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