secorvo
security consulting

Secorvo Security News

Januar 2017

Wie wirklich ist die Wirklichkeit?

Vor vierzig Jahren veröffentlichte Paul Watzlawick (1921-2007) sein wegweisendes Werk über die Relativität menschlicher Wahrnehmung. Darin belegt er überzeugend, dass unsere Weltsicht nie objektiv, sondern das Ergebnis von Kommunikation und (subjektiver) Interpretation ist. Neben kulturellen und sozialen Prägungen spielen dabei auch Phänomene wie sich selbst erfüllende Prophezeiungen eine Rolle. So wird unsere Wahrnehmung durch unsere eigene Weltsicht gefiltert: Konforme Erfahrungen werden als Beleg, widersprechende als die Regel bestätigende Ausnahme interpretiert.

Diese Einsicht müsste uns eigentlich skeptisch gegenüber unseren eigenen und tolerant gegenüber den Überzeugungen anderer stimmen. Stattdessen treibt uns eine unerschütterliche Wahrheitssehnsucht dazu, meist wenige Beispiele als Beweis für allgemeine Urteile zu akzeptieren: „Schau' Dir das einmal an. Da sieht man mal wieder, dass ...". Dabei dürfte nicht nur Mathematikern klar sein, dass man die Aussage „Jede Zahl ist eine Primzahl" nicht dadurch beweisen kann, dass man 3, 5, 7 und 11 als Beleg heranzieht.

In der von Blogs, Twitter und Facebook geprägten Meinungsöffentlichkeit finden wir heute unzählige solcher Belege für jedes unserer (Vor-)Urteile, die darüber zu Gewissheiten reifen. Darunter sind auch zahlreiche Falschbehauptungen („4 ist eine Primzahl"), die ebenfalls die eine oder andere Weltsicht zur Wahrheit veredeln. Keine guten Voraussetzungen für Selbstbescheidung und Toleranz.

Da passt es, dass Sprachlog.de am 31.01.2017 „Fake News" zum Anglizismus des Jahres 2016 gekürt hat. Würden wir wenigstens nur solche Behauptungen als „möglicherweise wahr" akzeptieren, deren Herkunft belegt ist, würden es „stille Post" und gezielte Falschmeldungen schwerer haben. Wäre das nicht mal eine wirklich großartige Aufgabe für digitale Signaturen?

Inhalt

secorvo
security consulting

Security News

Datenbank als Geisel

Im vergangenen Jahr machte Ransomware einen Großteil der Neuinfektionen mit Schadsoftware aus. Nach und nach erweiterten die Angreifer ihren Fokus und nahmen Unternehmen (vor allem deren Personalabteilungen) mit individualisierten E-Mails ins Visier. Jüngster Trend: Seit Anfang Januar sind über das Internet erreichbare mongoDB-Datenbanken von Verschlüsselungsangriffen betroffen. Eine neue Angriffswelle vom 12.01.2017 zielt dabei auf Installationen der Suchmaschine Elasticsearch. Die Angreifer verschlüsseln die Datenbankinhalte und fordern Lösegeld in Bitcoins. Nach Analysen des Sicherheitsforschers Niall Merrigan sind ihnen schon zehntausende Installationen zum Opfer gefallen.

Schutz vor den Angriffen bietet das Blockieren des Internet-Zugriffs auf die Datenbank. Außerdem sollten die Empfehlungen der Hersteller zur Zugriffskontrolle und sicheren Konfiguration umgesetzt werden. Und wie bei anderer Ransomware gilt auch hier: Regelmäßige Backups ermöglichen die Wiederherstellung der Daten, falls es doch zu einer Infektion kommen sollte.

Überfällige Regulierung

Die IT-Dienstleister von Berufsgeheimnisträgern wie Ärzten und Rechtsanwälten hadern schon lange mit der Strafbarkeit des (in der Praxis nicht auszuschließenden) Einblicks in die von ihnen verarbeiteten geheimen Daten. Nach Jahrzehnten der Rechtsunsicherheit hat sich nun die Bundesregierung mit einem Referentenentwurf vom 15.12.2016 der Überarbeitung des § 203 StGB angenommen.

Die Begründung des Entwurfs belegt (ohne es auszusprechen), dass sich die Mehrheit der Berufsgeheimnisträger seit Jahren durch die Inanspruchnahme von IT-Dienstleistungen strafbar macht. Die Gesetzesänderung sieht nun vor, dass der bisherige Gehilfenkreis um erforderliche Mitwirkende erweitert wird; dem Geheimnisträger fällt die Aufgabe zu, die Mitwirkenden sorgfältig auszuwählen, zu überwachen und zum Schweigen zu verpflichten.

Der insgesamt sehr zu begrüßende Entwurf benötigt sicher noch die eine oder andere Anpassung: So ist der Einsatz von Unterauftragnehmern nicht in § 203 StGB, wohl aber in der geplanten Rechtsanwaltsordnung erwähnt. Auch die Beauftragung einer juristischen Person scheint bezüglich der zu verpflichtenden Personen noch nicht zu Ende gedacht. Wenig überzeugend ist es auch, die korrespondierenden Zeugnisverweigerungsrechte erst in einem gesonderten Gesetz regeln zu wollen. Schließlich könnte das Kriterium der Erforderlichkeit erneut für Rechtsunsicherheit sorgen.

Volatility 2.6

Das Forensik-Framework Volatility ist nach 14 Monaten kontinuierlicher Weiterentwicklung seit dem 27.12.2016 nun als Release 2.6 verfügbar. Das bewährte Werkzeug für die Speicherforensik der Betriebssysteme Windows, Linux, Android und iOS hat viele neue und sinnvolle Funktionen für den Praktiker erhalten. Dazu zählen insbesondere die Unterstützung der aktuellen Versionen von Windows 10, Windows Server 2016 und KASLR Linux, deren neue Kernelstrukturen es schon längere Zeit deutlich erschwerten, spezifische Informationen aus dem Hauptspeicher zu analysieren.

