secorvo
security consulting

Secorvo Security News

Dezember 2018

Es wird geschehen.

Seit Jahrzehnten verstehen wir Informationssicherheit in erster Linie als Prävention: Wir versuchen zu verhindern, dass etwas passiert, was nicht passieren soll.

Das ist nicht grundsätzlich falsch. Allerdings wachsen mit immer mehr Webanwendungen, IoT-Lösungen und Cloud-Angeboten die Zahl der angreifbaren Systeme, durch die zunehmende Abhängigkeit der Geschäftsprozesse das Schadenspotential und die Wahrscheinlichkeit, dass eine unentdeckte Schwachstelle eines Tages wirksam ausgenutzt wird.

Wir müssen daher davon ausgehen, dass Sicherheitsvorfälle passieren werden. Und uns darauf vorbereiten. Denn der Schaden entsteht nach dem Vorfall – und lässt sich in der Regel durch schnelles und richtiges Reagieren wenigstens begrenzen.

Genau darauf aber sind Unternehmen (Rechenzentren ausgenommen) meist schlecht vorbereitet. Wer verfügt denn über ein ernsthaft und regelmäßig erprobtes Notfallkonzept – nicht in der Schublade, sondern in den Köpfen der Mitarbeiter? Daher werden Sicherheitsvorfälle oft zum Desaster. Denn wo soll ein Unternehmen kurzfristig Hilfe suchen, wenn es keine Sicherheitsexperten im Haus hat? Wem kann es vertrauen – und wie wahrscheinlich ist es, dass sich kurzfristig ein geeigneter und verfügbarer Experte findet?

Diesem Problem rückt Baden-Württemberg nun mit einer Cyber-wehr zu Leibe: Eine zentrale Telefonnummer mit Erstberatung und einem lokalen Netzwerk von qualifizierten (und zukünftig zertifizierten) Notfallexperten, aus dem kurzfristig ein Team zusammengestellt werden kann, das hilft, den Schaden vor Ort einzudämmen.

Wenn das vom Innenministerium des Landes finanzierte Pilotprojekt, das Anfang 2019 auf alle IHK-Unternehmen der Region Karlsruhe ausgedehnt wird, erfolgreich sein sollte, könnte dies eine Blaupause für Deutschland werden. Die Chancen stehen jedenfalls besser als beim Ansatz des BSI vom Oktober 2016...

Inhalt

secorvo
security consulting

Security News

Der Diesel und der Datenschutz

Die Wellen des Diesel-Skandals haben nun auch den Datenschutz erreicht. Der Bundesrat hat in seiner Stellungnahme vom 14.12.2018 zu einer Änderung des Straßenverkehrsgesetzes erhebliche Bedenken zur verfassungsrechtlichen Zulässigkeit der vorgesehenen Verarbeitung personenbezogener Daten geäußert und den Entwurf abgelehnt.

Der Entwurf sieht zur Durchsetzung von Fahrverboten eine Befugnis zum automatisierten Abgleich von KfZ-Kennzeichen sämtlicher Fahrzeuge in der Verbotszone mit dem Zentralen Fahrzeugregister vor. Weitere verarbeitete Daten sind Bilder von Fahrzeug und Fahrer, die relevanten Fahrzeugmerkmale und Ort sowie Zeit der Verkehrsteilnahme. Die Erhebung darf bei Zielgefährdung sogar verdeckt erfolgen. Die Daten von berechtigten Fahrzeugen werden unverzüglich gelöscht, positive Abgleiche aber erst ab Versand an die zuständige Ordnungsbehörde oder nach sechs Monaten. Die dreimonatige Verjährungsfrist aus § 26 Abs. 3 StVG wird damit um das Doppelte überschritten.

Der Bundesrat beruft sich in seiner Ablehnung auf das Urteil des Bundesverfassungsgerichts zum Kennzeichen-Scannen, das klare Grenzen für Abgleichprozesse formuliert. Durch die lange Aufbewahrungsfrist bis zur Durchführung des Abgleichs und durch die umfasste dauerhafte, nicht nur stichprobenweise Erfassung seien diese überschritten.

Da die Überschreitungen behebbar sind und die Ablehnung das Gesetzgebungsverfahren nicht beendet, werden automatisierte Kontrollen und Kennzeichenerfassungen in den Innenstädten damit nicht vom Tisch sein.

Der Vorgang zeigt jedoch erneut, wie weit datenschutzrechtliche Gestaltungsanforderungen reichen.

