secorvo
security consulting

Secorvo Security News

Januar 2018

Über Mittel und Zwecke

Er ist nicht nur einer meiner Lieblingsfilme, sondern er zählt zweifellos zu den Meisterwerken der Filmgeschichte: Hitchcocks „Das Fenster zum Hof“. Kürzlich konnte ich ihn das erste Mal im Kino bewundern – und war erneut fasziniert von den zahlreichen Parallelgeschichten, die er aus der Perspektive des Fotografen Jefferies (meisterhaft gespielt von James Stewart) erzählt. Der langweilt sich mit einem gebrochenen Bein in seinem New Yorker Apartment – und beobachtet die Nachbarn im Hinterhof durch sein Teleobjektiv. Dabei meint er, einem Mord auf die Spur gekommen zu sein und bittet seinen Freund Doyle von der Kriminalpolizei um Unterstützung. Nach dieser Szene sah ich den Film diesmal aus einer neuen Perspektive. Denn Doyle stellt seinem Freund zuliebe tatsächlich Ermittlungen an – allein auf der Grundlage vager Vermutungen. Erst als Jefferies ihn bittet, eine heimliche Wohnungsdurchsuchung vorzunehmen, erinnert sich Doyle an die rechtsstaatlichen Grenzen der Polizeiarbeit und verweigert seine Unterstützung – für Datenschützer eine Schlüsselszene. Wie vermutlich bei vielen Zuschauern stößt diese Haltung bei Jefferies auf Unverständnis: Schließlich ist für ihn die Sache klar, steht des von ihm Verdächtigten Schuld außer Frage.

Dabei geht es um eine große Errungenschaft des Rechtsstaats: die Unschuldsvermutung, die Beschränkung der Mittel der Strafverfolgung und eine Strafprozessordnung, die nicht der besseren Ahndung von Verbrechen dient, sondern nach Möglichkeit ausschließen soll, dass es zur Verurteilung von Unschuldigen kommt – und sei es um den Preis, einen Schuldigen davonkommen zu lassen. Diese Beschränkung in der Wahl der Mittel gilt es immer wieder aufs Neue zu verteidigen, damit sie nicht im Eifer der Verbrechensbekämpfung der Aufklärungsrate geopfert wird. Und da gibt eine kürzlich veröffentlichte Zahl zu denken: 310.000 stille SMS setzte der Verfassungsschutz 2017 zur Ortung von Mobilfunkteilnehmern ab. 44% mehr als 2016, 214% mehr als 2015. Sind wir da noch auf Kurs?

Inhalt

secorvo
security consulting

Security News

Bürgerrating

Bereits Ende 2017 berichteten verschiedene Online-medien über Chinas Pläne für ein *Social Credit System*. Das bereits im Aufbau befindliche System für einen Score-Wert aller Bürger kann als Beweis für die Berechtigung der Kernaussagen des vor über 30 Jahren ergangenen Volkszählungsurteils des Bundesverfassungsgerichts dienen. Das wegweisende Urteil, das viele Kernelemente des Datenschutzrechts auf den Punkt gebracht hat, warnt davor, dass ein Bürger, der die Erfassung und Auswertung seines Verhaltens nicht einschätzen kann, in seiner persönlichen Freiheit eingeschränkt wird, und dies auch die Wahrnehmung seiner demokratischen Rechte beschränkt. Chinas Pläne, anhand des Verhaltens auf Shopping-Plattformen, Social-Media-Plattformen und der Nutzung von Finanzdienstleistungen, aber auch anhand des Verhaltens vernetzter Freunde, für jeden seiner Bürger einen Score-Wert zu bilden, stellen die Umsetzung der schlimmsten Befürchtungen der damals urteilenden Richter dar.

Aus europäischer Sicht sollte hieraus ein starkes Argument für die bestehenden Datenschutzprinzipien, für Datensparsamkeit und Transparenz erwachsen. Doch das System zeigt auch, was sich bei vielen Nutzern sozialer Medien bereits abzeichnet: Mit dem Angebot zu erlangender Privilegien, Boni oder vereinfachten Zugängen bei „geeignetem" Score-Wert ist offenbar die Versuchung groß, trotz der offensichtlichen Verhaltenssanktionierung sogar freiwillig an der Bestimmung des Score-Werts teilzunehmen. Vor allem Kritiker des Datenschutzes wären gut beraten, die sich nun entwickelnden Szenarien genau zu beobachten.

HSMs jenseits der Donnerkuppel

„Zwei gehen rein, einer kommt raus" heißt es des Öfteren bei Firmenübernahmen wie derjenigen von Gemalto durch Thales, die am 17.12.2017 angekündigt wurde. Betroffen davon sind auch die beiden auf dem überschaubaren Markt für Hardware Security Module (HSMs) weit verbreiteten Produktreihen nShield/nCipher und Safenet/Luna, die ihrerseits durch vorherige Übernahmen im Portfolio der beiden Anbieter gelandet waren. Falls nicht noch die Kartellbehörden zur Auflage machen, eine der beiden Marken an einen Mitbewerber abzutreten, ist zu erwarten, dass Thales über kurz oder lang nur noch eine HSM-Produktreihe weiterführen wird.

Wer HSMs von Thales oder Gemalto z. B. für den Schutz von langlebigen CA-Schlüsseln einsetzt, sollte sich daher bald Gedanken über den langfristigen Support machen. Es wäre nicht das erste Mal, dass Sicherheitsforscher Nutzern helfen müssen, Schlüssel aus ihrem eigenen HSM zu hacken, um den Lieferanten (in diesem Fall: die Produktlinie) wechseln zu können.

WPA ... zum Dritten

Am 08.01.2018 kündigte die Wi-Fi Alliance an, im Laufe dieses Jahres einen neuen WLAN-Sicherheitsstandard WPA3 zu etablieren, der WPA und WPA2 ablösen soll. WPA3 soll in mindestens den folgenden vier Punkten Verbesserungen bringen:

- Eine nicht-authentifizierte Mindestverschlüsselung für bislang völlig offene WLAN-Netze wie öffentliche Hotspots
- Ein Verfahren für die WLAN-Security-Konfiguration von IoT-Geräten ohne eigenes Display (wohl ähnlich WPS, aber hoffentlich sicherer)
- Die bekannte Anfälligkeit von WPA2 Personal gegen Offline-Attacken auf schwache WLAN-Passwörter in einmal mitgeschnittenen Handshakes
- Zum Suite-B-Nachfolger CNSA kompatible Kryptoverfahren für „National Security Systems" in den USA

Genaue technische Details sind noch nicht bekannt, aber es darf vermutet werden, dass die Wi-Fi Alliance dieses Mal nicht direkt auf den IEEE 802.11 Standard zurückgreift, sondern u. a. auf RFC 7664 und RFC 8110.

Es lohnt wohl, evtl. geplante Investitionen in eine neue WLAN-Infrastruktur noch etwas zurück zu stellen, bis WPA3-fähige Geräte verfügbar sind – oder zumindest jetzt schon auf entsprechende Upgrade-Fähigkeit zu achten. Die Vorgänger WPA und WPA2 verbreiteten sich jeweils relativ zügig, wenn auch vor dem Hintergrund der Angriffe auf das bereits konzeptionell missratene WEP.

Komplexitätsklippen

Am 06.01.2018 veröffentlichten Paul Rösler, Christian Mainka und Jörg Schwenk von der Ruhr-Universität in Bochum eine vergleichende Untersuchung über die Sicherheit der Gruppen-Chats der verbreiteten Messenger-Dienste WhatsApp, Signal und Threema. Im Rahmen ihrer Analysen entdeckten die Autoren Schwachstellen in der Ende-zu-Ende-Verschlüsselung von Gruppen-Chats in WhatsApp und Signal, die einem Angreifer erlauben, unautorisiert beliebige Benutzer zu einer bestehenden Gruppe hinzuzufügen. Hierbei nutzen sie das Fehlen einer Authentisierung von *group management messages* aus. Diese Nachrichten werden an alle Gruppenmitglieder gesendet,

woraufhin diese einen Schlüsselaustausch mit dem neuen Mitglied durchführen.

Im Detail unterscheiden sich die Schwachstellen der beiden Messenger jedoch, sodass die Schwachstelle von WhatsApp als schwer wiegender einzustufen ist. Bei WhatsApp gibt es nur einzelne Administratoren, die berechtigt sind, neue Benutzer zu einer Gruppe hinzuzufügen. Hierfür laufen die Nachrichten über die zentralen Server von WhatsApp, um die Berechtigung der Benutzer zu prüfen. Eine Ende-zu-Ende-Verschlüsselung findet dabei nicht statt. Um die Schwachstelle auszunutzen, muss ein Angreifer einen WhatsApp-Server unter seiner Kontrolle haben und zusätzlich die komplexe ID des Chats kennen.

Beide Schwachstellen sind insgesamt diffizil und lassen sich in der Praxis wohl eher nicht ausnutzen, zumal die Nachricht, dass ein neuer Benutzer hinzugefügt wurde, weiterhin angezeigt wird. Dennoch zeigt die Analyse, wie komplex Ende-zu-Ende-Kommunikation in Gruppen sein kann. Gerade die Schnittstellen zwischen kryptografischen Protokollen und Management sind hierbei kritisch.

Big brother is watching

Der am 15.01.2018 in der Frankfurter Allgemeine erschienene Beitrag zu WeChat sollte aus Datenschutzsicht zu Vorsicht mahnen. Hinter der Entwicklung des Kurznachrichtendienst WeChat, der mittlerweile sehr viel mehr kann als Nachrichten auszutauschen und z. B. das Buchen von Reisen und Tickets, das Begleichen von Rechnungen, Arztterminvereinbarungen oder Geldtransfers ermöglicht, steht die chinesische Firma Tencent. Mittlerweile wird die App (überwiegend in China) von knapp einer Milliarde Menschen genutzt.

Durch die geografische Angebotserweiterung soll nun der Vorstoß in neue Weltmärkte gelingen. Seit 2017 ist die App auch aus Deutschland offiziell im App Store downloadbar. Obwohl die Messaging App von TrustArc (ehemals TRUSTe) zertifiziert ist und ein „Höchstmaß an Kontrolle über die Privatsphäre“ verspricht, raten wir – zumindest aus Datenschutzsicht – dringend vor einer Installation ab. Es sei denn, man möchte, dass alle Daten an den chinesischen Staat geliefert werden und diesem zur Datenauswertung zur Verfügung stehen.

Secorvo News

Weiterbildung 2018

Die Secorvo-Seminare starten in diesem Jahr mit einem Vorbereitungsseminar für sichere Softwareentwicklung und der Zertifizierung als T.P.S.S.E. (**12.–15.03.2018**), gefolgt von IT-Sicherheit heute (**20.–22.03.2018**). Im April bieten wir Ihnen die nächste Gelegenheit, sich als T.I.S.P. zu zertifizieren (**16.–20.04.2018**).

Die aktuellen Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

DSMSready2go

Eine der wichtigen Änderungen, die die europäische Datenschutz-Grundverordnung mit sich bringt, sind die erweiterten Dokumentationspflichten. Damit wird, davon sind wir überzeugt, der Datenschutz zukünftig den Aufbau von Managementsystemen erfordern, wie wir sie bereits aus der Informationssicherheit, insbesondere der ISO/IEC-Standard-Familie 2700x kennen.

Um diesen Prozess zu unterstützen hat Secorvo ein Datenschutz-Management-System auf der Grundlage eines Confluence CMS entwickelt, das Vorlagen, Prozesse, Richtlinien, Verfahrensverzeichnis und eine Methode zur Datenschutzfolgenabschätzung für die DSGVO-konforme Umsetzung des Datenschutzes in KMU bereitstellt – angelehnt an das erfolgreiche ISMSready2go. Nehmen Sie bei Interesse gerne Kontakt mit uns auf.

Who watches the watchmen?

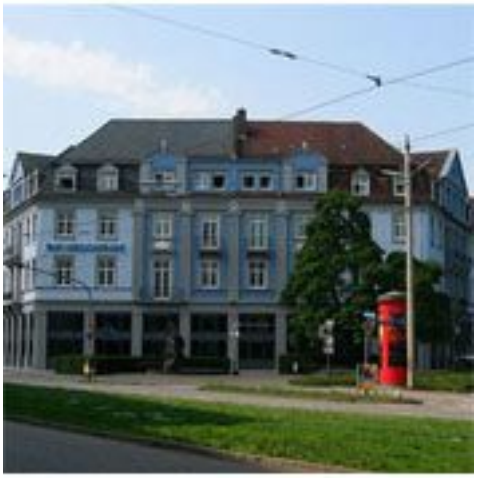
Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger“ zu machen. Doch was, wenn die Kontrolleure sich der Kontrolle entziehen – oder gar unkontrollierbar werden?

Zusammen mit dem ZAK (Zentrum für Angewandte Kulturwissenschaft und Studium Generale des KIT) lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg. Bei dieser Abschlussveranstaltung der Traumfabrik „BIG BROTHER – Surveillance Cinema“ wird der Film „THE CIRCLE“ von James Ponsoldt gezeigt. Die Einführung in den Film übernimmt Wolfgang Petroll, der bereits durch die gesamte Filmreihe führte. Im Anschluss an den Film findet eine Diskussion mit **Dr. Stefan Brink** (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), **Beate Bube** (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und **Thomas Rüttler** (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe) statt. Anschließend können Sie den Abend im persönlichen Austausch beim „Buffet-Networking“ ausklingen lassen (zur Anmeldung).

Veranstaltungshinweise

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

Februar 2018	
01.02.	Wie ich lernte, die Blockchain zu lieben (KA-IT-Si, Karlsruhe)
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.02.	Who watches the watchmen? (KA-IT-Si, Karlsruhe)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2018	
12.-15.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
20.-22.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/IT)
April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
16.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, 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

secorvo
security consulting

Secorvo Security News

Februar 2018

Des Kaisers neue Kleider

Keine Gazette, die etwas auf sich hält, konnte sich in den vergangenen 24 Monaten eines Beitrags zum Thema „Blockchain“ enthalten. „Disruptiv“, ja „revolutionär“ sei diese Technologie, kann man da lesen. Sie stelle ganze Wirtschaftszweige in Frage und ermögliche neue Geschäftsmodelle. Ein solches Wunderding mag man nicht unbeachtet vorbeiziehen lassen – und so stürzen sich allerorten große und größere Unternehmen darauf: Wer lässt sich schon gerne abschaffen? Also werden Kooperationen ausgerufen und Konzeptideen in die Welt gesetzt – und die Blockchain mutiert zum „Must have“: Wer jetzt noch nicht dabei ist, hat die Zukunft verspielt.

Unglücklicherweise ist das Blockchain-Konzept nicht so einfach zu verstehen; selbst Kryptologen ringen mit den Sicherheitsannahmen, die dem Verfahren zu Grunde liegen. Und so darf nicht verwundern, dass viele Beiträge nebulös bleiben – daher hat wohl auch der eine oder andere, der gerade neue Blockchain-Geschäftsideen herbeiträumt, nicht genau verstanden, wie das alles funktioniert. Details werden schließlich ohnehin meist überbewertet. Darum stieg das Vertrauen in die „Kryptowährung“ Bitcoin ins Unglaubliche – und machte das Konzept zur *self fulfilling prophecy*: Wenn alle vertrauen, dann ist das Verfahren sicherlich vertrauenswürdig…

So faszinierend die Ideen hinter der Blockchain, so schwer lassen sich Anwendungen jenseits von Bitcoin vorstellen, für die eine dezentrale, komplett transparente und aufwändig zu verifizierende Blockchain die richtige technische Umsetzung ist. Selbst für ein Zahlungssystem ist Bitcoin nur eingeschränkt geeignet: Transaktionen dauern lange, die Verifikation ist aufwändig und die dezentral zu speichernde Transaktionskette wird immer größer. Schließlich darf man seinen geheimen Schlüssel nicht verlieren, sonst ist das Vermögen futsch.

Für die Bitcoin- und Blockchain-Investoren bleibt daher zu hoffen, dass so schnell niemand „Der König ist ja nackt!“ ruft.