Der standardisierte Funktionsumfang ist ebenfalls stark angewachsen. Inzwischen umfasst er 111 Windows-, 77 Mac- und 71 Linux-Plugins. Gerade für Mac und Linux sind viele Plugins mit den Schwerpunkten Prozesse und Dateien hinzugekommen, mit denen in der Analyse deutlich mehr Einsichten verfügbar sind als zuvor. Für Windows wurde in zahlreichen *dump-Plugins eine "--memory"-Option ergänzt, die es ermöglicht, auch die umliegenden Adressbereiche ausgeführter Prozesse automatisiert zu extrahieren. Das vereinfacht die Lokalisierung aktiven Schadcodes, der sich häufig außerhalb des eigentlichen Prozess-Adressraums befindet.

Die Standardausstattung an Plugins wird durch das Community-Repository fast verdoppelt, und dank ausgiebiger Tests konnte die Robustheit des Werkzeugs erneut gesteigert werden.

Der letzte Vorhang

Bereits am 21.12.2016 hat der EuGH ein neues Urteil zur Vorratsdatenspeicherung gefällt. Nachdem die Richtlinie zur Vorratsdatenspeicherung am 08.04.2014 für nichtig erklärt worden war, wurden jetzt auch die Schranken für nationale Regelungen geklärt. Die Entscheidung misst die allgemeine und unterschiedslose Vorratsdatenspeicherung von Telekommunikationsdaten an Art. 15 der ePrivacy-Richtlinie und an den Artikeln 7 (Achtung des Privatlebens), 8 (Schutz personenbezogener Daten) und 11 (Meinungsfreiheit) der Europäischen Grundrechtecharta. Im Ergebnis wiegen nach Überzeugung des Gerichtshofs die Grundrechte schwerer als Überwachungs- und Ermittlungsinteressen.

Eine Vorratsdatenspeicherung soll wegen des damit erzeugten Eindrucks einer ständigen Überwachung nur bei einem konkreten Bezug zwischen gespeicherten Daten und dem Überwachungsziel möglich sein. Eine allgemeine und unterschiedslose Vorrats-

datenspeicherung sei hingegen nicht zu rechtfertigen. Der Zugriff auf Vorratsdaten darf nur auf Grundlage eines gerichtlichen Beschlusses ermöglicht werden, die Speicherung ist auf das absolut Notwendige zu beschränken. Mit diesem Urteil wird auch die deutsche Neuauflage vom Dezember 2015 hinfällig, denn inhaltliche Beschränkungen der Vorratsdaten sind darin nicht vorgesehen.

Noch eine Verordnung

Die EU-Kommission hat am 10.01.2017 einen weiteren, die Datenschutz-Grundverordnung ergänzenden Verordnungsentwurf „Regulation on Privacy and Electronic Communication" veröffentlicht. Er soll u. a. die e-Privacy-Richtlinie (RL 2002/58/EG) ersetzen und Widerspruchsfreiheit mit der neuen Regelungslage herstellen und ist Teil der Digital Single Market Strategy.

Die Verordnung zielt auf elektronische Kommunikationsdienste, Verzeichnisdienste und auch auf Software-Provider, die elektronische Kommunikationsdienste bedienen, sowie auf das Direkt-Marketing mittels elektronischer Kommunikation und auf Dienstleister, die Daten von Endgeräten sammeln. Sie soll als spezielle Regulierung der Datenschutz-Grundverordnung vorgehen.

Darin wird die Verwendung von Verkehrs- und Nutzungsdaten (außerhalb von technischen und Abrechnungszwecken) weitgehend auf Einwilligungen gestützt. Enthalten sind weiter umfangreiche Informationspflichten, Regelungen für Verzeichnisdiensteanbieter sowie Einwilligungserfordernisse bei Verwendung personenbezogener Daten und Regelungen zum Direkt-Marketing, die den bisherigen § 7 UWG berühren. Die Sanktionen lehnen sich an die Datenschutz-Grundverordnung an.

Gelten soll die Verordnung ab dem 25.05.2018. Sie führt zu tiefgreifenden Änderungen des deutschen Telemedienrechts und enthält eine Reihe neuer Bestimmungen. Für einen sorgfältigen Gesetzgebungsprozess erscheint der Zeitplan ambitioniert.

Secorvo News

Enkeltrick für Fortgeschrittene

Seit einem guten Jahr gehören auch deutsche Unternehmen zu den Opfern der als „CFO Fraud" oder „Fake President Fraud" bekannt gewordenen Social-Engineering-Angriffe. Dabei erhalten gezielt ausgewählte Mitarbeiter mittelständischer oder großer Unternehmen E-Mails und Anrufe, die vermeintlich von der Unternehmensleitung stammen oder von ihr initiiert wurden. Unter der Vortäuschung streng vertraulicher Akquisitionen werden die Mitarbeiter dazu gebracht, große Zahlungen unter Umgehung interner Prozesse auszulösen.

Auf der Jahresauftaktveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) berichten Dr. Boris Hemkemeier und Ronny Wolf von der Commerzbank AG am **02.02.2017** über diese und andere aktuelle Cybercrimeangriffe gegen Unternehmen und zeigen, wie man sich dagegen schützen kann.

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

Ihr Weg zum Zertifikat

In Kürze fällt die „magische Marke" der 1.000 Informationssicherheitsexperten, die ihre Kenntnisse und Erfahrungen mit einem T.I.S.P.-Zertifikat gekrönt haben. Falls auch Sie diesem wachsenden Kreis von Experten angehören möchten, bieten wir Ihnen vom **06. bis 10.03.2017** die Gelegenheit, Ihre Kenntnisse und Erfahrungen zertifizieren zu lassen. Das einwöchige T.I.S.P.-Seminar und das von uns verfasste Begleitbuch bereiten Sie gründlich auf die Prüfung vor.