Zwei-Faktor-Trojaner

Am 13.12.2018 veröffentlichte ESET einen Bericht über einen neuen Android-Trojaner, der die PayPal-Bezahlapplikation angreift. Wie so oft wird die Trojaner-App – getarnt als vermeintlich nützliche Anwendung – über den Store eines Drittanbieters installiert (und nicht über Googles offiziellen App-Store). Besonders ist, dass der Trojaner sich in die Anmeldung an PayPal einklinkt und der Angriff sogar – da es die „echte" Anmeldung an der Bezahl-App ist – funktioniert, wenn eine 2-Faktor-Authentisierung genutzt wird.

Daraus lernen wir: Ein zweiter Faktor allein erhöht die Sicherheit nicht – schließlich können wir mit Alkohol im Blut auch nicht dadurch sicherer Auto fahren, dass wir uns anschnallen. In unserem Fall bestünde eine vorsichtige „Fahrweise" darin, nicht einfach beliebige, vermeintlich nützliche Apps und erst recht nicht aus irgendwelchen Dritt-Stores zu installieren – unabhängig davon, ob man einen zweiten Faktor nutzt oder nicht.

Wer es wirksam sicherer haben möchte, dem sei empfohlen, aus dem zweiten Faktor einen unabhängigen zweiten Faktor zu machen – indem dieser auf einem separaten Gerät und nicht auf dem empfangen wird, auf dem die PayPal App läuft.

Der Schlüssel und die Fußmatte...

...kommen einem in den Sinn, wenn man die von zwei Forschern der Radboud University am 05.11.2018 veröffentlichte Studie Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs) liest. Die Autoren stellen darin ihre Untersuchung handelsüblicher selbstverschlüsselnder Festplatten vor und kommen zu dem erschreckenden Ergebnis, dass sich bei allen Produkten die Daten leicht entschlüsseln lassen. Für jedes der untersuchten Festplattenmodelle wird im Detail beschrieben, wie die Datenverschlüsselung mit wenig Aufwand rückgängig gemacht werden kann.

Für Microsoft war die Studie Anlass genug, bereits einen Tag später den Sicherheitshinweis ADV180028 zu veröffentlichen – denn Bitlocker ersetzt per Default, sofern möglich, die Softwareverschlüsselung durch eine von der Festplatte angebotene Hardwareverschlüsselung. Diese Bitlocker-Option sollte umgehend deaktiviert werden.

Facebook und der Datenschutz

Bereits am 26.09.2018 bestätigte der bayrische Verwaltungsgerichtshof mit einem nun veröffentlichten Beschluss die Untersagung der Nutzung von *Facebook Custom Audience*, sofern dem Werbetreibenden keine Einwilligung der Betroffenen vorliegt.

Mit *Custom Audience* bietet Facebook Werbekunden an, zur Schaltung von gezielten Werbekampagnen eine Liste mit Hashwerten von Kunden-E-Mail-Adressen zu übermitteln und Selektionskriterien wie Alter, Interessen und weitere Eigenschaften festzulegen. Facebook gleicht die erhaltenen Daten mit seinem Mitgliederstamm ab und spielt die Werbung bei den Facebook-Nutzern aus, bei denen die Kriterien zutreffen.

Das Bayerische Landesamt für Datenschutzaufsicht hatte im Januar 2018 einem Shop-Betreiber die Nutzung untersagt und die Übermittlung der Liste als Übermittlung gewertet. Diese Einschätzung teilt

der bayerische VGH: Eine Auftragsverarbeitung sei dies nicht, da Facebook die beworbenen Mitglieder selbständig auswähle und dem Auftraggeber keine Kontrolle möglich sei. Zwar erging die Entscheidung noch auf Grundlage des BDSG aF, sie ist jedoch in den Wertungen vollständig auf die DSGVO übertragbar. Da in der Übermittlung selbst bei Daten, die zu Werbezwecken genutzt werden dürften, eine Zweckänderung läge, fordert der VGH eine Einwilligung der betroffenen Facebook-Nutzer.

Ungeachtet der hinsichtlich Facebook bestehenden Transparenzbedenken und der Einzelentscheidung ziehen die Ausführungen des Gerichts einen sehr engen Rahmen für die Auftragsverarbeitung, wenn der Auftragnehmer nicht vollständig offengelegte, aber durch Anweisungen bestimmte Verarbeitungen vornimmt. Der Entscheidung kommt daher eine über den konkreten Dienst hinaus gehende Bedeutung zu.