Inhalt

Security News

Hack & Mine

Der sinkende Tauschwert der Krypto-Währung Bitcoin motiviert derzeit neue Geschäftsideen: Wenn die Kosten für Strom und Rechnerinfrastruktur bei der rechenintensiven Prüfung der Transaktionen der Bitcoin-Blockchain (derzeit jährlich ca. 52,48 TWh, etwa 800 kWh pro Transaktion) den Wert der dabei „geschürften" Bitcoin übersteigen, liegt es nahe, die Kosten zu „externalisieren" – sprich: sich den Zugang zu leistungsfähigen Rechnernetzen zu verschaffen und diese im Auftrag schürfen zu lassen. Bereits in den SSN 10/2017 haben wir vor Drive-By-Minern gewarnt. Inzwischen kommt es vermehrt zu gezielten Angriffen auf Rechenzentren, um deren Rechenleistung in Bitcoins zu transferieren. So wurde am 08.01.2018 öffentlich, dass das Landesamt für Besoldung und Versorgung Baden-Württemberg Opfer von „Cryptojacking" geworden war, am 12.02.2018 wurde vom Missbrauch eines europäischen Wasserwerks berichtet und offenbar erwischte es auch Tesla, wie am 21.02.2018 bekannt wurde.

Zwar entsteht durch die Kryptowährungen kein neuer Angriffsvektor – wohl aber eine neue Motivation, da sich beim Cryptojacking ein erfolgreicher Angriff unmittelbar in (un)bares Geld verwandeln lässt.

Hidden Champions & Risks

Als zu Beginn dieses Jahres die Meltdown-Sicherheitslücke bei Intel-x86-Prozessoren die Schlagzeilen beherrschte, war den meisten Anwendern weltweit klar, dass es dabei um die Sicherheit ihrer PCs ging. Schließlich hatte Intel über die Jahre mit etlichen Marketing-Millionen das „Intel Inside" Warenzeichen im Bewusstsein der Käufer verankert. Auch dass und wofür man sich den monatlichen Patch-Tuesdays des Windows Update Zyklus anschließen sollte, ist bei fast allen IT-Profis und vielen Durchschnittsbürgern längst angekommen.

Aber wer kennt – selbst unter IT-Fachleuten – beispielsweise Kalignite von der schottischen Softwarefirma KAL oder ForeSite von Orpak Systems Ltd. in Israel? Erstere ist eine Anwendungsplattform für Windows, die die Geldautomaten von 40 verschiedenen Herstellern in 80 Ländern antreibt. Letztere ist eine Software, die den Betrieb von 35.000 Tankstellen auf vier Kontinenten automatisiert. Und neben der weiten Verbreitung haben beide Systeme noch eines gemeinsam: Am 11.01. bzw. am 31.01.2018 wurde gemeldet, dass sie Schwachstellen enthalten, die in einem Fall bereits nachweisbar, in anderen potenziell von Kriminellen ausgenutzt werden und jeweils signifikante Teile einer ganzen Branche betreffen können.

Die Gefahr von „Monokulturen" bei Prozessoren und Betriebssystemen ist bekannt. Daneben bergen aber gerade die weniger augenfälligen „Hidden Champions" unter den Branchenanwendungen ein hohes Flächenrisiko, das dank der Goldgräberstimmung in den Buzzword-Themen Digitalisierung, IoT und Industrie 4.0 in nächster Zeit weiter zunehmen wird.

Da wäre es keine schlechte Idee für das im Koalitionsvertrag avisierte IT-Sicherheitsgesetz 2.0, die Prozesse für sichere Softwareentwicklung, Schwachstellensuche und -behebung bei marktbeherrschender Fachanwendungs-Software in kritischen Bereichen unter die Lupe zu nehmen – und zu regulieren.

Tot & lebendig

Der Entwickler der Bibliothek go-bindata hatte vor einiger Zeit seinen GitHub-Account gelöscht. Am 07.02.2018 tauchte der Account erneut mit dem gleichen Namen auf – denn der Benutzername eines gelöschten GitHub-Accounts kann unmittelbar danach wieder benutzt werden. Über diesen Mechanismus könnte ein Angreifer ein gefälschtes Repository einrichten und eine trojanisierte Version einer bekannten (Open Source) Software verbreiten. Darüber kann ein Angreifer beliebigen Code auf Systemen auszuführen, die eine Bibliothek aus dem (übernommenen) Repository beziehen.

Besondere Brisanz erlangt diese Schwachstelle dadurch, dass diverse Anwendungen und sogar Paketmanager mit namensbezogenen URLs auf GitHub-Repositories arbeiten. Für den Anwender sind solche Zusammenhänge jedoch bestenfalls erst mit einem zweiten, intensiveren Blick erkennbar.

GitHub prüft derzeit noch intern, ob ehemals verwendete Benutzernamen permanent oder temporär gesperrt werden sollen. Andere Anbieter wie Google setzen dies bereits seit langer Zeit um. Manchen wie beispielsweise Twitter wurden derartige Probleme in der Vergangenheit ebenfalls zum Verhängnis. Entwickler, die ihr kostenpflichtiges Konto nicht weiter benutzen möchten, sollten es nicht löschen sondern auf einen kostenlosen Account herunterstufen.

Die Prüfung auf Schwachstellen bei der Account-Löschung ist gängiger Bestandteil eines Penetrationstests einer Anwendung. Dies findet sich sogar in Prüfkatalogen wie dem OWASP Testing Guide. Neu ist diese Problematik also keinesfalls.

Zertifikate & Kleingedrucktes

Am 28.02.2018 erhielten ca. 23.000 Kunden des Zertifikats-Resellers Trustico eine E-Mail-Nachricht über die unmittelbar bevorstehende Sperrung ihres Webserver-Zertifikats aufgrund einer gemeldeten Kompromittierung des zugehörigen privaten Schlüssels. Hintergrund dieser Massen-Rückrufaktion war kein Cyberangriff, sondern ein bizarrer Vertragsstreit zweier Unternehmen, deren Geschäftsgrundlage eigentlich das Vertrauen in ihre sorgfältige und regelkonforme Arbeitsweise darstellt.

Trustico wollte nach der nicht ganz freiwilligen Übergabe des Trustcenter-Geschäfts von Symantec an DigiCert (vgl. SSN 09/2017) die Bezugsquelle wechseln, kündigte den bestehenden Reseller-Vertrag und schloss einen neuen mit Mitbewerber Comodo ab. Soweit noch ganz normale unternehmerische Handlungsweise. Offenbar wollte man aber kurzfristig auch die Zertifikate des Kundenbestands gegen solche des neuen Partners wechseln und dazu die vorhandenen Zertifikate der DigiCert-Marken sperren lassen. Da nach den Baseline Requirements (BR) des CA/Browser-Forums (Abschnitt 4.9.1.1) ein Vertragswechsel jedoch kein zulässiger Sperrgrund ist, verweigerte DigiCert dies solange, bis Trustico seiner Bitte offenbar 23.000 geheime Kundenschlüssel beifügte: Damit war ein Sperrgrund nach Abschnitt 4.9.1.1 Nr. 3 gegeben – Anzeichen für eine Kompromittierung privater Schlüssel.

Offenbar hat Trustico nicht nur – nach BR zulässig (!) – private Keys stellvertretend für Kunden erzeugt, sondern diese auch archiviert. Auch dies wäre zulässig, jedoch nur mit Einwilligung des Kunden (BR Abschnitt 6.1.2), die eventuell beim (Über-)Lesen der AGB erteilt wurde. Spätestens jedoch mit der Weitergabe hat Trustico wohl gegen die BR verstoßen – besonders pikant, da das Unternehmen auch selbst als CA auftritt. Die Lehre für Zertifikatskäufer: Das Vertrauen in einen Anbieter sollte man nicht nur am Preis festmachen, sondern u a. auch daran, wie klar und verständlich das „Kleingedruckte" präsentiert wird.

Hilfe & Selbsthilfe

Die Datenschutz-Grundverordnung (DSGVO) nimmt die Datenschutz-Aufsichtsbehörden in die Pflicht, insbesondere für kleine und mittelständige Unternehmen Praxishilfen für die Umsetzung der DSGVO zu entwickeln und zu veröffentlichen.

Dem ist die Bundesdatenschutzbeauftragte am 11.01.2018 mit der Veröffentlichung von Kurzpapieren nachgekommen, die von der Datenschutzkonferenz (dem ehemaligen „Düsseldorfer Kreis" der Aufsichtsbehörden des Bundes und der Länder) entwickelt und verabschiedet wurden. Darunter finden sich Erläuterungen beispielsweise zum Verzeichnis der Verarbeitungstätigkeiten, der Nutzung personenbezogener Daten für Werbezwecke, der Datenschutz-Folgenabschätzung oder dem Recht auf Löschung.

Die Nutzung dieser Kurzpapiere ist auch schon deshalb anzuraten, weil die Aufsichtsbehörden darin zugleich ihre Erwartungen an die Umsetzung der DSGVO konkretisieren.

Secorvo News

Das Netz, die Kaffeemaschine & unsere Fehler

Bei der Vernetzung der Produkte und Produktionsmaschinen tappen die Hersteller derzeit in die gleichen Fallen wie bei der Vernetzung der Computer „damals". Ob in Großindustrieanlagen, im Auto, im Stromzähler oder im trauten Heim: Überall sind inzwischen Computer eingebaut. Damit kaufen wir uns ein, dass diese Systeme nun dieselben Schwachstellen besitzen wie unsere PCs. Laptops, Smartphones und Tablets. Das Ergebnis: Industrieanlagen können via Internet herunter gefahren werden, unsere Autos lassen sich von Fremden öffnen, Stromzähler plaudern unsere Verbrauchswerte aus und der Staubsauger streamt Live-Videos aus unserem Wohnzimmer.

Dabei sind diese Schwachstellen alle vermeidbar: Angriffspunkte und auch die Schutzmaßnahmen sind meist bekannt – nur nicht an der richtigen Stelle.

Am Beispiel einer App-gesteuerten Kaffeemaschine wird Klaus J. Müller (Leitwerk AG) beim kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **15.03.2018** zeigen, was schief laufen kann und wie Sie die typischen Fallstricke vermeiden können. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Wissensaktualisierung

Im März startet die Secorvo-Seminar-Saison mit einem Vorbereitungsseminar für sichere Softwareentwicklung und der Zertifizierung als T.P.S.S.E. (**12.–15.03.2018**). Und im April bieten wir Ihnen die nächste Möglichkeit, sich als T.I.S.P. zu zertifizieren (**16.–20.04.2018**), danach erneut im Juni (**11.–15.06.2018**).

Die aktuellen Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Veranstaltungshinweise

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

März 2018	
12.-15.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
15.03.	Das Netz, die Kaffeemaschine und unsere Fehler (KA-IT-Si, Karlsruhe)
20.-21.03.	a-i3/BSI-Symposium 2018 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/I)
April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
12.-13.04.	11. GDD-Fachtagung Datenschutz international (Gesellschaft für Datenschutz und Datensicherung, Berlin)
19.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
25.-26.04.	BvD Verbandstag 2018 (BvD e.V., Berlin)
25.-27.04.	Sicherheit 2018 (Gesellschaft für Informatik e.V., Fachbereich Sicherheit, Konstanz)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)

Impressum

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

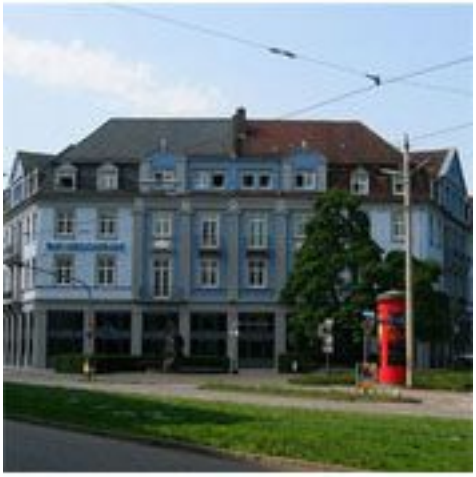
ISSN 1613-4311

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

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



secorvo
security consulting

Secorvo Security News

März 2018

Der Kern des Problems

Werbung hat Streuverluste. Niemand hat das so treffend auf den Punkt gebracht wie *Henry Ford* (1863-1947) in dem ihm zugeschriebenen Bonmot: „Ich weiß, die Hälfte meiner Werbung ist hinausgeworfenes Geld. Ich weiß nur nicht, welche."

Folgerichtig ist eines der zentralen Ziele im Marketing, diese Verluste zu reduzieren. Das gelingt allerdings nur, wenn der Werber möglichst präzise weiß, *wen* er erreichen muss und *wie* er diese Zielgruppe wirksam anspricht.

In beiderlei Hinsicht ist das Internet der Heilige Gral. Denn anders als bei einer Zeitschriftenanzeige, einer Plakatwerbung oder einem TV-Spot weiß jede Webseite, wer sie gerade besucht – und kann die zum Besucher passende Werbung einblenden.

Und zugleich, noch wertvoller, ist „im Netz" weit mehr über den Besucher bekannt, als anonyme Zuschauer- oder Leserbefragungen verraten – obendrein personalisiert. Dabei sind es sind nicht die „klassischen" personenbezogenen Daten wie Name, Geburtsdatum oder E-Mail-Adresse, die den eigentlichen Wert darstellen, sondern von vielen Betroffenen als wenig relevant eingestufte „Meta-Informationen": Zu welchen Zeiten wurden welche Seiten besucht? Welche Personen werden wie oft kontaktiert? Wie oft wurde wann nach was gesucht? Diese vermeintlich harmlosen Daten entblößen jedoch mit zunehmender Internet-Nutzung nahezu alles: die tatsächlichen Interessen (Suchziele), typische Verhaltensmuster (Nutzungszeiten, Verweildauern und Standortverläufe), Neigungen (Kontaktintensität) bis hin zur sexuellen Orientierung – und bei automatischer Auswertung von Nachrichteninhalten auch die persönlichsten Überzeugungen. Und mit jeder neuen App werden es mehr.

Ihre Analyse zielt dabei nicht auf Überwachung. Sondern darauf, die Unterschiede zu finden – bis zur Vorhersage des Verhaltens. Anders formuliert: Sie will die Persönlichkeit. Und genau deshalb ist nicht der Datenmissbrauch das Problem. Sondern diese Daten selbst.

Inhalt

secorvo
security consulting

Security News

Illegalisierte Blockchain

Wie in den SSN 2/2018 thematisiert, hat wohl nicht jeder, der die Blockchain als Lösung verschiedenster Probleme propagiert, das Konzept und seine Eigenschaften komplett durchdrungen. Einige „Nutzer" scheinen aber zumindest ein wesentliches Feature erfasst zu haben: Etwas, das einmal gültig in der Blockchain verzeichnet ist, kann nie wieder daraus verschwinden, allenfalls mit einem späteren Eintrag wieder rückabgewickelt werden.

Am 12.03.2018 veröffentlichten Forscher aus Frankfurt und Aachen eine Untersuchung von Dateninhalten, die bei vergangenen Transaktionen unauslöschlich in die Bitcoin-Blockchain aufgenommen wurden. Unter knapp 150 auffindbaren Bild-Dateien ist auch eine, die mutmaßlich den Tatbestand der Kinderpornographie erfüllt; dazu kommen mehrere Dutzend Links zu entsprechendem Material im sogenannten Darknet.

Damit sind die Beschaffung und der Besitz einer Kopie der kompletten Bitcoin-Blockchain, wie sie für das Bitcoin-Mining grundsätzlich erforderlich ist, in Deutschland und vielen anderen Ländern vermutlich illegal – ganz unabhängig vom rechtlichen Status der Bitcoin als Zahlungsmittel.