Auch Absolventen einer T.I.S.P.-Zertifizierung kommen im März auf ihre Kosten: Vom **14. bis 16.03.2017** bietet Ihnen das Seminar „IT-Sicherheit heute" die Gelegenheit, Ihre für die Rezertifizierung erforderliche fachliche Weiterbildung nachzuweisen.

Entwickler und Systemdesigner bereitet das Seminar T.P.S.S.E. (vormals CPSSE) vom **27. bis 30.03. 2017** systematisch auf die Prüfung als zertifizierter Professional für sicheres Software-Engineering vor. Hier erlernen Sie die konkrete Umsetzung von Security by Design in der Praxis. Weitere Seminarangebote und die Möglichkeit zur Anmeldung finden Sie unter www.secorvo.de/seminare.

Save the Date

Informationssicherheit und Datenschutz erfreuen sich seit Jahren wachsender Aufmerksamkeit. Inzwischen fordern Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen in den Mittelpunkt des Interesses.

Was aber bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich der? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Diesen Fragen widmet sich die diesjährige **Secorvention** am **30. und 31.05.2017**. Das Programm finden Sie in Kürze auf unseren Webseiten.

Veranstaltungshinweise

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

Februar 2017	
02.02.	Wenn der Vorstand zweimal klingelt ... (KA-IT-Si, Karlsruhe)
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
15.-16.02.	27. Smart Card Workshop (Fraunhofer SIT, Darmstadt)
März 2017	
06.-10.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, 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

Februar 2017

Die Awareness-Falle

Wie haben wir uns das doch vor 20 Jahren herbeigesehnt: Kaum ein Tag ohne Schlagzeile über einen Security-Vorfall und nur noch wenige Unternehmensleitungen, die dem Thema Informationssicherheit mit Ignoranz begegnen.

Allerdings drohen wir inzwischen diesem Awareness-Erfolg selbst zum Opfer zu fallen. Immer häufiger lotst er Sensibilisierte in eine Fatalismus-Sackgasse: Wenn jedes Kryptoverfahren früher oder später gebrochen und jede Webanwendung geknackt wird – was nützen da noch Schutzmaßnahmen? Warum nicht die Ausgaben sparen und das Beste hoffen?

Nachlässig recherchierte oder mit Halbwissen verfasste Meldungen geben dieser Haltung immer wieder neue Nahrung. Nicht genug damit: Die jüngste Salonfähigkeit von „Fake News" gibt uralten Verschwörungstheorien neuen Aufwind („Tolles Geschäftsmodell: erst Viren(warnungen) verbreiten und dann Virenschutz verkaufen").

Aber die Komplexität der Wirklichkeit ist bekanntlich schwer zu vermitteln. Dabei gleicht die Arbeit eines Sicherheitsbeauftragten der eines Lotsen, der bekannte Untiefen umschifft und für alle unbekannten einen Notfallplan bereithält. Natürlich senkt er mit seiner Expertise Wahrscheinlichkeit und Schadensausmaß einer Havarie – wenn auch er sie nie gänzlich ausschließen kann.

Geht der Lotse seiner Arbeit still und sorgfältig nach, werden mangels Wertschätzung womöglich seine Einflussmöglichkeiten beschnitten oder sein Budget gekürzt. Buhlt er (oder die Öffentlichkeit) umgekehrt zu viel um Aufmerksamkeit für sein Thema, kann ihm dasselbe drohen: Denn wenn wenig passiert, kann das sein Verdienst sein – oder aber der Wirbel um das Thema erscheint übertrieben.

Das richtige Maß zu finden ist im Leben häufiger eine Herausforderung. Helfen kann die Orientierung an Standards und Best Practices: Ruhige Professionalität statt aufregungsgetriebener operativer Hektik wird auch hier auf mittlere Sicht den größeren Nutzen stiften.

Inhalt

secorvo
security consulting

Security News

SHA-1-Kollision

Schon lange war das näher rückende Unwetter am Horizont zu sehen, nun hat der erste Blitz eingeschlagen: Am 23.02.2017 präsentierte eine Gruppe von Forschern des CWI Amsterdam und Google die erste SHA-1-Kollision – zwei PDF Dateien mit gleichem Hashwert. Mit 6.500 CPU-Jahren (oder 110 GPU-Jahren) ist der Aufwand zwar unrealistisch für Massenangriffe, aber immerhin um den Faktor 10^5 schneller als ein „Brute-Force"-Angriff.

Damit ist der SHA-1 nicht komplett gebrochen: Anwendungen, bei denen nur die Einweg-Eigenschaft gefordert ist, sind von dem Angriff nicht betroffen; auch Fingerprints und Signaturen, die nachweislich schon vor längerer Zeit erstellt wurden, sind nicht akut gefährdet. Die Autoren des Angriffs bieten sogar einen File-Tester an, der typische Muster ihres Angriffs erkennt.

Die Normung des SHA-2 und die ersten Angriffe auf den SHA-1 liegen 15 bzw. 12 Jahre zurück. Einen zügigen Wechsel hat behindert, dass der SHA-1 in Standards festgeschrieben war und Systeme in Umlauf gebracht wurden, deren Kryptofunktionen nicht per (Firmware-)Update ausgetauscht werden konnten. Vorausschauende Hersteller sollten gleich zusätzlich den SHA-3 implementieren, damit der nächste Wechsel weniger holperig verläuft.