Stille Kundenrückgewinnung

Aufgrund der unüberschaubaren Fülle an Apps haben wir als Smartphone-Nutzer die Qual der Wahl: Wir installieren und deinstallieren, wie es uns gefällt. Mit erfolgter App-Löschung sind auch alle Daten auf unserem Smartphone weg. Aber sind sie es auch beim App-Anbieter?

Am 22.10.2018 informierte Bloomberg über eine neue Methode, mittels welcher App-Anbieter durch so genannte *Silent Push Notifications* verlorene Kunden wiedergewinnen können. Bei diesen Datenpaketen handelt es sich um Remote-Mitteilungen, die im Hintergrund und ohne weitere Hinweise (z. B. Ton oder Symbol) erfolgen und bspw. Inhaltsaktualisierungen ermöglichen.

Das Vorgehen kommt jedoch auch für Marketing Zwecke zum Einsatz. Die *Notifications* dienen dabei als Basis für ein Tracking des Nutzerverhaltens. Bleiben die erwarteten Antworten auf die *Notifications* aus, wird die entsprechende App als gelöscht eingestuft. Die Verknüpfung von sog. „Deinstallations-Trackern“ mit dem eigenen Smartphone ermöglicht dann die Schaltung gezielter Werbung zur Kundenrückgewinnung. Solche Deinstallations-Tracker werden bspw. von Adjust oder CleverTap angeboten.

Betroffene Enduser können das Schalten von Werbung beschränken, indem das Ad-Tracking entsprechend eingeschränkt wird. Noch ungeklärt ist allerdings die Frage, ob dieses Vorgehen gegen Nutzungsbestimmungen bspw. von Apple oder Google verstößt.

Secorvo News

Secorvo Seminare

Wem noch ein Weihnachtsgeschenk für sein Team fehlt: Wie wäre es mit einer Weiterbildung für das Jahr 2019? Das Seminarangebot und die Termine unserer PKI-, T.I.S.P.- und T.P.S.S.E.-Seminare (alle ab März 2019) sowie die Möglichkeit zur Online-Anmeldung finden Sie – noch rechtzeitig vor der Bescherung – unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme…

Gut gehört und schon gehackt.

Oder: Wie Sennheiser das TLS-Protokoll aushebelte. Leser der Security News kennen die Hintergründe (SSN 10/2018): Ein klitzekleiner „Workaround“ der Entwickler wuchs sich zu einem Sicherheits-Desaster für alle betroffenen Systeme aus: Eine Design-Schwachstelle im Zertifikatsmanagement der Software Sennheiser HeadSetup unterhöhlte ohne Wissen der Nutzer die Sicherheit aller TLS-Verbindungen – für die Beseitigung der Schwachstelle war die Mitwirkung von Microsoft erforderlich. Dass ein solches Desaster überhaupt möglich war, hatte allerdings mehrere Ursachen, für die nicht ausschließlich Sennheiser verantwortlich gemacht werden sollte.

Beim Jahresauftakt-Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 21.02.2019 zeigen die Secorvo-Experten André Domnick und Hans-Joachim Knobloch, wie durch die Schwachstelle ein Man-in-the-Middle-Angriff auf TLS gelingt, stellen dar, gegen welche lang bekannten Design-Prinzipien für sichere Software verstoßen wurde und wie eine sichere Lösung hätte aussehen können. Abschließend betrachten sie einige zentrale Grundprinzipien, gegen die Entwickler nie verstoßen sollten – erst recht nicht bei der Nutzung von Zertifikats-basierten Sicherheitslösungen.

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

Veranstaltungshinweise

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

Januar 2019	
18.-20.01.	ShmooCon 2019 (The Shmoo Group, Washington/US)
21.-23.01.	Omnisecure 2019 (in TIME berlin, Berlin)
22.-25.01.	AppSec Cali 2019 (OWASP Foundation, California/USA)
Februar 2019	
06.-07.02.	26. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.02.	Gut gehört und schon gehackt. Oder: Wie Sennheiser das TLS-Protokoll killte. (KA-IT-Si, Karlsruhe)
März 2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Im August 2018 veröffentlichte das US Government Accountability Office einen Untersuchungsbericht zum Angriff auf den Finanzdienstleister Equifax, bei dem 2017 Daten von ca. 143 Mio. US-Bürgern kompromittiert wurden. Der Bericht veranschaulicht sehr gut, welche katastrophalen Folgen auch einfache Schwachstellen haben können...

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer.

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