Man in the ISP

Citizen Lab beschreibt in einer Veröffentlichung vom 09.03.2018, wie die Internet Service Provider (ISP) Türk Telekom und Telecom Egypt Deep-Packet-Inspection-Technologien (DPI) nutzen, um ihren Kunden Schadsoftware oder Krypto-Miner unterzuschieben. DPI erlaubt es, nicht nur Metadaten von Datenpaketen zu durchsuchen, sondern auch deren Inhalte. Diese Möglichkeit wurde vor allem zur Erkennung und Filterung von Schadsoftware und Spam im Netzwerkverkehr entwickelt, lässt sich jedoch auch für Zensur und Einschränkung der Netzneutralität nutzen.

Offenbar werden von Türk Telekom unverschlüsselte Programmdownloads bekannter Programme wie VLC, Skype oder Opera mit einer Schadsoftware infiziert, die es erlaubt, die Computer der Benutzer auszuspähen. In Ägypten werden Teile des Verkehrs auf Affiliate-Programme und Krypto-Miner geleitet, um zusätzliche Einnahmen zu generieren.

Auch der Download von Programmen sollte wie jede andere sensible Kommunikation über einen TLS geschützten Kanal stattfinden. Mechanismen wie HSTS verhindern dabei ungewollte Downgrades auf HTTP. Manipulationsangriffe muss man dabei offenbar nicht mehr nur bei offenen WLANs unbekannter Anbieter befürchten, sondern sollte auch besser Providern keinen Vertrauensvorschuss mehr gewähren. Leider gibt es noch immer zahlreiche Softwareanbieter und andere Hersteller, die ihre Downloads unverschlüsselt bereitstellen.

Darf's ein bisschen mehr sein?

Weltweit gültige TLS-Serverzertifikate bekommt man nach den Richtlinien des CA/Browser-Forums in den Geschmacksrichtungen DV, OV und EV. Die EV (Extended Validation) Zertifikate enthalten über den oder die Servernamen hinaus weitere Angaben zum dahinter stehenden Unternehmen. In einem für Antragsteller und Trustcenter gleichermaßen aufwändigen Validierungsprozess wird sichergestellt, dass alle enthaltenen Angaben korrekt sind, das Unternehmen die fragliche Internet-Domain besitzt und die Erstellung des Zertifikats auch tatsächlich veranlasst hat. EV-Zertifikate werden eingesetzt, wo dies regulatorisch verlangt ist, bspw. beim Online-Banking, oder wo immer der Serverbetreiber Wert auf den „grünen Balken" legt, mit dem Browser besondere Vertrauenswürdigkeit anzeigen.

OV (Organization Validation) Zertifikate vereinen die Nachteile der beiden anderen Typen: Bei der Ausstellung werden zwar ähnlich wie bei EV Angaben zum Unternehmen geprüft, vom Browser wird jedoch kein Unterschied zu DV-Zertifikaten angezeigt.

Bei der einfachsten Kategorie, den DV (Domain Validation) Zertifikaten, wird vor der Ausstellung lediglich geprüft, ob der Antragsteller Kontrolle über die Internet-Domain hat, in der der zu zertifizierende Servername liegt. Dieser Check ist gut automatisierbar. Genau das macht sich die gemeinnützige CA Let's Encrypt zunutze, die kostenfrei DV-Zertifikate ausstellt.

Am 13.0.3.2018 aktivierte Let's Encrypt ACMEv2, die neue Version ihres Protokolls zum automatischen Zertifikatsbezug. Damit sind nun auch Wildcard-DV-Zertifikate für alle Server einer bestimmten Subdomain kostenfrei erhältlich.

Seither gibt es kaum noch Gründe, bei einem kommerziellen Trustcenter zu kaufen, wenn es kein EV-Zertifikat sein soll. Interne Serverzertifikate der eigenen PKI kann jedoch auch Let's Encrypt nicht komplett ersetzen – rein intern genutzte Server- bzw. Domain-Namen oder IP-Adressen sind für öffentliche DV-Zertifikate tabu.

Schwachstellensuche bei LTE

Am 06.03.2018 veröffentlichten Forscher der Universitäten Purdue und Iowa Details zu dem von ihnen entwickelten Tool LTEInspector. Ähnlich wie der bekannte IMSI-Catcher zu GSM-Zeiten setzt sich

dieses Tool als Emulation eines Access Points und eines Endgeräts zwischen LTE-Endgerät und Providernetz und erlaubt es, Analysemethoden für Kryptoprotokolle automatisiert auf reale LTE-Netze anzuwenden. Damit wurden auch gleich zehn neue und neun bereits bekannte Angriffe gegen den LTE-Verbindungsaufbau (wieder-)entdeckt und in echten LTE-Netzen durchgespielt.

So hoch der Wert des Tools für Analyse und Validierung von Sicherheitsprotokollen einzuschätzen ist, muss man doch die Tragweite der Schwachstellen relativieren. Ein Angreifer muss sich in Funkreichweite des Opfers befinden: Dadurch sind bspw. eine grobe Lokalisation des Opfers und die Möglichkeit, dessen Funknetz-Aktivitäten zeitlich zu erfassen, auch ohne elaborierten Protokollangriff gegeben. Auch ein Denial-of-Service wäre protokollunabhängig durch einen Störsender möglich.

Einer der Angriffe erlaubt, unautorisiert für Erdbeben oder Tsunamis gedachte Warnmeldungen abzusetzen. Dies scheint im Sinne einer Risikoabwägung plausibel – dass Sicherheitshürden im Katastrophenfall fatal sein könnten, hat sich u. a. bei der verzögerten Entwarnung nach dem Raketen-Fehlalarm auf Hawaii im Januar bestätigt.

Verblüffend ist, dass bei einem großen US-Provider unverschlüsselte LTE-Verbindungen möglich waren. Warum Handys nicht – wie jeder WWW-Browser – dem Anwender den Verschlüsselungsstatus seiner Verbindung anzeigen, bleibt nach wie vor ein Rätsel.

Orientierungspunkte

Die Art. 29 Gruppe beschloss am 06.02.2018 eine Reihe neuer Orientierungshilfen zur DSGVO. Mehrere beziehen sich auf den Datenverkehr mit Drittstaaten, u. a. mit Bezug die einschlägige EuGH-Rechtsprechung und Art. 44 ff DSGVO. Sie beschäftigen sich mit der Feststellung eines angemessenen Datenschutzniveaus (WP 254 rv.01), den Ausnahmeregelungen des Art. 49 (WP261/262) und mit den notwendigen Elementen von *Corporate Binding Rules* (BCR, WP 257 rev.01). Zur Feststellung des angemessenen Datenschutzniveaus sei nur die Umsetzung der Kerninhalte der Europäischen Gesetzgebung zu prüfen; dabei wird jedoch sehr weitgehend auf die bestehenden Instrumente wie Zweckbindung, Betroffenenrechte und Transparenz zurückgegriffen. Daneben werden eine unabhängige Aufsicht und eine wirkungsvolle Beschränkung staatlicher Eingriffsbefugnisse gefordert. Die Ausführungen zu BCR umfassen eine Tabelle mit kommentierten Inhaltsanforderungen, darunter direkte Ansprüche des Betroffenen als Drittbegünstigtem. Der Art. 49 schließlich sei als Ausnahmeregelung zu verstehen und sehr eng auszulegen.

Weiter passte die Art. 29 Gruppe die Richtlinien zur Meldung von Datenschutzvorfällen (WP250rev.01), zu automatisierten Einzelentscheidungen (WP251-rev.01) und zur Bußgeldbemessung (WP253) an.

WP250 setzt sich umfangreich mit dem Zusammenspiel von Auftragsverarbeiter und Verantwortlichem, dem Meldeinhalt und dem Ablauf zur Vorfallsklärung auseinander. Am Ende steht eine Liste mit Beispielvorfällen. Eine Meldung wird regelmäßig innerhalb von drei Tagen erwartet; Prozesse zur technischen Vorfallserkennung und –untersuchung werden nach Art. 32 DSGVO vorausgesetzt.

WP251 zu automatisierten Einzelfallentscheidungen fasst in einer Liste am Ende konkrete Umsetzungsanforderungen als *best practice* zusammen. Das Papier zur Bußgeldfestsetzung (bereits vom Oktober 2017) enthält zahlreiche Bemessungskriterien, eine sehr weite, Art. 4 Nr. 19 DSGVO ignorierende Unternehmensdefinition zur Erfassung ganzer Konzerne, allerdings keine konkreten beispielhaften Bemessungen. Intensiv diskutiert werden jedoch alternative Maßnahmen wie Verwarnungen.

Insgesamt tragen die Orientierungshilfen dazu bei, das künftige Vorgehen der Aufsichtsbehörden besser einschätzen zu können. Teilweise tendieren die Papiere allerdings zu einer eher restriktiven Auslegung der einzelnen Bestimmungen.

Secorvo News

Für Kurzentschlossene

Noch wenige freie Plätze können wir für unser nächstes T.I.S.P.- (**16.–20.04.2018**) und das PKI-Seminar (**23.–26.04.2018**) anbieten. Programme, weitere Termine und Online-Anmeldung unter https://www.secorvo.de/seminare

Sesam, öffne Dich – nicht.

Dass der Betreiber der hausinternen IT gerne eigenständig kontrolliert, was in seinem Rechenzentrum vorgeht und wie die dortigen Betriebsbedingungen sind, ist bekannt. Doch um das Ziel einer möglichst hohen Verfügbarkeit zu erreichen, muss auch immer der Gefahrenfaktor Mensch betrachtet werden. Bei unserem kommenden KA-IT-Si-Event am **12.04.2018** werden Ihnen von Fabian Schäfer (Rittal) an Anwendungsbeispielen die technischen Einsatzmöglichkeiten automatisierter Zutrittskontrollsysteme im IT-Umfeld vorgestellt.

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

Veranstaltungshinweise

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

April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
19.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
25.-27.04.	GI SICHERHEIT 2018 (Gesellschaft für Informatik e.V., Konstanz)
25.-26.04.	BvD Verbandstage 2018 (BvD e.V., Berlin)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)
Mai 2018	
02.-03.05.	Security Forum 2018 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
07.-09.05.	11th International Conference on IT Security Incident Management & IT Forensics (GI, SIDAR, DFN-Cert, Hamburg)
15.-18.05.	European Identity & Cloud Conference 2018 (KuppingerCole Ltd., München)
16.-18.05.	19. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)

Impressum

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

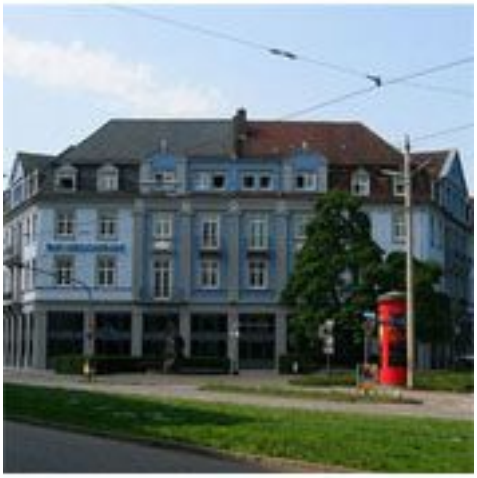
ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, 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



secorvo
security consulting

Secorvo Security News

April/Mai 2018

Der Spion, den ich liebe

Tim Berners-Lees Vision des World Wide Web war die eines freien Informationszugangs und der virtuellen Zusammenarbeit. Aber schon Mitte der 90er Jahre änderte sich der Charakter des WWW: Zwischen die Informationsquellen mischten sich die ersten Shops, die neben Besuchsdaten (IP-Adresse, Herkunft, Verweildauer) auch Kontaktdaten (Adresse, Kreditkartendaten oder die Bankverbindung) erfragten und Käuferprofile erstellten. Seither fordern immer mehr Dienste Daten, wie Sport-Coaches, Tourenplaner oder Gesundheitsberater. Dank Social Networks werden sie immer persönlicher: Fotos, Lebensläufe und Chatinhalte landen nun auch im Netz. Mit Smartphones wurden die Dienste mobil und werten jetzt auch Ortsinformationen aus, und inzwischen liefert das Internet of Things (IoT) Daten unserer smarten Fahrzeuge (Geschwindigkeit, Fahrverhalten) und smarten Homes (Kameraaufzeichnungen, Stromverbrauch, Steuerbefehle).

Was noch fehlte, war die Sprache. Nur auf den ersten Blick sind Alexa, Siri und Cortana lediglich eine Sprachsteuerung. Denn die Internet- und KI-basierten Sprachdienste funktionieren nur, wenn sie viel über uns wissen – unseren Geschmack, unsere Gewohnheiten und unseren Haushalt kennen. Und hemmungsbefreit beginnen wir, ihnen bereitwillig so viel wie möglich mitzuteilen: welche Musik wir präferieren, über welche Steckdose die Kaffeemaschine angeschaltet werden kann und wann wir das Haus verlassen oder betreten. Wir machen unsere Stimme, unsere Wünsche, unseren Tagesablauf, unsere Vorlieben, unseren Geschmack und sogar die Stimmen unserer Gäste zugänglich – weil wir möchten, dass Alexa & Co. verstehen, was wir wollen: Dass der Morgenkaffee fertig ist, wenn Alexa uns weckt und die Wohnung beleuchtet ist, wenn wir nach Hause kommen.

Und wenn sie das erste Mal das Badezimmer vorheizt, bevor wir selbst wissen, dass wir gleich ein Bad nehmen wollen, werden wir sie wirklich lieben.

Inhalt

secorvo
security consulting

Security News

Netflix schnorren mit Gmail

Ein schönes Beispiel, wie durch die Kombination zweier unabhängiger Internet-Dienste eine neue Angriffsmöglichkeit entsteht, beschreibt James Fischer in seinem Blogeintrag vom 07.04.2018: Warum Punkte in E-Mail-Adressen wichtig sind ("dots do matter"). Hintergrund ist, dass Googles Gmail-Dienst die Punkte in E-Mail-Adressen nicht auswertet – james.hfisher@gmail.com wird also genauso behandelt wie jameshfisher@gmail.com. Eine Ergonomiefunktion.

Dies kann bei der Netflix-Registrierung ausgenutzt werden. Durch einen Rateangriff lässt sich feststellen, ob für eine Gmail-Adresse bereits ein Konto existiert. Da Netflix die Punkte in der E-Mail-Adresse auswertet, kann ein zweiter Netflix-Account zu einem existierenden angelegt werden, indem bei der E-Mail-Adresse die Punkte verwendet respektive weggelassen werden. Die E-Mail-Adresse wird nicht überprüft, eine weitere Ergonomiefunktion: Warum auch, schließlich ist die Nutzung für vier Wochen kostenfrei. Die E-Mail-Adresse wird nur zur Benachrichtigung z. B. über neue Serien verwendet.

Was passiert aber, wenn man für das künstlich geschaffene Zweitkonto eine Kreditkarte mit sehr kurzer Laufzeit hinterlegt? Dann wird jameshfisher@gmail.com benachrichtigt, seine Kreditkartendaten zu aktualisieren. Die Nachricht geht, Google-intern, an james.hfisher@gmail.com. Kommt von Netflix, ist original Netflix. Wenn James Fisher dann die Daten aktualisiert, bestehen auf einmal zwei Netflix-Konten – dass doppelt abgebucht wird, fällt frühestens bei der nächsten Abrechnung auf.

Stutzig wurde James Fischer nur, weil die zu aktualisierenden Kreditkartendaten überhaupt nicht zu seiner echten Kartennummer passten. Unser Tipp, wie im Straßenverkehr: Augen auf – und mit dem Fehlverhalten anderer rechnen. Auch wenn im konkreten Fall keine der Parteien wirklich etwas falsch gemacht hat, gehen Sie einfach nicht davon aus, dass sich ein Internet-Dienst so verhält, wie Sie das erwarten.

Efail – HTMLfail?

Als am 13.05.2018 die Entdecker der Efail-Angriffe und die EFF die ersten Hinweise und Warnungen veröffentlichten, war die Rede von Schwachstellen in der PGP- und S/MIME-Verschlüsselung. Wenn man jedoch auf die Website schaut, die ein Forschungsergebnis – ebenso wie ein mehr oder weniger eingängiges Logo – in der heutigen Aufmerksamkeitsökonomie offenbar braucht, dann sieht man schnell den eigentlichen Schuldigen an der Misere: HTML.