DSAnpUG-EU

Das Bundeskabinett hat am 01.02.2017 nach einem neuen Anlauf des Bundesministeriums des Inneren ein Datenschutz-Anpassungs- und Umsetzungsgesetz EU beschlossen. Kernstück ist ein an die DS-GVO angepasstes Bundesdatenschutzgesetz (BDSG-E). Nachdem der vorausgegangene Gesetzentwurf sehr unübersichtlich und wiederholungslastig war (SSN 12/2016) hat sich nun Einiges getan: Er wurde unterteilt in die Umsetzung der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für Polizei und Justiz. Ein wichtiger Regelungsgegenstand ist die künftige Aufsichtsstruktur: Die Vertretung im Europäischen Ausschuss übernimmt die Bundesdatenschutzbeauftragte mit einem gewählten Vertreter aus den Bundesländern.

Die §§ 32 ff. BDSG-E enthalten Einschränkungen der Informationspflichten und Betroffenenrechte. Dabei bleibt fraglich, ob diese ausreichend durch Öffnungsklauseln der DS-GVO gedeckt sind. Der Beschäftigtendatenschutz wurde um eine Freiwilligkeitsdefinition zur Einwilligung ergänzt, ansonsten entspricht er im Wesentlichen dem (ursprünglich provisorischen) bisherigen § 32 BDSG. Die Zulässigkeit der Videoüberwachung wird in § 4 BDSG-E massiv ausgedehnt. Daran haben die Aufsichtsbehörden bereits deutliche Kritik geübt.

Immerhin handelt es sich um einen Stand, an dem sich Unternehmen bei der Umsetzung der DS-GVO bereits vorsichtig orientieren können. Als Stärkung des Datenschutzes kann der Gesetzentwurf allerdings kaum gewertet werden.

VPN-Apps im Playstore

Seit Edward Snowdens Veröffentlichungen haben zahlreiche Apps mit VPN-Funktionalität den Weg in Googles Playstore gefunden. Ernüchternd allerdings die Ergebnisse einer Untersuchung von 238 VPN-Apps, die am 15.11.2016 auf der ACM-Konferenz IMC vorgestellt wurde: Danach weisen die meisten der von den Forschern analysierten Apps schwere Mängel auf. So verschlüsseln ganze 18 % den Datenverkehr gar nicht, nur 16 % verschlüsseln IPv6-Pakete und 66 % tunneln keine DNS-Anfragen. Einige verwenden Proxys, um den HTTP-Verkehr zu manipulieren und JavaScript-Code für Werbung oder Tracking in HTTP-Antworten unterzubringen. Andere haben keinen definierten Tunnelendpunkt, sondern leiten die Daten über andere Nutzer in Peer-to-Peer-Netzwerken weiter. Vier der untersuchten Apps brechen sogar den TLS-Verkehr auf.

Beim Einsatz von VPN-Apps muss man sich darüber im Klaren sein, dass das virtuelle Netzwerkinterface vollständig in der Hand des App-Herstellers liegt. Der Betrieb einer VPN-Infrastruktur ist nicht gratis, und dies kompensieren die Betreiber kostenfreier VPNs auch durch den Handel mit Nutzerdaten. Wem es mit dem Schutz der Privatsphäre ernst ist, der sollte nur Apps von Herstellern verwenden, die eine gute Reputation genießen – auch wenn dies mit Kosten verbunden sein sollte.

DIY-Umkopierstation

Am 02.02.2017 veröffentlichte das Computer Incident Response Center Luxembourg Version 2.1 des Projekts CIRCLean, einer Open Source-Lösung zum sicheren Umkopieren von Dokumenten von einem potentiell mit Malware infizierten auf einen vertrauenswürdigen USB-Stick. Die auf einem Raspberry Pi zu installierende Software unterstützt zahlreiche Datei- und Dateisystemformate, die auf der Projektseite aufgelistet sind.

Zur Installation der Umkopierstation genügt es, das Image auf eine SD-Karte zu schreiben, die SD-Karte und den zu kopierenden USB-Stick in den Raspberry Pi einzustecken und die Stromversorgung herzustellen. Auf dem Zielsystem werden die Dateien nach Datenarten (Text, Video, Audio etc.) sortiert abgelegt. Gefährliche Formate erhalten im Dateinamen

die Ergänzung "Dangerous"; dabei werden u. a. komprimierte Dateien auf Zip-Bomben überprüft. Der Abschluss des Kopiervorgangs wird akustisch signalisiert – solange der Raspberry Pi beschäftigt ist, spielt er einen Song aus der mitgelieferten Musiksammlung. Zumindest für das gelegentliche Kopieren von Dateien ist das ein praktikabler Ansatz – sicherlich verträglicher als das generelle Aussperren von USB-Speichermedien und womöglich wirksamer als ein Virenscanner.

Zulässige Videoüberwachung

Der Bayerische Landesbeauftragte für den Datenschutz, Prof. Dr. Petri, hat sich in seinem jüngsten, am 31.01.2017 veröffentlichten 27. Tätigkeitsbericht mit der Videoüberwachung vor allem in problematischen Umgebungen auseinandergesetzt. So fordert er z. B. für den Krankenhausbereich u. a. die Umsetzung einer maximalen Speicherfrist von zehn Tagen; im medizinischen Bereich habe die Aufzeichnung gänzlich zu unterbleiben.

Die umstrittene Frage, ob auf Kameraattrappen auch die datenschutzrechtlichen Bestimmungen anzuwenden sind, befürwortet der Landesbeauftragte unter Verweis auf das Bundesverfassungsgericht. Zudem fordert er als Nachweis für bestehende Gefahren als Überwachungsgrund eine längerfristige Vorfallsdokumentation.

Kameras, die sich selbst nur bei bestimmten Aktionen wie bspw. dem Betätigen eines Öffnungsschalters aktivieren, werden dagegen als regelmäßig unbedenklich eingeschätzt. Allerdings seien Kameras nach Wegfall der Gefährdungslage (z. B. dem Ausbleiben abzuwehrender Schadensfälle) auch wieder abzubauen. Insgesamt belegt der Bericht zahlreiche Fehler bei der Einrichtung von Videoüberwachungen, stellt allerdings – unter Verweis auf die bereit gestellten Schemata und Hilfestellungen des Landesbeauftragten – hohe Anforderungen an die Ausgestaltung.

