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