Was anfänglich eine Möglichkeit war, die ursprünglich spartanischen reinen Text-E-Mails ansprechender zu formatieren, zieht einen Rattenschwanz an Missbrauchsmöglichkeiten nach sich. Angefangen mit Aufrufen externer URLs, die Efail nutzt, um entschlüsselte E-Mail-Inhalte zu exfiltrieren, könnte das bis zur Echtzeit-Übertragung von Bildschirm-Inhalten oder Kamera-Bildern gehen, falls denn die HTML-„formatierten" Inhalte über einen WebRTC-fähigen Browser gerendert werden.

Mit PDF/A wurde eine Teilmenge von PDF standardisiert, die keine externen Referenzen oder aktiven Inhalte erlaubt und zur Darstellung der meisten üblichen Dokumente völlig ausreicht. Es wird Zeit, über ein vergleichbares statisches HTML/A-Format nachzudenken, das es ermöglicht, bspw. E-Mails wesentlich gefahrloser aufzuhübschen, als über unbeschränktes HTML mit allen zwischenzeitlich definierten Erweiterungen inklusive JavaScript. Auch oder gerade, wenn damit ein Tracking von Mail-Empfängern über Web-Bugs o. ä. ebenfalls nicht mehr möglich wäre.

Facebook-Nachlese

In seiner Anhörung vor dem US-Repräsentantenhaus hat Mark Zuckerberg, CEO von Facebook, am 11.04.2018 die weltweite Anwendung der im neuen europäischen Datenschutzrecht vorgesehenen Kontrollen angekündigt. Falls das kein Lippenbekenntnis bleibt, könnte dies ein wichtiger Schritt zu einer amerikanisch-europäischen Annäherung beim Datenschutzverständnis sein. Immerhin: Anders, als sein Statement aus dem Jahr 2010 vermuten lässt, Privatheit sei nicht länger eine „social norm", ist Zuckerberg zumindest um seine eigene Privatsphäre sehr besorgt: Im Jahr 2013 kaufte er die vier an sein Haus angrenzenden Grundstücke in Palo Alto – für 30 Mio. US$.

Während sich die Facebook-Aktie nach dem 18% Einbruch vom 17.03.2018 inzwischen wieder erholt hat, hat die Aufregung um die Nutzung der Daten von 87 Mio. Facebook-Nutzern für den britischen Datenanalysedienstleister Cambridge Analytica nun handfeste Konsequenzen: Am 02.05.2018 musste das Unternehmen Insolvenz anmelden. Offensichtlich gibt es eine große Diskrepanz zwischen den Erwartungen der Nutzer an den Umgang mit ihren Daten – und der tatsächlichen Rechtslage in Teilen der Welt.

Hoteltüren-Crack

Am 25.04.2018 veröffentlichten Tomi Tuominen und Timo Hirvonen, Mitarbeiter des finnischen Sicherheitsunternehmens F-Secure, dass es ihnen bereits 2017 gelungen ist, durch die Kombination mehrerer kleiner Schwachstellen den Master-Key für das Türschließsystem von Assa Abloy aus einer einzigen Schlüsselkarte abzuleiten. Inzwischen hat der schwedische Hersteller ein Update für das in mehr als 42.000 Hotels weltweit eingesetzte Schließsystem bereitgestellt – das allerdings manuell in jedes einzelne Schloss eingespielt werden muss.

Der Angriff ist ein Beispiel für die latente Gefahr, die in allen digitalen Zutrittssystemen lauert: Jede entdeckte Schwachstelle, die den Zutrittsschutz aushebelt, skaliert sofort, da sie alle bereits installierten Einheiten betrifft. Und da die Installation von Updates – anders als bei PCs oder Smartphones – weder üblich ist noch automatisiert erfolgt, ist eine erfolgreiche Ausnutzung einer solchen Lücke sogar sehr wahrscheinlich.

APT-Simulation

Am 30.04.2018 erweiterte MITRE sein vor ziemlich genau einem Jahr veröffentlichtes ATT&CK-Framework über auftretende Angriffsklassen, -typen und -techniken von 188 auf 219 Angriffstypen, verständlich gruppiert in einer technischen Angriffs-Matrix. Nicht erst seitdem fragen sich viele CISOs, ob ihr Netzwerk nicht bereits Opfer eines Advanced Persistent Threat-Angriffs geworden ist.

Mit dem APT Simulator von Florian Roth, der seit dem 09.04.2018 in einer stabilen Version 0.80 verfügbar ist, kann das eigene Red Team die Erkennung von APT-Angriffen trainieren: Damit lassen sich Windows-Enterprise-Clients per *.bat-Script mit derzeit bis zu 25 Testfällen aus den Bereichen Antivirus, Network Intrusion Detection, Endpoint Detection, Security Monitoring und Compromise konfrontieren – und jede zweite Kalenderwoche einen vermeintlichen Incident simulieren. Noch vielversprechender ist die Möglichkeit, auch eigene Testfälle zu ergänzen.

Simple DSGVO-Compliance

Für alle, bei denen Weihnachten jedes Jahr ganz überraschend kommt und der Datenschutz erst seit der DSGVO (General Data Protection Regulation, GDPR) ein Thema ist, gibt es eigenwillige Angebote wie https://gdpr-shield.io.

Falls die Seite wegen Überlastung nicht erreichbar sein sollte, kann man dem Suchmaschinen-Cache die Zielsetzung entnehmen: „Making your website GDPR compliant can take thousands in legal fees ...“. Die Idee des Angebotes: Man sperre EU-Besucher von den eigenen Webseiten aus – was wäre auch einfacher? Geo-IP-Filterung als Compliance-Maßnahme...

Secorvo News

ISO-zertifiziertes ISMS

Anfang 2017 hat das Kirchliche Rechenzentrum Südwestdeutschland (KRZ-SWD), einer der führenden IT-Dienstleister für Kirche, Diakonie und Caritas begonnen, sich mit dem Information Security Management System ISMS ready2go von Secorvo auf eine ISO 27001-Zertifizierung vorzubereiten.

Mit dem Auditbericht vom 02.05.2018 wurde dem Rechenzentrum nun nach wenig mehr als einem Jahr Vorbereitung die Erfüllung der Anforderungen der ISO 27001 bestätigt – ohne eine einzige Abweichung: der „Proof of Concept“, dass ein ISMS „out of the box“ den Weg zum Zertifikat erheblich beschleunigen kann. Wir gratulieren herzlich und bedanken uns für die hervorragende Zusammenarbeit!

Secorvo Seminare

Vor der Sommerpause bieten wir Ihnen noch einmal die Möglichkeit, sich Ihre Kenntnisse und Erfahrungen in der IT-Sicherheit mit einem T.I.S.P.-Zertifikat bestätigen zu lassen: Das T.I.S.P.-Seminar findet statt vom **11. bis 15.06.2018**. Wir freuen uns auf Ihre Anmeldung.

10. Tag der IT-Sicherheit

Auf dem diesjährigen zehnten Karlsruher „Tag der IT-Sicherheit“, einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe und dem CyberForum e. V., werden aktuelle Herausforderungen der IT-Sicherheit für Unternehmen diskutiert und Präventionsmöglichkeiten vorgestellt. Als Keynote-Speaker konnten wir in diesem Jahr Stefan Krebs gewinnen, den CIO Baden-Württemberg, Beauftragter der Landesregierung für Informationstechnologie. Er verfügt über vieljährige Erfahrung im IT-Sicherheitsbereich, im Bankensektor und der Verwaltung.

Die Veranstaltung findet am **07.06.2018** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

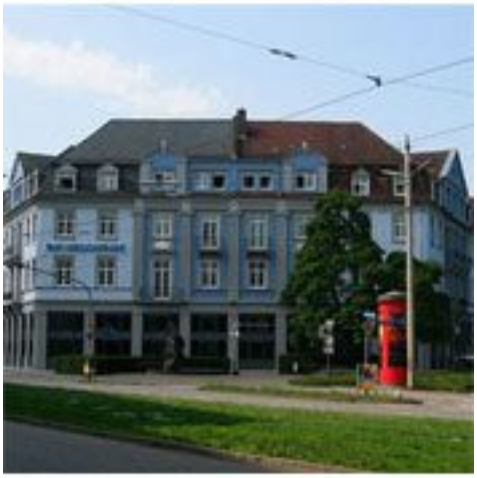
Veranstaltungshinweise

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

Juni 2018	
07.06.	10. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
11.-12.06.	DuD 2018 (COMPUTAS, Berlin)
11.-15.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2018 (ENISA, EC DG Connecct, Universität Wien, Barcelona/ES)
15.-16.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
17.-21.06.	OWASP AppSec EU 2018 (OWASP Foundation, Tel Aviv/ISR)
20.-22.06.	Entwicklertag 2018 (VKSI, GI, ObjektForum, Karlsruhe)
26.-27.06.	EssoS 2018 (EssoS Organization, Paris/FR)
Juli 2018	
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)

Fundsache

Unter dem Titel „Human Rights under Surveillance“ veröffentlichte Amnesty International einen spannenden und betroffen machenden Bericht über IT-Angriffe auf Menschenrechts-Aktivisten in Pakistan. Langfristig geplante Attacken, unter anderem über Spearfishing-E-Mails und gefakte Social-Media Seiten sowie gefakte Personen, werden im Detail beschrieben. Lesenswert.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Jochen Schlichting

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

secorvo
security consulting

Secorvo Security News

Juni 2018

Panik 4.0

Unter Panik verstehen wir eine durch eine plötzliche, echte oder vermeintliche Gefahr hervorgerufene, übermächtige Angst, die zu unüberlegten Reaktionen führt. Sie kann sich zur kollektiven oder Massenpanik entwickeln, wenn in „eng stehenden Gruppen“ Menschen ihre Handlungen gegenseitig beobachten und darauf reagieren – und dabei ihre Selbstkontrolle verlieren.

In Zeiten allgegenwärtiger Digitalisierung kann auch Panik digital werden: Verursacht im digitalen Kontext und verstärkt durch die Verbreitung über verzugsfreie digitale Kommunikationsmedien wie Instant Messaging oder Social Networks entsteht so schnell eine Massenpanik 4.0. Dabei zeigen sich die fatalen Folgen des zunehmenden Fast-Food-Gebarens bei der Erzeugung und Verbreitung von Informationen: Publizierte Nachrichten sind immer nachlässiger recherchiert und werden allerorten ungeprüft kopiert – die Empfänger haben sich bereits so daran gewöhnt, dass sie den Wahrheitsgehalt nicht mehr aus der Seriosität einer Quelle (gibt es das noch?) sondern aus der Anzahl der Nachrichten ähnlichen Inhalts ableiten.

Erleben konnte man das in den vergangenen Wochen im Zusammenhang mit dem Inkrafttreten der DS-GVO. Bestenfalls halbrichtige Darstellungen der Anforderungen in den Medien ließen den Verdacht aufkeimen, es kämen völlig neue Herausforderungen auf Unternehmen, Vereine und Verbände zu – und es sei mit Ordnungsgeldern in Höhe von 4% des Jahresumsatzes zu rechnen.

Zu den Panik-Reaktionen auf dieses Halbwissen zählen E-Mails von Vereinen, die eine Einwilligung der Mitglieder für die erforderliche Verarbeitung personenbezogener Mitgliederdaten erbitten, Kühlschränke mit Datenschutzerklärung oder Tageszeitungen, die den Webauftritt abschalten. Blenden wir den volkswirtschaftlichen Schaden aus, so bleibt ein sehr bitterer Nachgeschmack: Dem Schutz unserer Persönlichkeitsrechte hat das mehr geschadet als genutzt.

Inhalt

secorvo
security consulting

Security News

Alte Zöpfe

Nachdem sich seit März 2018 Version 1.3 des Protokolls Transport Layer Security (TLS) in den letzten Zügen der Standardisierung befindet, gibt es zunehmend Bestrebungen, alte Zöpfe abzuschneiden. Gemeint sind insbesondere die Protokollversionen TLS 1.0 (1999) und 1.1 (2006). Die alten Protokollversionen weisen kryptografische Schwächen auf und sind im Vergleich mit TLS 1.2 und 1.3 nicht mehr zeitgemäß. Diese Erkenntnis ist auch im Standard PCI DSS angekommen: Ab dem 01.07.2018 sind TLS 1.0 und 1.1 nicht mehr erlaubt.

In den meisten Fällen sollte eine Deaktivierung der alten Versionen keine merkbaren Folgen nach sich ziehen: TLS 1.2 ist bereits seit 10 Jahren standardisiert und wird dementsprechend auch von allen gängigen Browsern und Bibliotheken unterstützt. Diverse aktuelle Browser unterstützen übrigens bereits TLS 1.3. – sind Sie schon dabei?

Stand der Technik

Am 14.06.2018 veröffentlichte TeleTrusT die deutlich überarbeitete Fassung der „TeleTrusT-Handreichung zum Stand der Technik“ nach IT-Sicherheitsgesetz und DSGVO. Die Erstfassung von 2016 wurde um Erklärungen zur Bestimmung des Technologiestandes und um eine Methode zur Bewertung der Maßnahmen ergänzt. Die Beiträge wurden gründlich überprüft und ggf. gestrichen oder überarbeitet. Eine Bewertung soll transparent machen, warum Maßnahmen aufgrund von „Grad der Anerkennung“ und „Grad der Bewährung in der Praxis“ als Stand der Technik aufgeführt sind. Zusätzlich wurden die Struktur verbessert und neue Maßnahmen und Prozesse ergänzt.

Ein weiterer schöner Meilenstein für die Pioniere der IT-Sicherheit und eine hilfreiche Grundlage zur Positionsbestimmung, wenn es um die Konzeption von Maßnahmen und Prozessen geht.

Unter der Gürtellinie

Traditionell setzten viele Bedrohungsanalysen und Sicherheitskonzepte auf der Ebene des Betriebssystems an. Durch zunehmende Virtualisierung kommt u. U. noch ein unterliegendes Hypervisor-System mit ins Bild. Seit ein paar Monaten gerät nun die Sicherheit unterhalb der Betriebssystem-Ebene zusehends ins Blickfeld: Seit der Entdeckung der Spectre- und Meltdown-Schwachstellen finden Forscher immer neue Varianten, um Informationen über Prozessgrenzen hinweg auszuspähen. So veröffentlichte OpenBSD am 05.06.2018 einen Patch gegen eine Prozessor-Schwachstelle – das zugehörige Advisory wurde von Intel erst am 13.06.2018 veröffentlicht.

Und auch auf der proaktiven Seite gibt es Aktivitäten: Microsoft hat – experimentell und unabhängig von Schwachstellen durch spekulative Ausführung von Befehlen – bereits Windows 10 auf eine Prozessor-Architektur portiert, bei der der Compiler die optimierte Abarbeitungsfolge vorgibt. Und am 18.06.2018 veröffentlichten Forscher einen Vorschlag für eine „Leak“-freie spekulative Ausführung.

Derweil holen uns wieder totgehoffte Altlasten ein: So wurde am 19.06.2018 gemeldet, dass sich die Anmeldung an HPs iLO4 Management-System mittels eines simplen Pufferüberlaufs übertölpeln lässt.

Wer heute neue Sicherheitskonzepte erstellt, tut gut daher daran, in die Bedrohungsanalyse auch die relevanten Ebenen unterhalb des Betriebssystems einzubeziehen.

Gezahnter Papiertiger

„Lieber offline als abgemahnt“, „Was Ihr Chef jetzt verbieten kann“ oder „Selbst Anwälte sind ratlos über die neuen Datenschutzregeln“ sind nur einige der Headlines, welche dieser Tage in den Medien zum Thema Datenschutz gestreut werden. Nach Ablauf der zweijährigen Übergangsfrist gelten seit dem 25.05.2018 die Vorgaben der Datenschutz-Grundverordnung (DS-GVO). Den Aufsichtsbehörden wird nun eine wesentlich höhere Bedeutung zugemessen als bisher. Wer sich nicht datenschutzkonform verhält, riskiert Bußgelder bis zu 20 Mio. € oder 4% des weltweit erzielten Jahresumsatzes. Zahlen, die mittlerweile durch die Medien Omnipräsenz erlangt haben und einen Großteil der Angst und Unsicherheit verantworten, die sich in den letzten Monaten ausgebreitet haben.