Metasploit-Erweiterung

Mit der Veröffentlichung der Metasploit Hardware Bridge wurde das bekannte Exploitation Framework am 02.02.2017 um Schnittstellen erweitert, mit denen auch Systeme angegriffen werden können, die nicht über TCP/IP erreichbar sind. Ursprünglich lag der Fokus darauf, eine Schnittstelle zum CAN-Bus zu schaffen, um darüber beispielsweise Abläufe beim Car-Hacking denen „klassischer" Exploits anzunähern. Entstanden ist daraus jedoch eine generische Schnittstelle, die es zukünftig sehr erleichtert, Metasploit um neue Schnittstellen zu erweitern. ZigBee und JTAG werden bereits getestet. Da heute kaum mehr ein Gerät ohne eingebauten Computer und komplexe Software auskommt, ergeben sich so zahlreiche neue Angriffsszenarien, zumal Schnittstellen abseits von TCP/IP vielfach als Angriffsvektor vernachlässigt werden. Aus der Sammlung von Exploits ist mittlerweile ein für Pentester unverzichtbarer Werkzeugkasten mit mächtigen Tools zur Entwicklung von Exploits und Ausnutzung von Schwachstellen geworden.

Secorvo News

Seminare

Für Kurzentschlossene: Vom **14. bis 16.03.2017** geben wir Ihnen auf dem Seminar „IT-Sicherheit heute" einen Überblick über aktuelle Themen der IT-Sicherheit. Ein besonderes Highlight: der „Live Hacking Day" mit der Vorführung verschiedener Angriffsmethoden (Programm und Anmeldung).

Wie sichere Software-Entwicklung professionell funktioniert, zeigt das Seminar „T.P.S.S.E." am **27.-30.03.2017** mit der anschließenden Möglichkeit zur Zertifizierung (Agenda und Anmeldung).

SECORVENTION 2017

Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung fordern immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen verstärkt in den Mittelpunkt des Interesses. Was aber bedeutet beispielsweise eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich das? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen? Diesen Fragen geht die diesjährige SECORVENTION am **30. und 31.05.2017** auf den Grund. Sie findet statt in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen. Das vollständige Programm und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.secorvention.de.

Lass den Bauch entscheiden ...

... oder warum klassische Risikoanalysen in der Informationssicherheit nicht funktionieren: Bei unserem kommenden KA-IT-Si-Event am **23.03.2017** wirft Kai Jendrian (Secorvo) in seinem Vortrag einen tieferen Blick auf die Herausforderungen bei der praktischen Durchführung von Risikoanalysen in der Informationssicherheit. Dabei wird er verbreitete Ansätze gegenüberstellen und Anregungen für eine praxisorientierte Umsetzung gegeben.

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

März 2017	
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
23.03.	No risk, no fun. (KA-IT-Si, Karlsruhe)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Fundsache

Ein Team von Sicherheitsforschern (u. a. von Mozilla und Google) hat die HTTPS-Verbindungen von Security-Software und -Appliances untersucht. Dabei stellten sie fest, dass bei einigen Lösungen Angriffe auf die gesicherten Verbindungen möglich sind.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Dr. Safuat Hamdy, 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

März 2017

Sündenfall

In der Genesis beendet der Biss in die verbotene Frucht vom Baum der Erkenntnis, zu dem sich Adam und Eva verführen lassen, ihr Leben im Paradies. Wie auch immer man diese Szene interpretieren mag – die Strafe folgt dem Verstoß gegen das Verbot auf dem Fuße.

Selbst aus dieser existentiellen Erfahrung hat der Mensch offenbar nichts gelernt, und wird bis heute selten aus Erfahrung klüger. Denn auch die Informatik hat ihren Sündenfall, den sie bis heute nicht korrigiert hat. Die von *John von Neumann* (1903-1957) im Jahr 1945 veröffentlichte Referenzarchitektur für Computer, die auf Ideen *Konrad Zuses* (1910-1995) basierte, gehorchte ebenso wie die konkurrierende Harward-Architektur einem zentralen Grundprinzip: der strikten Trennung von Daten und Programm. Bis heute folgen Prozessorarchitekturen diesem Grundsatz: Befehle stehen in Befehls-, Daten in Datenregistern.

Bei den Betriebssystemen und Anwendungen nahmen es die Entwickler mit dem Prinzip schon bald nicht mehr so genau. Schließlich bereicherte die Makro-Programmiersprache Visual Basic for Applications Microsofts Office-Programme – der Biss in den Apfel: Wer seitdem ein Word-Dokument oder ein Excel-Sheet öffnet, startet zugleich etwaige darin enthaltene Programme oder Skripte.

Anfang der 90er Jahre folge die Strafe: Eine Welle von Makro-Viren verseuchte großflächig ganze PC-Netze. Gelernt haben wir fast nichts daraus: Seit fast 30 Jahren versuchen (nicht nur) Microsoft-Programmierer eifrig, jedes nur denkbare Skript in einem Office-Dokument auszuführen. Damit später niemand mit dem Finger auf sie zeigt, schalten sie Makros standardmäßig ab; klickt der Benutzer auf die Warnung („Inhalt aktivieren“ – klar, will ich doch das Dokument lesen), liegt die Verantwortung bei ihm, wenn anschließend unerwünschte Dinge passieren. Fallen die besonders hässlich aus, runzelt Microsofts Security Officer darob überrascht die Stirn.

