 11. Oktober auf der it-sa – Sie finden uns in Halle 10, Standnummer 10.1.-628. Am 09.10.2018 um 14:00 Uhr spricht Dirk Fox im Forum M10 – Management zum Thema DSMS – Datenschutz mit System.

Sie haben noch kein Ticket? Registrieren Sie sich mit unserem Gutscheincode **A398906** für ein kostenfreies Tagesticket.

Secorvo-Seminare

Ende Oktober findet bei Secorvo das Zertifizierungsseminar T.P.S.S.E. (**22.–25.10.2018**) statt, gefolgt im November von dem Seminar IT-Sicherheit heute (**20.–22.11.2018**) und der letzten Gelegenheit in diesem Jahr, sich als T.I.S.P. zu qualifizieren (**26.–30.11.2018**). Wir freuen uns, sie in unserem renovierten Seminarbereich begrüßen zu dürfen. Programme und Online-Anmeldung unter https://www.secorvo.de/seminare.

Verordnete IT-Sicherheit

Die MiRO – Mineralölraffinerie Oberrhein ist als Teil der kritischen Infrastruktur verpflichtet, die Anforderungen des § 8a IT-Sicherheitsgesetz zu erfüllen. Beim kommenden KA-IT-Si-Event am **08.11.2018** stellt Alessandro Wittig vor, wie die MiRO diese Herausforderung bewältigt hat, welche Vorteile sich daraus ergeben haben und wie der Nachweis gegenüber dem BSI erbracht wurde. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Wir freuen uns auf Ihre Teilnahme (Anmeldung).

Veranstaltungshinweise

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

Oktober 2018	
09.-11.10.	it-sa 2018 (NürnbergMesse GmbH, Nürnberg)
15.-19.10.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
15.-19.10.	ACM CCS 2018 (ACM/SIGSAC, Toronto/CA)
16.-18.10.	heise devSec 2018 (dpunkt.verlag, Heidelberg)
22.-25.10.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
23.10.	Anwendertag IT-Forensik (SIT, Darmstadt)
30.10.	Swiss Cyber Storm 2018 (Swiss Cyber Storm Association, Bern/CH)
November 2018	
06.-07.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-16.11.	42. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit e.V., Köln)
20.-21.11.	7. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
20.-22.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
26.-30.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.-30.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp, Friederike Schellhas-Mende.

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