Seit Inkrafttreten des Gesetzes ist nun ein Monat vergangen. Haben die Unternehmen nun überreagiert, oder wurden sie gerechtfertigt dazu gedrängt, in hektische Tätigkeit zu verfallen, um DS-GVO-konform zu werden? Sicher ist: Vieles, was bereits im nun von der DS-GVO verdrängten Bundesdatenschutzgesetz (BDSG) gefordert wurde, behält seine Gültigkeit. Und angesichts der Übergangsfrist von zwei Jahren hatten Unternehmen ausreichend Zeit, sich auf die neuen Anforderungen vorzubereiten.

Die Verantwortung sollte jedoch nicht allein den betroffenen Unternehmen zugeschoben werden. Denn es bestehen gerechtfertigt Unsicherheiten, die aufgrund dehnbarer DS-GVO-Bestimmungen

noch ausgelegt und geklärt werden müssen. Nicht zuletzt auch aufgrund der noch im Entwurfsstadium befindlichen E-Privacy-Verordnung für den Bereich der elektronischen Kommunikation, deren „go live" nicht vor 2019 zu erwarten ist, und von welcher erwartet wird, dass sie konkretisierende und ergänzende Anforderungen zu den Vorgaben der DS-GVO formuliert.

Doch was bedeutet diese aktuelle Rechtslage für Unternehmen konkret: Soll man sich von dem aktuellen Hype mitreißen lassen? Ist mit einem Abflachen des Datenschutz-Aktivismus zu rechnen, sobald sich die Unruhe etwas gelegt hat?

Tatsächlich wäre es ratsam, sich auf die (Weiter-) Entwicklung des Grundgerüsts der Datenschutz-Organisation und deren Implementierung zu konzentrieren. Denn mit entsprechender Dokumentation der Prozesse und kontinuierlicher Verbesserung ist nicht nur ein nachhaltigerer Datenschutz-Reifegrad zu erreichen – es ist auch der beste Schutz vor behördlichen Maßnahmen.

Bulk-Forensik

Lange Zeit war es recht still um die Weiterentwicklung des forensischen Carving-Werkzeuges bulk_extractor. Dies hat sich aber am 30.12.2017 geändert: Die hilfreiche Scanner-Komponente „scan_ntfsusn" wurde integriert, mit der USN-Journal-Metainformationen (Zeitstempel und Schreibtransaktionen für Dateien und Verzeichnisse) in einem NTFS-Dateisystem von Windows parallel ausgewertet werden können.

Da bulk_extractor tatsächlich jeden CPU-Core und Thread nutzt, kann mit Nutzung von scan_ntfsusn ein erheblicher Zeitgewinn bei der vollautomatischen Datenaufbereitung erzielt werden. Dazu kommt seit 28.01.2018 eine Weiterentwicklung namens bulk_extractor-rec, die nicht der offiziellen Entwicklung folgt, aber dafür aus den verschiedenen internen NTFS-Logdaten noch die Record-Typen INDX, RSTR/RCRD und FILE durch zusätzliche Scanner-Komponenten extrahiert. Wer also schnell Informationen braucht und nicht auf Plaso warten möchte, den werden diese Funktionen freuen.

Secorvo News

Teamverstärkung

Dank der zunehmenden Nachfrage nach Unterstützung benötigt auch Secorvo personelle Verstärkung. Und wir freuen uns, in den vergangenen Wochen mit Michael Knöppler und Thomas Maus zwei sehr kompetente IT-Sicherheitsexperten für unser Team gewonnen zu haben.

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Secorvo Seminare

Nach der Sommerpause startet die Herbst-Seminarserie von Secorvo im Oktober mit den beiden Zertifizierungsseminaren T.I.S.P. (15.-19.10.2018) und T.P.S.S.E. (12.-15.11.2018). Wir freuen uns auf Ihre Teilnahme – und empfehlen für das T.I.S.P.-Seminar eine frühzeitige Anmeldung.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

Freiwild im Cyberspace

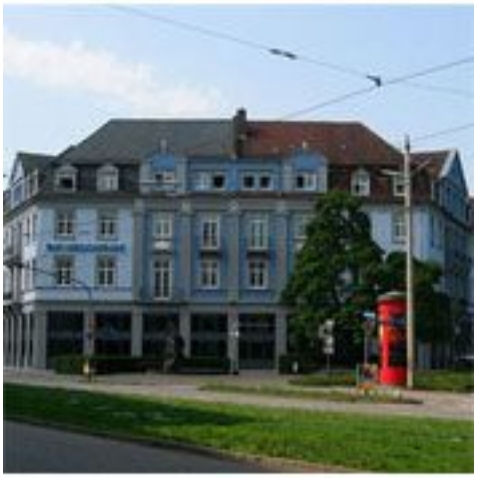
Die Anforderungen an die Mobilität von Arbeitnehmern steigen beständig - unterstützt von immer kleineren und leistungsfähigeren Endgeräten. Wie aber lässt sich diese Flexibilität mit Sicherheitsanforderungen vereinbaren? Bei unserem kommenden KA-IT-Si-Event am **12.07.2018** stellt Dirk Fox (Secorvo) in seinem Vortrag wichtige Anforderungen und technische Möglichkeiten für sicheres mobiles Arbeiten vor. Anschließend geht Holger Bajak (ophelis) in seinem Vortrag "Mobil und vernetzt" auf das Arbeiten in neuen Strukturen ein. Arbeiten ist im digitalen Zeitalter überall und jederzeit möglich. Das Büro gewinnt dadurch eine neue Bedeutung: Es ist weit mehr als ein Arbeitsraum. Das Büro wird zum Treffpunkt, dient dem Austausch und der Zusammenarbeit. Es erzeugt Zugehörigkeit und bietet den Mitarbeitern Heimat.

Die Veranstaltung findet in Kooperation mit feco-feederle und ophelis statt. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

Juli 2018	
12.07.	Freiwild im Cyberspace (KA-IT-Si Karlsruhe)
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)
August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
24.09.	Datenschutztag 2018 (COMPUTAS Gisela Geuhs GmbH, Köln)
28.-30.09.	FIfFKon 2018 (FIfF e.V., Berlin)



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Jochen Schlichting

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

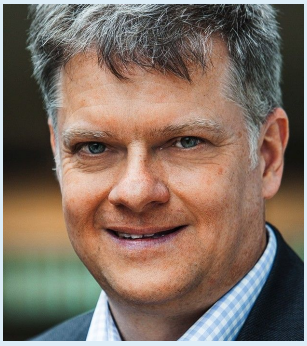
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juli 2018



Falsche Baustelle

Seit Jahren geistert das Bild der E-Mail als „Postkarte“ unausrottbar durch Gazetten und Datenschutzempfehlungen: Wer E-Mails unverschlüsselt versende, der müsse damit rechnen, dass sie mitgelesen werden. Tatsächlich übermitteln Mailserver die ihnen anvertrauten Nachrichten heute meist wirksam verschlüsselt: Als Reaktion auf Edward Snowdens Veröffentlichungen stellten 2014 im Projekt „E-Mail made in Germany“ mehrere Provider und immer mehr Unternehmen ihre Mailserver auf eine TLS-Verbindungsverschlüsselung um, und Zugriffe auf das Postfach werden sowohl von Web-Clients als auch unternehmensintern schon längst verschlüsselt. Ein Mitlesen von E-Mails erfordert daher heute einen erfolgreichen DNS-Angriff – oder den direkten Zugriff auf die Postfächer.

Genau dort lauert in Wirklichkeit die reale Bedrohung: Amerikanische Anbieter kostenloser E-Mail-Dienste wie insbesondere GMail geben Drittfirmen, die Apps mit E-Mail-Anbindung realisieren, großzügig den Zugriff auf Kundenpostfächer frei, sofern diese dafür eine Zustimmung der Benutzer einholen. Und dann wird, automatisiert oder manuell, die persönliche Nachrichtenablage durchwühlt – z. B. um Spam-Diensten die Optimierung der Empfängeransprache zu ermöglichen (wie Return Path), passende Werbung zu generieren oder Testdaten für die Verbesserung der eigenen App zu gewinnen. Immerhin: Wer wissen will, welchen Apps er bereits Zugriff auf sein GMail-Konto eingeräumt hat, kann dies in den Privacy-Einstellungen seines Google-Accounts nachprüfen.

Dass es so etwas wie ein Fernmeldegeheimnis gibt und persönliche Kommunikationsinhalte nicht in Testumgebungen gehören hat sich offenbar noch nicht bei allen Anbietern herumgesprochen. Und für Anwender ist es noch immer nicht selbstverständlich, dass man Datenschutzerklärungen von Apps sehr genau lesen sollte, bevor man ihnen zustimmt – allen Datenschutzskandalen zum Trotz.

Inhalt

secorvo
security consulting

Security News

WPA ... zum Dritten

Nicht nur das TLS-Protokoll (SSN 06/2018), sondern auch das als WPA2 bekannte und ebenfalls in die Jahre gekommene Sicherheitsverfahren hat ein Facelifting erhalten: Die WiFi Alliance veröffentlichte am 09.04.2018 eine Zusammenfassung der neueren Sicherheitsmechanismen, die in 802.11s, 11w bzw. 11ac standardisiert wurden, unter der Bezeichnung WPA3:

- das Passwort-basierte Schlüsselaustauschverfahren SAE, das Sicherheit gegen Offline-Wörterbuchattacken auf das WLAN-Passwort verspricht,
- die Absicherung von Management-Frames, wie bspw. Deauthentication, die Angreifer zum Abmelden einer angegriffenen Station missbrauchen konnten und
- die durchgängige Nutzung von Kryptoalgorithmen, die einer 192-bit-Stärke nach aktuellen US-Behördenstandards entsprechen.

Dass dabei recht sorgfältig gearbeitet wurde, zeigt sich u. a. daran, dass nicht nur die Stärke der WLAN-Verschlüsselung selbst, sondern auch die TLS Cipher Suites festgelegt wurden, die bei einer vorangegangenen EAP-Authentifikation zum Einsatz kommen dürfen.

1:0 für 802.11 vs. Bluetooth SIG

Ordentlich implementierte WPA3-Produkte sollten auch gegen die Schwachstelle vieler Bluetooth-Implementierungen gefeit sein, die am 24.07.2018 publiziert wurde – die Bluetooth SIG hingegen muss ihre Spezifikation um einen Schritt zur Prüfung der übergebenen Elliptische-Kurven-Punkte nachbessern, um von Angreifern konstruierte Punkte zuverlässig zu verwerfen. Für SAE ist eine solche Prüfung bereits in Abschnitt 12.4.5.4 von IEEE 802.11-2016 beschrieben – siehe Seite 1942.

Framing 4.0

Bisher waren für einen kritischen, mit den Möglichkeiten der Bildmanipulation und Bildsynthese vertrauten Beobachter Fälschungen durch Video-Rewriting meist mit bloßem Auge erkennbar. Diese Zeiten sind nun allerdings vorbei: Am 29.05.2018 wurde von einer Forschergruppe um das Max-Planck-Institut für Informatik ein Verfahren veröffentlicht, welches dreidimensionale Kopfmodelle erstellt und die Qualität der Fälschung durch einen KI-Gegenspieler prüfen lässt.

Ob die von den Autoren der Studie in den Vordergrund gestellte Lippenkorrektur bei synchronisierten Filmen zukünftig der bevorzugte Anwendungsfall sein wird, darf bezweifelt werden – Fake News und Fake Porn erscheinen da viel wahrscheinlicher. Auch der Aufwand wird eine breite Anwendung kaum verhindern: Diese Hoffnung war schon vor 35 Jahren trügerisch, als erste Warnungen vor digitaler Foto-Fälschung ausgesprochen wurden. Hardware für rund 2.000 € und eine Rechenzeit von einigen Stunden bis wenigen Tagen sind bereits heute kein unüberwindliches Hindernis.

1000 x T.I.S.P.

Das deutsche Schwergewicht der Personenzertifizierung für Informationssicherheit T.I.S.P. (TeleTrusT Information Security Professional) wurde am 10.04.2018 zum 1.000sten Mal verliehen – an Herrn Kai Riecke, CTO der Hubert Burda Media Holding.

Prof. Dr. Norbert Pohlmann, Vorstand von TeleTrusT, äußert sich stolz: „Der T.I.S.P. hat eine Anerkennung erreicht, die den Vergleich mit ähnlichen Personen-Zertifikaten im deutschsprachigen Raum nicht scheuen muss."

Mit der erfolgreich abgelegten Prüfung zum T.I.S.P. belegt ein IT-Sicherheits-Spezialist seine umfassenden Kenntnisse im IT-Sicherheitsumfeld auf technischem, rechtlichem und strategischem Gebiet. Das Zertifizierungsprogramm umfasst eine fünftägige Schulung, an die sich eine intensive Prüfung anschließt. Die Schulungsanbieter Secorvo, isits und Fraunhofer SIT freuen sich bereits auf die Ausstellung von Zertifikat Nr. 2.500...

Löschkonzept goes ISO

Die englische Fassung der von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect geförderten „Leitlinie Löschkonzept", die am 08.04.2016 als DIN 66398 verabschiedet worden ist (siehe SSN 4/2016), wurde jetzt bei der ISO als Grundlage eines internationalen Standards eingereicht.

Nach den bisherigen Rückmeldungen wird sich an der darin beschriebenen Vorgehensweise nichts ändern. Anpassungen sind notwendig, weil die Beispiele in der Norm noch auf das alte BDSG und nicht auf die DSGVO oder andere internationale Vorschriften abstellen und einige Begriffe an die ISO-Terminologie angepasst werden sollen.

Das Standardisierungsprojekt soll in den kommenden Wochen vom zuständigen Gremium beschlossen werden. Ein ISO-Standard könnte dann Ende 2021 verabschiedet werden und die in Deutschland bereits genormte Vorgehensweise für Löschkonzepte sich auch international durchsetzen.

Informationspflicht

Nach der Datenschutz-Grundverordnung (DSGVO) entsteht zum Zeitpunkt der Erhebung personenbezogener Daten eine Informationspflicht des verantwortlichen Datenverarbeiters gegenüber dem Betroffenen (Art. 13 DSGVO). Dabei können sich in der praktischen Umsetzung zahlreiche Problemfälle ergeben:

- das Unternehmen erhält spontan zugesandte Informationen (z. B. eine Initiativbewerbung),
- es laufen Hintergrundprozesse ab (wie eine automatisierte Erhebung z. B. bei Bonitätsprüfungen),
- es sind gar keine Interaktionen vorgesehen oder
- ein Dienstleister erhebt die Informationen.

Meist liegt die Hauptschwierigkeit darin, einen geeigneten Kommunikationskanal zu finden, der den Betroffenen erreicht und die Anforderungen der DSGVO erfüllt – auch in Bezug auf den Inhalt der Information: So lassen sich komplexe Verarbeitungen oft nicht ohne weiteres in zugleich präziser, transparenter, verständlicher und leicht zugänglicher Form darstellen.

Bleibt zu hoffen, dass die Aufsichtsbehörden eine pragmatische Auslegung dieser Anforderungen vornehmen, die noch etwas einfacher ausfällt als die derzeitigen Vorschläge zur Ausweisung der Videoüberwachung. Denn es wird immer wieder Fälle geben, in denen die Daten verarbeitende Stelle ihren Informationspflichten entweder nicht unmittelbar oder nicht zugleich präzise und verständlich nachkommen kann.

Facebook unter Druck

Nachdem der Europäische Gerichtshof in seinem Urteil vom 05.06.2018 die grundsätzlich gemeinsame Verantwortlichkeit für die Verarbeitung der Nutzerdaten von Unternehmensauftritten bei Facebook („Fanpages“) geklärt hat, haben auch die deutschen Datenschutzaufsichtsbehörden erste Stellungnahmen abgegeben.