Inhalt

secorvo
security consulting

Security News

oldClouds

Am 16.03.2017 warnte das BSI, dass über 20.000 der in Deutschland betriebenen ownCloud- (bzw. Nextcloud-) Instanzen verwundbare Softwareversionen einsetzen, die kritische Sicherheitslücken enthalten. ownCloud wird oft als Alternative zu Dropbox oder ähnlichen Diensten für den vertraulichen Austausch großer Dateien empfohlen. Der Eigenbetrieb birgt allerdings die Herausforderung, die eigene Instanz sicher zu betreiben.

Auch andere Web-Anwendungen (wie Online-Shops oder CMS) werden oft nicht ausreichend gewartet und auf dem aktuellen Stand gehalten. Eine Hilfe dabei sind kostenfreie Dienste zur Prüfung von ownCloud (bzw. Nextcloud) auf bekannte Schwachstellen. Die automatische Installation von Sicherheitsupdates steht jedoch oft im Konflikt mit Schutzmaßnahmen wie dem Entzug von Schreibrechten auf den Verzeichnissen des Webservers. Daher sollte man einen zuverlässigen Dienstleister, der die Anwendung professionell wartet, einem halbherzigen Eigenbetrieb immer vorziehen.

Nicht gehackt = sicher?

Am 26.01.2017 spendierte Mozilla seinem Browser Firefox in Version 51 ein neues Feature: Der Browser warnt nun vor Passwortfeldern, die über eine unsichere HTTP-Verbindung übertragen werden. Der Betreiber einer Nachrichtenseite über die Öl- und Gasindustrie nahm diese Neuerung zum Anlass, am 20.03.2017 einen Fehlerbericht bei Mozilla einzureichen, da die Warnung die Nutzer seiner Seite verunsichere. Er betreibe ein selbstentwickeltes Sicherheitssystem, das in 15 Betriebsjahren kein einziges Mal geknackt worden sei. Diese Aussage nahmen einige Internet-Nutzer zum Anlass, die Seite einmal auf Herz und Nieren zu prüfen. Kurze Zeit später war ein Login nicht mehr möglich – die Benutzerdatenbank war gelöscht worden. Mittlerweile ist die Webseite nicht mehr erreichbar.

Leider ist der Glaube an die eigene Unfehlbarkeit bei der Entwicklung „unknackbarer" Sicherheitssysteme noch immer verbreitet. Oder, um es mit Bruce Schneier zu sagen: Jeder kann ein Sicherheitsystem erfinden, dass so sicher ist, dass er es selbst nicht knacken kann. Unknackbar ist es deshalb noch lange nicht...

Datenschutz an der Grenze

Die Electronic Frontier Foundation veröffentlichte am 07.03.2017 ein Whitepaper zum Datenschutz bei der Einreise in die USA. Laut Regierungsinformationen hat sich die Zahl der Durchsuchungen von Smartphones oder Notebooks 2016 auf knapp 24.000 verfünffacht. Für Berufsgeheimnisträger, aber auch für Reisende mit umfangreichen privaten oder geschäftlichen Daten auf ihren Geräten können solche Kontrollbefugnisse zum Problem werden. Das Papier empfiehlt daher vor Reiseantritt eine Risikoabschätzung, zu der zu beachtende Kriterien vorgeschlagen werden.

Der Rechtsteil erläutert u. a. die zugrunde liegende Ausnahme für Grenzkontrollen von dem vierten Verfassungszusatz, der gegen unverhältnismäßige Durchsuchungen oder Beschlagnahmen schützt. Durch die Ausnahme werden Durchsuchungen ohne richterlichen Beschluss an der Grenze möglich. Das Herausverlangen von Passwörtern wird am fünften Verfassungszusatz gemessen, nach dem niemand gezwungen werden darf sich selbst zu beschuldigen, und die unterschiedlich interpretierte Befugnislage thematisiert. Gewarnt wird vor einer unbeabsichtigten oder voreiligen Einwilligung in die Durchsuchung, da diese die Betroffenen weitgehend schutzlos stellt.

Die Maßnahmenvorschläge beginnen mit dem Löschen vor Reiseantritt und der Warnung vor der Wiederherstellbarkeit. Umfangreich diskutiert wird die verschlüsselte Speicherung über Cloud-Dienste. Eine empfehlenswerte Lektüre für USA-Reisende.

Zertifikatsdesaster

Am 23.03.2017 publizierte der Chrome-Entwickler Ryan Sleevi die Entscheidung des Chrome-Teams, von Symantec ausgestellten Zertifikaten das Vertrauen zu entziehen. In mehreren Fällen hätten die Entwickler seit Mitte Januar insgesamt über 30.000 Zertifikate identifiziert, bei denen Symantec sich bei der Ausstellung nicht an die Grundprinzipien eines seriösen Zertifikatsausstellungsprozesses gehalten habe. Sleevi kündigte an, in Chrome – gestuft nach Browser-Versionen – Symantecs Root-Zertifikate auf „ungültig" zusetzen und damit geschützte Webseiten als „unsicher" zu qualifizieren, beginnend mit Version 64 in neun Monaten.

Die relativ lange Übergangszeit für offensichtlich nicht vertrauenswürdige Zertifikate ist der Tatsache geschuldet, dass (Statistiken von Mozilla zu Folge) etwa 42 % aller Zertifikatsprüfungen Symantec-Zertifikaten zuzuordnen sind, da Symantec inzwischen zahlreiche CAs der ersten Stunde übernommen hat. Derzeit „verhandelt" Symantec noch mit Google. Bleibt es bei der Entscheidung und ziehen die anderen Browseranbieter nach, könnte das erhebliche Erschütterungen auslösen – beim Vertrauen der Nutzer in HTTPS ebenso wie bei den Unternehmen, die dann kurzfristig ihre Zertifikate ersetzen müssen.