Die Pflichten gemeinsam Verantwortlicher regelt die DSGVO in Art. 26. Danach müssen die Zuständigkeiten insbesondere bezüglich der Betroffenenrechte und Informationspflichten in einer transparenten Vereinbarung festgelegt werden. Dementsprechend fordern die Aufsichtsbehörden, dass dem Fanpage-Besucher diese Informationen beim Besuch zugänglich gemacht werden müssen. Für das Tracking soll Facebook grundsätzlich eine Einwilligung einholen; die Seitenbetreiber müssen sich vergewissern, dass Facebook die Pflichten erfüllt.

Bislang hat Facebook den Seitenbetreibern keine entsprechende Vereinbarung zur Verfügung gestellt. Für Seitenbetreiber ist damit auch nach dem Urteil unklar, womit sie zu rechnen haben und in wieweit sie derzeit ihre Pflichten bezüglich der Informationspflichten auf der Fanpage erfüllen.

Secorvo News

Weiterbildung

Schon im Sommer an den Herbst denken: Im Oktober starten wir unsere Seminarserie mit den beiden Zertifizierungsseminaren T.I.S.P. (**15.–19.10.2018**) und T.P.S.S.E. (**12.–15.11.2018**). Wir freuen uns, sie in unserem frisch renovierten Seminarbereich begrüßen zu dürfen – und empfehlen für das T.I.S.P.-Seminar eine baldige Anmeldung, da uns schon zahlreiche Anmeldungen vorliegen.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

Digitale Mülltrennung

Die DSGVO fordert das Löschen personenbezogener Daten. Wie aber organisiert man diese Aufgabe für eine Organisation effizient und systematisch? Die DIN 66398 „Leitlinie Löschkonzept“, an deren Entwicklung Secorvo maßgeblich beteiligt war, gibt zahlreiche Hilfestellungen dafür.

Dr. Volker Hammer (Secorvo) war Editor der Norm und gibt beim kommenden **KA-IT-Si-Event** am **13.09.2018** im Panoramasaal der IHK Karlsruhe einen Überblick über die Inhalte aus erster Hand (Beginn: 18 Uhr). Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Veranstaltungshinweise

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

August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
13.09.	Digitale Mülltrennung (KA-IT-Si, Karlsruhe)
Oktober 2018	
01.-03.10.	ISSE 2018 (EEMA, Rom/IT)
08.-12.10.	OWASP AppSec USA 2018 (OWASP Foundation, San Jose/US)

Fundsache

Studien zur IT-Sicherheit gibt es viele – aber nur wenige liefern statistisch belastbare Aussagen und sind deutlich mehr als eine willkürliche Befragung zufällig ausgewählter Unternehmen. Daher hebt sich die wik-Studie „Aktuelle Lage der IT-Sicherheit in KMU“ vom 18.05.2018 erfreulich vom sonstigen Einerlei der Kaffeesatzerkenntnisse ab.

Impressum

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

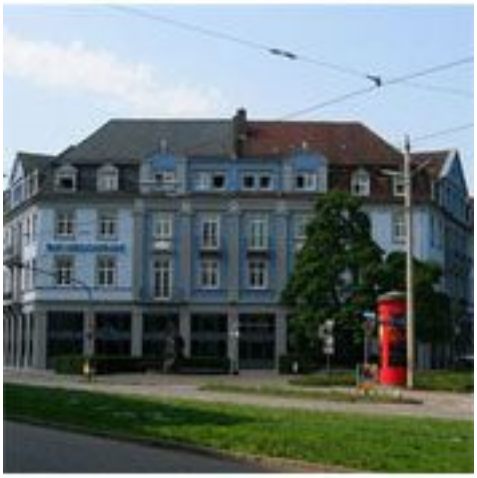
ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Dr. Volker Hammer, Hans-Joachim Knobloch, Michael Knopp, Thomas Maus, Sarah Niederer, Jochen Schlichting

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



secorvo
security consulting

Secorvo Security News

August 2018

Früher war die Realität besser

Realität kommt aus der Mode. War sie in der Aufklärung der Prüfstein und das Bindeglied der gemeinsamen Welterkenntnis – ein objektiv von jedermann beobachtbarer und per reproduzierbarem Experiment befragbarer Bezugsrahmen – so genügt sie heute nicht mehr: „Augmented Reality", „Virtual Reality" und „Fake-News" erheben – in unterschiedlichen Graden der Transparenz – die Illusion über die Realität.

Die technisch vermittelte Realitätswahrnehmung steht jedoch an vielen Fronten unter Beschuss: Fotofälschungen sind ein alter Hut, signifikante Fortschritte in der Videofälschung (SSN 7/2018) erschweren deren Erkennung, gefälschte Stimmen und andere biometrische Merkmale täuschen erfolgreich biometrische Sensoren.

Der Glaube an die unbewiesenen Versprechungen der Technik ist regelmäßig weit verbreitet, das Vertrauen in fundierte Warnungen (selbst der Techniker) hingegen oft gering - bis an die Grenzen der Realitätsverweigerung, siehe schon Joseph Weizenbaums Eliza.

Technik bändigt die Komplexität der Welt in vereinfachenden, aber selbst immer komplexeren Modellen. Das kann dazu führen, dass die Technik der Realität nicht mehr glaubt – zum Beispiel wenn selbstfahrende Autos immer anhalten, solange ein Stoppschild in der Karte verzeichnet ist. Selbst wenn jemand das Schild abmontiert. Wie kalkulierbar das für andere Verkehrsteilnehmer ist und wie rücksichtsvoll das autonome Fahrzeug auf dieses fehlende Verkehrsschild reagiert, ist eine offene Frage, ebenso wie die Aktualität und Akkuratesse der Karte, die Reaktion auf rechtmäßig entfernte Vorfahrtsschilder, Aufhebungszeichen und viele, viele weitere Szenarien.

Über eines aber sollten wir uns im Klaren sein: Die Realität kann Illusionen länger ignorieren als umgekehrt. Wenn sich der helle Himmel des Modells als die weiße Plane eines LKWs entpuppt, hat die Realität das letzte Wort. Hybris.

Inhalt

secorvo
security consulting

Security News

WPA2-Schwachstelle

Am 04.08.2018 wurde im hashcat-Forum unter dem Pseudonym atom ein neuartiger Angriff auf WLAN-Netzwerke vorgestellt, die mit WPA-PSK und WPA2-PSK gesichert sind. Bisher mussten Angreifer einen Vier-Wege-Handshake eines Clients abwarten, diesen aufzeichnen und im Anschluss eine Wörterbuchattacke über den gesamten Handshake ausführen.

Einige Router-Hersteller integrieren jedoch gleich im ersten Paket einen SHA1-Hash über Informationen, die auch einem Angreifer bekannt sind. Der Schlüssel, der zur Bildung des Hash verwendet wird, ist in diesem Fall der Pre-Shared-Key. Da der zu brechende Hash deutlich kürzer ist als ein Vier-Wege-Handshake benötigt die Wörterbuchattacke deutlich weniger Zeit.

Der vor kurzem verabschiedete WLAN-Standard WPA3 (SSN 07/2018) ist nicht von diesem Angriff betroffen und sollte daher möglichst bald eingesetzt werden – auch unter dem Gesichtspunkt, dass alte WLAN-Standards auch weiterhin von Sicherheitsforschern unter die Lupe genommen werden und daher das Bekanntwerden weiterer Schwächen nicht auszuschließen ist.

Sennheisers Root-Zertifikat

Sennheiser Communications sorgte in diesem August bei manchen Anwendern der Software HeadSetup, die die Schnittstelle zwischen einem Sennheiser-Headset und dem Softphone bildet, für Unbehagen: Wird die Software installiert, so bringt diese huckepack ein vom Hersteller selbstsigniertes Root-Zertifikat mit, welches unbemerkt im Windows-Zertifikatspeicher als vertrauenswürdige Stammzertifizierungsstelle installiert wird. Damit nicht genug: Das Zertifikat trägt den „vertrauenswürdigen" Common Name 127.0.0.1. Der Aussteller des Zertifikats (oder ein Angreifer, der den zugehörigen Private Key erbeutet) kann damit Man-in-the-Middle-Angriffe auf mit TLS gesicherte Verbindungen beteiligter Systeme durchführen.

Dabei ist der Zweck des CA-Zertifikats unklar: Wir konnten keine negativen Folgen nach dem Löschen des ungebeten installierten Zertifikats feststellen. Bis Redaktionsschluss erhielten wir auch keine Antwort vom Hersteller auf die Frage nach dem Zweck dieser Maßnahme.

Dieser fahrlässige Umgang eines Herstellers mit der Sicherheit der IT-Infrastruktur der Kunden erinnert an Vorfälle wie Superfish auf Lenovo-PCs und –Laptops. Betroffenen empfehlen wir, Kontakt mit Sennheiser aufzunehmen und das Zertifikat aus dem Windows-Zertifikatspeicher zu entfernen.

Grundschutz runderneuert

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 08.08.2018 einen neuen Online-Kurs veröffentlicht, der allen Anwendern einen Einstieg in und einen Überblick über den in den vergangenen Jahren modernisierten IT-Grundschutz bietet.

Im Rahmen der Modernisierung wurden Überarbeitungen der BSI-Standards veröffentlicht: Managementsysteme für Informationssicherheit (200-1), IT-Grundschutz-Methodik (200-2) und Risikomanagement (200-3). Die IT-Grundschutz-Kataloge löste das IT-Grundschutz-Kompendium ab. Es besteht weiterhin aus Bausteinen, allerdings trennt der IT-Grundschutz jetzt zwischen Bausteinen mit Anforderungen und solchen mit Umsetzungshinweisen. Deren Vermischung war eine große Schwäche der alten Bausteine.

Eine Zertifizierung nach dem modernisierten IT-Grundschutz ist seit Ende 2017 möglich. Die Übergangsfrist für eine Zertifizierung nach dem bisherigen IT-Grundschutz endet am 30.09.2018.

Insgesamt ist dem BSI damit eine deutliche Qualitätsverbesserung gelungen. Die größte verbleibende Schwäche in der Praxis ist, dass leider nicht alle existierenden Bausteine in das neue Format übertragen wurden.

Fax-Angriff

Die von Checkpoint Research entdeckte und am 15.08.2018 veröffentlichte Schwachstelle „Faxploit" ermöglicht einem Angreifer, HP-Multifunktionsdrucker zu übernehmen. Sie nutzt eine Buffer-Overflow-Verwundbarkeit in dem Codeteil, der JPEG-Dateien interpretiert. Da Farb-Faxe als JPEG-Dateien übertragen werden, kann der Angriff über die Telefonleitung erfolgen – vorbei an Firewalls, Intrusion-Detection-Systemen und Content-Scannern. Betroffen sind möglicherweise nicht nur andere Fax-Empfangsgeräte, sondern auch Fax-Konvertierungssoftware, die den betroffenen Code verwendet.

Der Fall erinnert daran, dass alle Peripheriegeräte, die von außen erreicht werden können, Schwachstellen enthalten und daher ein Einfallstor für Angriffe sein können. Solche Geräte sollten daher geeignet abgeschottet werden, um im Falle eines erfolgreichen Angriffs ein Eindringen in das interne Netzwerk wirksam zu verhindern.

secorvo
security consulting

Biometriekritik

Die Kritik an der Nutzung biometrischer Merkmale für die Authentifikation ist nicht neu: Biometrische Merkmale können nicht abgelegt oder ausgetauscht werden, viele der heute eingesetzten Systeme lassen sich täuschen und können sogar deren Nutzer zum (physischen) Angriffsziel machen.

Am 06.08.2018 berichteten Deutschlandfunk und Bayerischer Rundfunk, dass schon heute der Handel mit gefälschten biometrischen Pässen und biometrischen Daten blüht. Selbst Prof. Dr. Udo Helmbrecht, Präsident der ENISA, warnt, der Überwindungssicherheit biometrischer Systeme nicht blind zu vertrauen. Dabei sind noch immer Anwendungen im Einsatz, die biometrische Daten im Klartext übermitteln – während die Verbreitung biometrischer Authentifikationsverfahren rasant wächst.

Wer seine eigenen einmaligen biometrischen Merkmale vor unerwünschter Verbreitung schützen will, sollte bei der Nutzung solcher Verfahren Zurückhaltung üben – und bei sicherheitskritischen Anwendungen lieber auf Zwei-Faktor-Authentifikationsverfahren mit „Besitz und Wissen" zurückgreifen.

Staatstrojaner

Im Jahr 2007 hat das Bundesverfassungsgericht hohe Hürden für die technische Ausspionierung von IT-Systemen Verdächtiger formuliert (SSN 10/2007). Nun hat der Bundestag am 22.06.2017, wenig beachtet, über einen Änderungsantrag der Bundesregierung eine Ausweitung von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung beschlossen. Dass neben unverschlüsselten Kommunikationsdaten bspw. von Messenger-Diensten wie WhatsApp weitere Inhalte eines mit einem „Staatstrojaner" infiltrierten informationstechnischen Systems abgezogen werden ist nach § 100b StPO nur bei besonders schweren Straftaten zulässig – und „wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre": eine sehr weit auslegbare Ermächtigung. Dank einer Anpassung des § 100e StPO dürfen bei einer Online-Durchsuchung gewonnene Daten nun auch „zu Zwecken der Gefahrenabwehr" genutzt werden.

Gegen diese Ausweitung der Online-Durchsuchung hat nach dem Verein Digitalcourage am 20.08.2018 auch die FDP Verfassungsbeschwerde eingelegt. Hoffentlich bleibt das Bundesverfassungsgericht seinen 2008 formulierten Grundsätzen treu.

Secorvo News

Teamverstärkung

Am 01.09.2018 stößt Friederike Schellhas-Mende, Juristin und Datenschützerin, zu unserem Consulting-Team dazu. Und ebenfalls am 01.09.2018 übernimmt Joanna Klotz den Seminarbereich bei Secorvo. Willkommen im Team!

Secorvo@it-sa

Vom 09. bis 11.10.2018 sind wir mit einem Stand auf der IT-Security-Messe it-sa in Nürnberg vertreten und werden dort unsere Managementsysteme für Datenschutz und Informationssicherheit DSMS ready2go und ISMS ready2go zeigen. Sie finden uns in Halle 10 (Standnummer: 10.1-628). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail.

Seminare

Bald ist es so weit: Im Oktober startet unsere Herbst-Seminarserie mit den beiden Zertifizierungsseminaren T.I.S.P. (**15.–19.10.2018**) und T.P.S.S.E. (**22.–25.10.2018**). Im November folgen das PKI-Seminar (**12.–15.11.2018**) und das Seminar IT-Sicherheit heute (**20.–22.11.2018**).

Wir freuen uns, sie in unserem renovierten Seminarbereich begrüßen zu dürfen – und empfehlen insbesondere für das T.I.S.P.-Seminar eine baldige Anmeldung, da uns schon zahlreiche Anmeldungen vorliegen. Programm und Online-Anmeldung unter https://www.secorvo.de/seminare.

Geburtstag

Vor genau 20 Jahren, am 01.09.1998, wurde Secorvo als Beratungsunternehmen für IT-Sicherheit und Datenschutz gegründet – in einer Zeit, in der die Informationstechnik zwar aus vielen Bereichen des (vor allem Wirtschafts-) Lebens schon nicht mehr wegzudenken war, die Beschäftigung mit IT- oder Informationssicherheit aber doch eher bestimmten Branchen wie dem Bankenbereich oder leicht pathologisch veranlagten Menschen vorbehalten schien. Seitdem hat sich die Welt verändert – kaum jemand, den die Themen Informationssicherheit oder Datenschutz heute nicht beträfen.

Diese Entwicklung haben wir über 20 Jahre aktiv begleitet. Fast 200 Ausgaben der Security News sind in dieser Zeit erschienen, unterstützt von rund 98.000 Tassen Kaffee und einem Team von mittlerweile 25 Mitarbeitern. Und wir sind ein wenig stolz auf das uns von unseren Kunden in mehr als 2.000 erfolgreichen Projekten entgegengebrachte Vertrauen. Vielen Dank dafür – und auf hoffentlich viele weitere Jahre so guter Zusammenarbeit.