Google Analytics

Der Hamburgische Datenschutzbeauftragte hat seine Handreichung zum Einsatz von Google Analytics am 21.02.2017 aktualisiert. Anlass war zum einen die EU-US-Privacy Shield Zertifizierung von Google, zum anderen das Schrems-Urteil des EuGH zur Safe Harbor Entscheidung. Die Handreichung hält nach wie vor einen datenschutzkonformen Betrieb von Google Analytics für möglich, nun gestützt auf die Angemessenheitsentscheidung über den Privacy Shield.

Als Voraussetzungen werden weiterhin die Beschränkung auf pseudonyme Profile, der Hinweis auf das Widerspruchsrecht und dessen technische Umsetzung sowie der Abschluss des von Google zur Verfügung gestellten Auftragsdatenverarbeitungsvertrages genannt. Bei letzterem ist die Nichtigkeit des Verweises auf Safe Harbor zu beachten. Weiter sind die Nutzer durch Verlinkung auf den von Google formulierten Datenschutzhinweis aufzuklären. Besondere Pflichten ergeben sich, wenn Webangebote durch Browser genutzt werden, die den Widerspruch nicht unterstützen. Auch hierfür wird von Google eine Lösung bereitgestellt. Außerdem ist weiter der Programmcode zur Kürzung der IP-Adressen durch Google zu verwenden. Bis Mai 2018 ist damit die Nutzung von Google Analytics rechtssicher möglich. Welche Konsequenzen sich aus der Datenschutzgrundverordnung ergeben lässt die Handreichung leider offen.

Secorvo News

Seminare

Wer beim PKI-Aufbau und –Betrieb nicht in dieselben oder ähnliche Fallen tappen will wie Symantec (siehe oben), dem sei das Seminar „PKI – Grundlagen, Vertiefung, Realisierung“ vom **25. bis 28.04. 2017** ans Herz gelegt. 20 Jahre Erfahrung mit der Konzeption und dem Aufbau von PKIs verstecken sich hinter der ständig aktualisierten Konzeption. Sie werden in Theorie und praktische Umsetzung eingeführt und dürfen selbst „Hand anlegen“. Es gibt nur noch wenige freie Plätze.

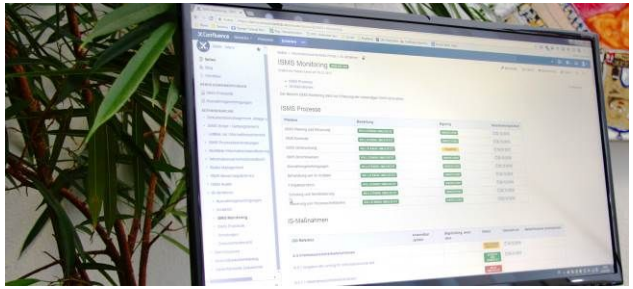
Im Juni bietet sich Ihnen vom **19.–23.06.2017** die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informationssicherheit mit dem T.I.S.P.-Zertifikat zu krönen. Ihre Referenten sind die Autoren des Begleitbuchs zum T.I.S.P., das sie vorab zur Vorbereitung erhalten.

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

ISMS – Ready2Go

Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001:2015 erfordern in der Regel erhebliche Aufwände: ISMS-Prozesse müssen gestaltet und gelebt, die erforderliche Dokumentation erstellt und gepflegt, die Umsetzung von Vorgaben muss überwacht und kontrolliert werden. Nicht zuletzt müssen belastbare Umsetzungsnachweise erbracht werden. Die Erfüllung all dieser Anforderungen stellt insbesondere kleinere und mittlere Unternehmen vor besondere Herausforderungen.

Mit ISMS ready2go bietet Secorvo nun eine Lösung: Anstatt das Rad ständig wieder neu zu erfinden, hat Secorvo Best-Practice-Vorgaben aus über 15 Jahren Erfahrung mit Aufbau und Zertifizierung von ISMS in ein Produkt einfließen lassen, das es Unternehmen erlaubt, mit überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit die Anforderungen und Vorgaben der DIN ISO/IEC 27001 zu erfüllen und eine Zertifizierung effizient vorzubereiten. In Kürze steht die Zertifizierung der beiden ersten Kunden bevor.



Sollten Sie ebenfalls den Aufbau eines ISMS planen, setzen Sie sich gerne mit uns in Verbindung. Und melden Sie sich für die diesjährige SECORVENTION 2017 am **30.+31.05.2017** an.

Software ist sicher.
Und die Erde eine Scheibe.

Das nächste KA-IT-Si-Event am **18.05.2017** nimmt das Thema „Sichere Softwareentwicklung“ in den Fokus: Matthias Honka (asknet AG) wird die wichtigsten Prinzipien für die Softwareentwicklung und das technische Design sicherer Software-Systeme vorstellen.

Wenige einfache Regeln reichen dafür aus – und erschließen sich dem gesunden Menschenverstand. Oft genug jedoch werden sie missachtet, und Produktmanager, Entwickler und Administratoren reißen dadurch Sicherheitslücken.

Im Anschluss an den Vortrag 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 2017	
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)
Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP Foundation, Dubai/AE)
08.-12.05.	OWASP AppSec EU 2017 (OWASP Foundation, Belfast/NIR)
09.-12.05.	European Identity & Cloud Conference 2017 (KuppingerCole Ltd., München)
16.-18.05.	15. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-18.05.	18. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, 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 2017

Moving Targets

Es ist die Königsdisziplin des Jägers: das Erlegen bewegten Wildes, „Bewegungsschießen“ genannt. Kein Auflegen der Waffe, kein ruhiges Zielen auf ein stehendes Tier – sondern Zielen und Schießen direkt aus der Bewegung.

Dabei dürfte sich der Jäger fühlen wie ein CISO: ständig neue, plötzlich auftauchende Ziele (≈ Bedrohungen) und wechselnde Bewegungsmuster (≈ Angriffstechniken) bei durch Bäume verstellter Sicht (≈ unvollständigen Spuren).