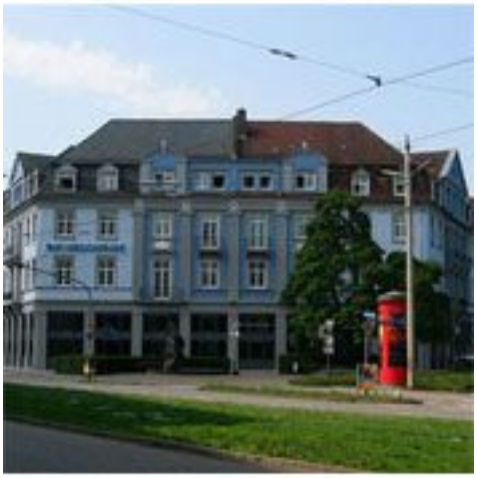
Veranstaltungshinweise

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

September 2018	
04.-05.09.	D•A•CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018 (ULD, Kiel)
13.09.	Digitale Mülltrennung (KA-IT-Si, Karlsruhe)
24.09.	Datenschutztag 2018 (COMPUTAS, Köln)
28.-30.09.	FIfFKon 2018 (FIfF, Berlin)
Oktober 2018	
01.-03.10.	ISSE 2018 (EEMA, Rom/IT)
08.-12.10.	OWASP AppSec USA 2018 (OWASP, San Jose/US)
09.-11.10.	it-sa 2018 (NürnbergMesse, Nürnberg)
15.-19.10.	T.I.S.P. (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. (Secorvo, Karlsruhe)
23.10.	Anwendertag IT-Forensik (Fraunhofer, Darmstadt)
30.10.	Swiss Cyber Storm 2018 (Swiss Cyber Storm Association, Bern/CH)

Fundsache

Der Zentralverband des Deutschen Handwerks bietet mit 10 Tipps eine gute Antwort auf die Frage, was Handwerker für die IT-Sicherheit unternehmen sollten. Darin werden wichtige Schritte beschrieben und gute Hinweise und Empfehlungen in Form von Broschüren oder verlinkten Webseiten gegeben.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Thomas Maus (Editorial).

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

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.

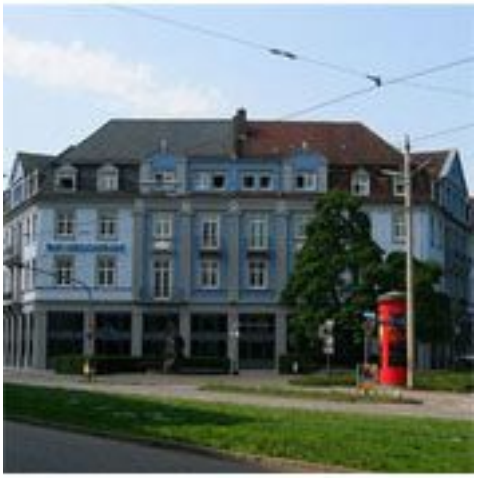
Verordnete IT-Sicherheit

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

secorvo
security consulting

Secorvo Security News

Oktober 2018

Rote Linien

Der Preikestolen ist ein Fels in der Nähe von Stavanger in Norwegen, der über 600 Meter senkrecht bis zum darunter liegenden Fjord abfällt. Hunderttausende besichtigen jährlich dieses Naturwunder. Aber keiner der Besucher, der noch bei Sinnen ist, käme auf die Idee, von dort im Wingsuit hinunter zu springen, ohne über ein gerüttelt Maß an Erfahrung als Fallschirmspringer zu verfügen.

Beim Software-Entwurf sind die roten Linien, die man tunlichst nicht überschreiten sollte, meist nicht ganz so leicht zu erkennen wie die Kante des Preikestolen. Und die möglichen Leidtragenden sind in der Regel die Anwender – und nicht die Entwickler, die die Linie überschreiten. Oft, oder besser: allzu oft verändern Designer einer Anwendung übergreifende Rechteeinstellungen des Systems, hantieren mit hoch privilegierten Benutzern und deren Credentials oder – so wie die in diesen Security News beschriebene Headset-Software – schieben dem System ein Root-Zertifikat unter, dessen Schlüssel sie gleich mit ausliefern. In solchen Fällen sollte man jedoch mindestens zweimal überlegen, ob man nicht auch ans Ziel kommt, ohne diese Linie zu überschreiten.

M M from Switzerland
(CC-BY-SA 2.0)

Wer sich dennoch in derart unsichere Gefilde begibt, der sollte beizeiten Experten für dieses Territorium hinzuziehen, die ein unabhängiges Design-Review durchführen. Zwar kann selbst dann noch etwas schief gehen – so wie leider nur zu oft auch bei Extremsportlern in Wingsuits – aber ohne eigene Erfahrung ist das Risiko unkalkulierbar und ein Scheitern wahrscheinlich.

Und noch etwas können Entwickler von Extremsportlern lernen: Hinter sich aufzuräumen und beim Gehen die Umgebung hinter der roten Linie so zurückzulassen, wie man sie vorgefunden hat.

Inhalt

secorvo
security consulting

Security News

Sennheisers HeadSetup revisited

In den SSN 08/2018 warnten wir vor dem fahrlässigen Umgang der Software Sennheiser HeadSetup mit CA-Zertifikaten. Anschließend analysierten wir einige ältere Versionen der betroffenen Software genauer – und dabei zeigte sich, dass die Schwachstelle gravierender ist als ursprünglich angenommen. Denn mit Informationen aus der Anwendung konnte auch der geheime CA-Schlüssel ausgelesen und missbraucht werden. Als „Proof of Concept" realisierten wir mit der Root-CA einen Man-in-the-Middle-Angriff auf TLS-Verbindungen und hebelten so die HTTPS-Verschlüsselung aus: Die Schwachstelle untergräbt für betroffene Systeme die gesamte zertifikatsbasierte Vertrauensinfrastruktur.

Im Gespräch mit dem Hersteller stellte sich heraus, dass die CA lediglich genutzt wird, um vertrauenswürdige Serverzertifikate für den lokal betriebenen Websocket-Dienst bereitzustellen. Dieser Dienst soll Schnittstellen zwischen Headset und Web-basierten Softphones implementieren. Dafür hätte es jedoch keiner eigenen Root-CA bedurft.

Als sei das noch nicht genug, unterliefen dem Hersteller in seinem Deinstallations- bzw. Update-Programm weitere Fehler: So werden die nicht mehr benötigten CA-Zertifikate nicht aus dem Zertifikatsspeicher von Windows entfernt. Alle Systeme, auf denen irgendwann eine der von der Schwachstelle betroffenen Versionen von HeadSetup installiert war, sind daher weiterhin angreifbar – obwohl jüngere Versionen von HeadSetup mittlerweile eine nicht so einfach zu missbrauchende CA nutzen.

Auch wenn wir die Kopfhörer des Herstellers lieben - ein Beispiel, pars pro toto, für die drastischen Folgen eines unbesonnenen Umgangs mit Credentials und Zertifikaten. Details zur Schwachstelle und Empfehlungen zu Gegenmaßnahmen finden sich in unserem Vulnerability Report zur Schwachstelle CVE-2018-17612.

Gefährliche Abhängigkeiten

Bereits am 19.01.2017 wurde über den offiziellen Twitter-Account von PHP darauf hingewiesen, dass am 31.12.2018 die Versorgung mit Sicherheits-Updates für PHP 5.6 eingestellt wird. Knapp zwei Jahre später verwenden nach den Statistiken von W3Tecs jedoch immer noch 61% aller erfassten Webseiten diese bald nicht mehr unterstützte Version. Abhilfe schafft eine rechtzeitige Migration auf eine neuere PHP-Version – die kann allerdings (zeit-)aufwändig sein.

Derartige Abhängigkeiten von Komponenten stellen vor allem im Bereich von Web-Anwendungen ein steigendes Sicherheitsrisiko dar. In der jüngsten Ausgabe der OWASP Top 10, einer Auflistung der zehn größten Sicherheitsrisiken in Web-Anwendungen, ist die Nutzung verwundbarer Komponenten erstmals in den Risiko-Katalog aufgenommen worden.

Lösungsmöglichkeiten zeigen Projekte wie RetireJS oder OWASP Dependency Check auf, die bei der Erstellung von Anwendungen bei allen Abhängigkeiten (Komponenten, Bibliotheken) prüfen, ob Versionen mit bekannten Schwachstellen verwendet werden. Das Auslaufen des Supports lässt sich allerdings noch nicht automatisiert prüfen.

Gehackte Boxen

Wer sich für die Welt der Hacks und Exploits interessiert, findet in Hackthebox eine neue Herausforderung: ein Übfeld für Hacker-Trainings. Über einen kostenlosen VPN-Zugang können Zielsysteme auf Netzwerkebene untersucht und angegriffen werden. Auch die Pentesting-Experten von Secorvo zerlegen dort regelmäßig Maschinen, testen Tools und vertiefen dabei ihre Fertigkeiten.

Der Dienst steht allen offen, die – als kleine Fingerübung – die Registrierungsseite hacken. Eine klare Empfehlung!

Abofalle „Datenschutzauskunft"

Die Schreiben der selbsternannten „Datenschutzauskunft-Zentrale" schlagen derzeit hohe Wellen in der Presse, Verbraucherschutzzentralen und Datenschützer warnen. Was ist passiert? Die in Malta ansässige „Datenschutzauskunft-Zentrale" fordert Unternehmer per Schreiben auf, sich in das Datenschutzauskunft-Register eintragen zu lassen und bietet verschiedene Dienste an. Wie bereits früher bei den so genannten „Gewerbeauskünften" steckt eine „Abofalle" dahinter: Wer das Formular ausfüllt, unterschreibt und zurücksendet schließt einen Vertrag über einen Eintrag in das Datenschutzauskunft-Register – gegen Entgelt: Es folgt eine Rechnung über mehrere hundert Euro.

Zwar gibt es bereits einstweilige Verfügungen, die der Datenschutzauskunft-Zentrale untersagen, derartige Werbung per Fax zu übersenden. Dennoch: Was tun, wenn man auf die Masche hereingefallen ist und die Betreiber mit Mahnverfahren und gerichtlicher Vollstreckung der Forderung drohen?

Nach Auffassung des Bundesgerichtshofs sind Entgeltklauseln, die derart unauffällig im Gesamtbild

eines Schreibens eingefügt sind und Dienste betreffen, die für gewöhnlich unentgeltlich erbracht werden, überraschend und damit gem. § 305c Abs. 1 BGB nicht Vertragsbestandteil, da der Vertragspartner an dieser Stelle nicht damit rechnet. Daher entsteht mit der Unterschrift keine Zahlungsverpflichtung. Allerdings gibt es bisher im Internet keine derartigen Register (warum auch), deshalb ist offen, ob die Gerichte davon ausgehen werden, dass solche Dienste in einer Vielzahl von Fällen unentgeltlich erbracht werden. Das Tätigwerden externer Datenschutzbeauftragter ist schließlich in der Regel nicht kostenlos. Allein auf das Urteil des BGH sollte man sich daher nicht verlassen, sondern den Vertrag umgehend wegen arglistiger Täuschung anfechten und rechtliche Beratung in Anspruch nehmen.

DSGVO-Abmahnungen

Vor dem Inkrafttreten der DSGVO wurde häufig eine neue „Abmahnwelle" vorhergesagt. Nun ist zu dieser Frage am 13.09.2018 eine erste Entscheidung des LG Würzburg ergangen: Ein Wettbewerber hatte die Datenschutzerklärung einer Webseite, die nicht den Anforderungen der DSGVO genügte, als wettbewerbsrechtlichen Verstoß gegen § 3a UWG abgemahnt und eine einstweilige Verfügung beantragt, die das Landgericht auch erließ.

Von einer Abmahnwelle kann bislang aber noch nicht die Rede sein, auch wenn zu erwarten ist, dass noch viele solcher Entscheidungen folgen werden. Befürchtet werden ähnliche Fallzahlen wie bei fehlerhaften oder fehlenden Widerrufsbelehrungen. Anders als bei der Widerrufserklärung gibt es hier jedoch kein gesetzliches Muster, an dem sich der Anwender orientieren könnte. Daher ist die Gefahr von Fehlern bei Datenschutzerklärungen sogar größer, wenn man nicht die notwendige Sorgfalt walten oder sich diesbezüglich beraten lässt.

Das Bundesministerium für Justiz und Verbraucherschutz hat inzwischen einen Gesetzentwurf veröffentlicht, mit dem ein weiterer Versuch unternommen wird, missbräuchlichen, auf Gewinnerzielung ausgerichteten Abmahnungen einen Riegel vorzuschieben.

Dies soll über eine Beschränkung der Klagebefugnis auf Mitbewerber und Wettbewerbsverbände erfolgen; daneben ist eine Stärkung des Schutzes von Kleinstunternehmen vorgesehen, indem ein Gegenanspruch für den Abgemahnten geschaffen wird und unangemessen hohe Vertragsstrafen keinen Anlass zur Klage begründen – sie müssen in einem angemessenen Verhältnis zum abgemahnten Verstoß und seinen wettbewerbsrechtlichen Folgen stehen, und der Streitwert darf nicht missbräuchlich hoch angesetzt werden.

Die meisten Verbände befürchten, ihre Mitglieder bzw. Verbraucherinnen und Verbraucher würden in ihrem Schutz vor Wettbewerbsverstößen beschnitten und lehnen die Einschränkung der Klagebefugnis daher ab. Begrüßt wird jedoch die Abschaffung der datenschutzrechtlichen Klagebefugnis, da für kleinere und mittlere Unternehmen ein erhöhtes Abmahnungsrisiko bestehe.

Streicht man jedoch die Klagebefugnis wegen Verstößen gegen die DSGVO aus dem Gesetz gegen den unlauteren Wettbewerb (UWG), so dürfte das den Eindruck vermitteln, dass Unternehmen es zumindest aus wettbewerbsrechtlicher Sicht mit dem Datenschutz nicht so genau nehmen müssen. So verleiht man dem Datenschutz kein größeres Gewicht, daher sollte der Gesetzentwurf sich besser darauf beschränken, missbräuchliche Abmahnungen mit Gewinnerzielungsabsicht weiter zu erschweren.

Secorvo News

Secorvo Seminare

Aktuelle Fragen der IT-Sicherheit thematisieren wir im November auf unsrem Seminar IT-Sicherheit heute (**20.–22.11.2018**). Im neuen Jahr haben Sie dann im März die nächste Gelegenheit, sich als T.I.S.P. zu qualifizieren (**25.–29.03.2019**). Wir freuen uns, Sie auf einem unserer Seminare zu begrüßen. 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).

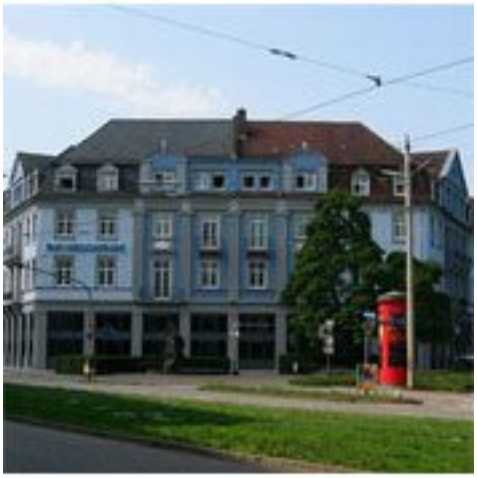
Veranstaltungshinweise

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

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)
27.-28.11.	8. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.-30.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
Dezember 2018	
03.-06.12.	Black Hat Europe 2018 (Blackhat, London/UK)
2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Am 11.10.2018 veröffentlichte das BSI den Bericht zur "Lage der IT-Sicherheit in Deutschland 2018". Darin finden sich – gut dargestellt – zahlreiche Beispiele aufgedeckter Angriffe und konkrete Empfehlungen zum Schutz der eigenen Infrastruktur.



Impressum

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

ISSN 1613-4311

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

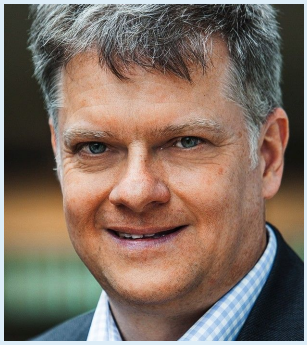
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

November 2018



Ende des Kuschelkurses

Jetzt sind sie da – die ersten DSGVO-Bußgelder. Und tatsächlich: Allen Unkenrufen und wilden Spekulationen zum Trotz, die höchste Bußgelder für Minimalverstöße bei kleinen und mittleren Unternehmen voraussagten, sind sie ein Zeichen von Augenmaß und klarer Kante zugleich.

Während Knuddels nach einem Daten-Leak von Millionen Kundendaten (inklusive Klartext-Passwörtern) als Anerkennung für die unverzügliche Vorfallsmeldung und die enge Kooperation mit der Aufsichtsbehörde bei der Beseitigung der Schwachstellen nur ein moderates Bußgeld in Höhe von 20.000 € auferlegt wurde (siehe den Beitrag in diesen SSN), haben die Aufsichtsbehörden von Großbritannien und den Niederlanden nun den amerikanischen Taxi-Konkurrenten Uber nach einem über ein Jahr geheim gehaltenen Datenschutzvorfall, von dem 57 Millionen Nutzer und Fahrer betroffen waren, mit einem Bußgeld von insgesamt mehr als einer Million Euro belegt.

Die Fälle zeigen dreierlei: So werden gerade aus den zahnlosen Tigern, die die Datenschutzaufsichtsbehörden mit ihren übersichtlichen maximalen Bußgeldern bislang waren, einflussreiche Mitspieler bei der Durchsetzung eines sicherheitssensiblen Umgangs mit personenbezogenen Daten. Dabei konzentrieren sich die Aufsichtsbehörden zweitens, wie von Experten erhofft, mit ihren Bußgeldbescheiden auf tatsächlich materiell relevante Vorfälle – und sanktionieren nicht bürokratische Nachlässigkeit, wie vielfach befürchtet wurde. Und sie senden drittens ein wichtiges Signal in alle Welt: Wer in einem der größten Binnenmärkte Geschäfte mit europäischen Bürgern macht, hat sich an europäisches Datenschutzrecht zu halten – und das gilt, wie der Europäische Gerichtshof schon 2014 deutlich gemacht hat, auch für amerikanische Anbieter. Google, Amazon, Facebook & Co. werden das in Bälde zu spüren bekommen. Womöglich bricht gerade ein neues Datenschutzzeitalter an – „Post Privacy" jedenfalls war gestern.

Inhalt

secorvo
security consulting

Security News

Erstes DSGVO-Bußgeld

Bußgelder im Rahmen der DSGVO waren vor Inkrafttreten Zündstoff für hitzige Diskussionen. Es wurde erwartet, dass angesichts des Strafrahmens (maximal 10 bis 20 Mio. € bzw. 2-4% des weltweiten Gesamtumsatzes) hohe, wenn nicht sogar sehr hohe Strafen zur Abschreckung verhängt werden.

Im Fall des Daten-Leaks bei Knuddels, bei dem Millionen Nutzerdaten (inklusive Klartext-Passwörter) abgezogen wurden, wurde nun der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg tätig und verhängte das erste DSGVO-Bußgeld in Höhe von 20.000 € - eine entgegen den Erwartungen moderate Bußgeldhöhe. Doch der Landesdatenschutzbeauftragte begründet die Entscheidung klar und gut nachvollziehbar: Für ihn sei ausschlaggebend, wie sich ein Unternehmen im Falle eines Datenschutzvorfalls verhält. Die Reaktion von Knuddels – umgehende Information aller Betroffenen, zügige Meldung an die Aufsichtsbehörde und Kooperation mit den zuständigen Stellen – sei in dieser Hinsicht vorbildlich gewesen.

Die moderate Höhe des Bußgelds sollte daher nicht als Einladung zu einem nachlässigen Umgang mit Datenschutzbelangen missverstanden werden. Das gilt vor allem, wenn Passwörter und IDs von Nutzern betroffen sind – schließlich handelt es sich dabei um besonders schützenswerte Daten. Daraus folgt vor allem, dass diese sicher gespeichert werden müssen, beispielsweise als Hashwert – jedenfalls unter keinen Umständen im Klartext.

In jüngster Vergangenheit zeigte sich allerdings, dass auch einige andere Plattformbetreiber es mit der Passwortsicherheit nicht so genau nehmen. Mitte des Jahres blamierte sich T-Mobile Österreich auf Twitter, und dann schaffte es Instagram sogar, Passwörter durch ein DSGVO-Tool abfließen zu lassen. Kandidaten für höhere Bußgeldbescheide gibt es also bereits.

DSGVO-Services

Die Datenschutz-Grundverordnung hat die Benennung des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) neu eingeführt und die Meldung von Datenschutz-Vorfällen (Art. 37 Abs. 7) deutlich aufgewertet, letztere durch eine enge Frist und erhöhte Sanktionen. Einige Aufsichtsbehörden haben die Sanktionierung bei unterbliebener Benennung bis Anfang 2019 ausgesetzt – vielleicht auch, weil für beide Meldeformen nach wie vor nicht alle Online-Meldeportale funktionsbereit sind.

Es fällt auf, dass gerade die großen Bundesländer hier Defizite aufweisen. Während die Online-Benennung außer in Thüringen überall möglich ist, ist eine Online-Vorfallsmeldung (neben Thüringen) auch in Brandenburg, Bremen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein nicht verfügbar.

Beinahe alle Bundesländer gehen zudem sehr unterschiedliche Wege bei dem Angebot; teilweise sind die Portale sehr versteckt und schlecht zu finden. Hessen bietet den Versand eines Upload-Links für ein ausgefülltes Vorfallsformular an. In Bayern und NRW ist für die Benennung des Datenschutzbeauftragten zudem eine vorherige Registrierung des Verantwortlichen erforderlich. Eine Benennung für mehrere Verantwortliche in einem Online-Formular ist durchweg nicht möglich, entgegen Art. 37 Abs. 2 DSGVO.

Bei der Meldung eines Vorfalls kann durchaus eine fallspezifische Vorlage sinnvoll sein, doch gerade wenn für Unternehmensgruppen die Benennungen vorzunehmen sind, sind die vorhandenen Erschwernisse durchaus ärgerlich – da hinkt die Praxis dem Vereinheitlichungsgedanken der DSGVO noch deutlich hinterher.

Autopsy

Seit dem 09.11.2018 ist die erheblich verbesserte Version 4.9.1 des kostenfreien forensischen Werkzeugs Autopsy verfügbar und läuft nun bei hoher Last mit vielen Falldaten noch einmal deutlich stabiler. Sehr hilfreich ist die neue Funktion einer zusammengeführten Datenbasis (Central Repository), die validierte und normalisierte Daten fallübergreifend vorhält. Wer bisher dachte, man kann mit Autopsy „nur" Datenträgerforensik durchführen, irrt, denn durch Aktivierung der „Experimental Plugin"-Funktion wird der Zugriff auf den weiterentwickelten Volatility Data Source Processor möglich, so dass Datenträger- und Hauptspeicherartefakte in einer Analyse zusammengeführt werden können.

Beide Funktionen zusammen erlauben eine mächtige Suche nach Gemeinsamkeiten, Querbeziehungen und Datenspuren sowohl für systembezogene als auch systemübergreifende Artefakte. Ein Tool, das in keinem Forensik-Labor fehlen sollte.

HeadSetup – Nachlese

In den SSN 10/2018 berichteten wir bereits über die Schwachstelle CVE-2018-17612 in Sennheisers HeadSetup. Mittlerweile beschäftigten sich auch

das Microsoft Security Advisory (ADV180029) und diverse weitere Medien mit der Schwachstelle.

Anschließend setzen wir uns mit den möglichen Ursachen dieser Schwachstelle auseinander, denn Katastrophen sind meist das Ergebnis einer Verkettung ungünstiger Ereignisse. So handelt es sich im vorliegenden Fall auch nicht um einen reinen Implementierungsfehler; auch bei Design und Architektur wurden gravierende Fehler begangen – die zur Lösung eines allerdings nicht von Sennheiser zu vertretenden Problems in Kauf genommen wurden.

Denn maßgeblich dafür, dass überhaupt eine CA zur Kommunikation mit dem lokalen Dienst zum Einsatz kam, ist der Umgang der Browser mit sogenanntem Mixed-Content – unverschlüsselten Inhalten, die in mittels HTTPS geschützte Seiten eingebunden werden. Mike West aus dem Chrome Security Team wies schon am 29.04.2016 darauf hin, dass unverschlüsselte Inhalte vom lokalen System als vertrauenswürdig angesehen werden sollten, da ansonsten die Anwender veranlasst werden könnten, neue Root-CAs nur zu diesem Zweck zu installieren. Dies führte Mitte 2016 zu einer Änderung des Standards. Trotzdem unterbindet derzeit ein Großteil der Browser (Firefox 63.0.1, Safari, Internet Explorer 11) genau diese Anfragen. Lediglich Google Chrome und in der aktuellen Version auch Microsoft Edge erlauben die unverschlüsselte Kommunikation mit den lokalen Diensten. Dies führt Entwickler, die lediglich die Kompatibilität ihrer Software mit verschiedenen Browsern gewährleisten wollen, auf dünnes Eis.

Ein „Zuviel" an Sicherheit kann auch Unsicherheit verursachen. Um ähnliche Schwachstellen zukünftig auszuschließen müssen die Browser-Hersteller schnellstens ihre Sicherheitsstrategie den Standards anpassen.

Datenschutz-Standardisierung

Am 10.09.2018 veröffentlichte das ULD Schleswig-Holstein neue Module des Standarddatenschutzmodells (SDM). Dabei handelt es sich noch um Entwürfe, zu denen nun Anwender ihre Erfahrungen mitteilen sollen. Die vorgestellten Bausteine betreffen die Themen Aufbewahrung, Planung und Spezifikation, Dokumentation, Protokollierung, Trennung, Löschen und Vernichten sowie Datenschutzmanagement. Das SDM soll eine Blaupause für die Prüfung von Verarbeitungstätigkeiten liefern, die gleichzeitig eine Prüfung der Gestaltungsentscheidungen ermöglicht. Die einzelnen Bausteine enthalten unverbindliche Maßnahmenkataloge, die sich am IT-Grundschutz des BSI und den Maßnahmen der früheren Anlage zu § 9 BDSG aF orientieren.

Ob das SDM in der Praxis die versprochene Erleichterung und den Nachvollziehbarkeitsgewinn liefert, hängt von der inhaltlichen Fortentwicklung der Module ab: Noch deckt das Vorgehen nur einen Teil der Verarbeitungstätigkeitsprüfung ab, die Prüfung der Rechtsgrundlage bleibt bspw. außen vor. Das Vorgehen und die Ausführungen zu den Gewährleistungszielen stellen sich recht kompliziert dar und erfordern erhebliche Datenschutzerfahrung zur Einordnung. Den betrieblichen Datenschutzbeauftragten in Nebentätigkeit dürfte dies überfordern.

Secorvo News

Teamverstärkung

Auch mit Blick auf die große Nachfrage nach unseren Penetrationstests freuen wir uns sehr, dass seit Mitte November Christian Titze unser Team verstärkt. Und Monika Contag hat das Rechnungswesen übernommen. Willkommen im Team!

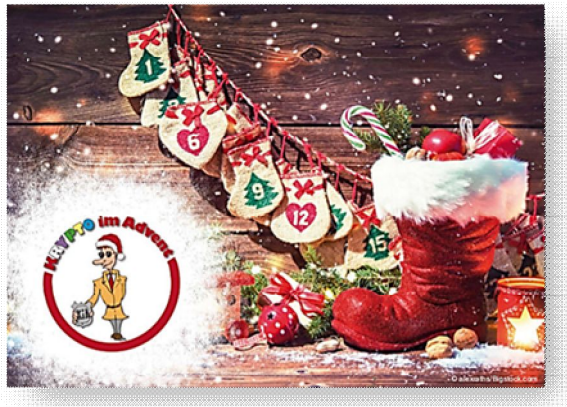
Seminare

Wer seine Weiterbildung 2019 langfristig plant, findet das Seminarangebot, die Termine unserer PKI-, T.I.S.P.- und T.P.S.S.E.-Seminare (alle ab März 2019) sowie die Online-Anmeldung unter www.secorvo.de/seminare.

Krypto im Advent

Am 01.12.2018 startet unser viertes Adventsrätsel „Krypto im Advent" für Schülerinnen und Schüler der Klassen 3 bis 9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Kryptologie. Diesmal gilt es, die entführte Geheimagentin Kryptina wiederzufinden.

Wer alle Rätsel richtig beantwortet, kann einen der zahlreichen von unseren Sponsoren beigesteuerten Preise gewinnen. Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.



Veranstaltungshinweise

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

Dezember 2018	
03.-06.12.	Black Hat Europe 2018 (Blackhat, London/UK)
27.-30.12.	35C3 – 35. Chaos Communication Congress 2018 (Messe Leipzig, Leipzig)
Januar 2019	
18.-20.01.	ShmooCon 2019 (The Shmoo Group, Washington/US)
21.-23.01.	Omnisecure 2019 (in TIME berlin, Berlin)
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)
März 2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-21.02.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Der Beuth Verlag hat das Taschenbuch 408 zum Informationssicherheitsmanagement herausgegeben. Es enthält acht Normen aus der ISO270xx-Familie sowie die DIN 66398 und ist mit € 180 sogar günstiger als je zwei der enthaltenen Normen zum Einzelpreis. Ein Weihnachts-Schnäppchen...

Impressum

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

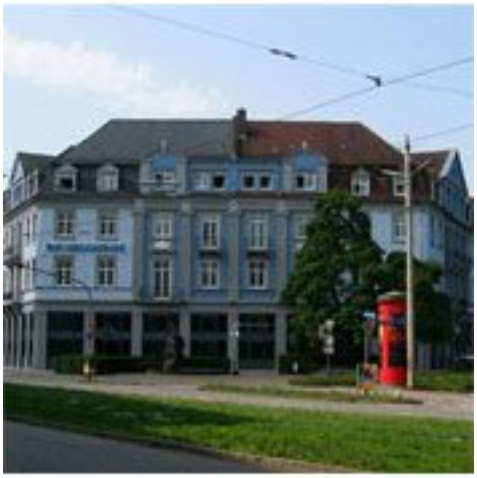
ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, Michael Knopp, Friederike Schellhas-Mende, Jochen Schlichting

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“)

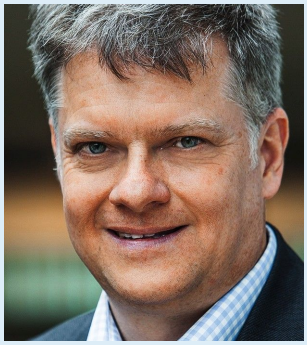
Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de



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).

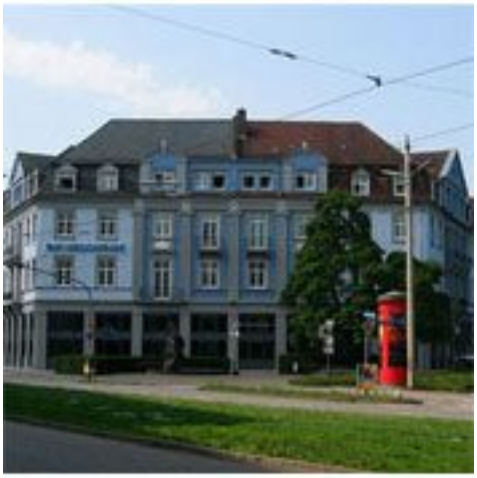
Veranstaltungshinweise

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