Dennoch hat der Jäger dem CISO etwas voraus: Er kann die Bewegungsabläufe am Schießstand üben. Der CISO hingegen ist dem Haken schlagenden Angreifer ausgeliefert: Während dieser seinen Angriff planen und strukturieren kann, ist jener zum Reagieren verdammt. Kein Wunder, dass sich da häufig das Bild eines „Katz‘ und Maus“-Spiels aufdrängt – bei dem der CISO nicht die Katze ist.

Aber stimmt das Bild tatsächlich? Die zahlreichen Berichte über erfolgreiche Angriffe täuschen leicht darüber hinweg, dass die weit überwiegende Mehrzahl der Angriffsversuche gerade nicht erfolgreich ist. Denn oft ist auch für einen Angreifer das Ziel ein *Moving Target*: Ständige Software-Patches und Betriebssystem-Upgrades, Änderungen an der Infrastruktur oder Wechsel des Schutzmechanismus‘ lassen wochenlange Recherchen und Vorbereitungen schnell Makulatur werden. Und auch der Angreifer hat keinen Schießstand – viele IT-Infrastrukturen sind so individuell, dass kein „Standardvorgehen“ zum gewünschten Ziel führt.

Warum machen wir daraus nicht eine Tugend? „Hase und Igel“ statt „Katz‘ und Maus“? Updates und Patches sollten ohnehin selbstverständlich sein – warum also das Ziel nicht auch durch Weiterentwicklungen der Schutzmechanismen „in Bewegung“ halten? Wer genug schnelle Haken schlägt, wird auch den Jäger ermüden. Bis dieser sich auf seinen Hochsitz zurückzieht und sich wieder dem äsenden Schwarzwild zuwendet.

Inhalt

secorvo
security consulting

Security News

Versteckte Open-Source-Software

Am 19.04.2017 veröffentlichte die Firma Black Duck die Open Source Security and Risk Analysis (SSRA) 2017. Der Bericht basiert auf der Analyse von über 1.000 kommerziellen Anwendungen auf die Verwendung quelloffener Software. Bei 96% der untersuchten Anwendungen wurden die Autoren fündig. Dabei interpretiert ein Großteil der Hersteller die Lizenzbedingungen der quelloffenen Komponenten offenbar recht freizügig.

Aus Sicherheitssicht bedenklich ist allerdings, dass in 67% der Anwendungen verwundbare quelloffene Komponenten enthalten sind. Typische Kandidaten sind OpenSSL, jQuery oder Apache Tomcat. Ähnliches gilt für die am 20.04.2017 veröffentlichte Schwachstelle im NVIDIA-Grafikkartentreiber: Die proprietäre Software enthält einen NodeJS-Server, den Angreifer zum Umgehen von Sicherheitsmechanismen nutzen könnten. Das eigentliche Sicherheitsrisiko ist dabei nicht die Open-Source-Software an sich, sondern das unzureichende Schwachstellenmanagement der Softwarehersteller.

Um den Überblick zu behalten, sollten Abhängigkeiten wie Frameworks und Bibliotheken inklusive eingesetzter Versionsstände inventarisiert werden. Da sind die Entwickler in der Pflicht: Unter Rückgriff auf Schwachstellen-Datenbanken könnten sie so rechtzeitig Software-Updates bereitstellen.

Anti-Virus Assisted Attacks

Auf der diesjährigen ASIACCS am 05.04.2017 stellten Forscher der TU Braunschweig und der Universität Göttingen „Anti-Virus Assisted Attacks“ vor. Dabei werden keine Implementierungsfehler in der Antivirensoftware ausgenutzt, sondern die prinzipielle Funktionsweise signaturbasierter Erkennungsverfahren als Angriffsmittel missbraucht. Auf raffinierte Weise gelang es Wressnegger, Freeman, Yamaguchi und Rieck Bytefolgen herauszufinden, auf welche die untersuchten Virenscanner anschlagen. Diese Bytefolgen sind ein Erkennungsmerkmal („Marker“) infizierter Dateien.

Gelingt es nun, diese Bytefolgen in Dateien einzuschleusen, können erhebliche Störungen ausgelöst werden. Werden die Marker beispielsweise als Teil eines Textes oder Headers per E-Mail übermittelt, schlägt ein Virenscanner in der Regel nicht an, da er nur Anhänge prüft. Wird diese E-Mail von einem E-Mail-Client wie Thunderbird in einer Inbox-Datei gespeichert, kann ein lokaler Virenscanner die Inbox-Datei als „infiziert“ klassifizieren und entweder löschen oder in Quarantäne nehmen.

Kennt man den verwendeten Virenscanner, kann die Marker-Wahl auf ein bestimmtes Zielsystem abgestimmt werden. Zwar sind solche gezielten Angriffe mit einem gewissen Aufwand verbunden; auch hilft es, die „Inbox“ des E-Mail-Systems vom Virenscan auszunehmen. Dennoch ist dies ein weiterer überraschender Ansatz, um eine Schutzsoftware für Angriffe zu missbrauchen. Der erwartete Nutzen von Sicherheitslösungen sollte daher immer möglichen neuen Gefährdungen durch die Lösung selbst gegenübergestellt werden.

DSAnpUG-EU

Das Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) wurde am 27.04.2017 vom Bundestag verabschiedet, knapp drei Monate nach Beschluss des Kabinettentwurfs und ein halbes Jahr nach Bekanntwerden des stark kritisierten ersten Entwurfs.

Von den Änderungsvorschlägen des Bundesrats und der Kritik aus der Sachverständigenanhörung aus dem Innenausschuss wurde nur wenig berücksichtigt. Den Bedenken gegenüber den zusätzlichen Ausnahmeregelungen zu den Transparenzpflichten und Betroffenenrechten wurde lediglich durch kleinere Korrekturen Rechnung getragen. Die Einschränkung des Rechts auf Löschung beispielsweise wurde zwar auf analoge Daten beschränkt, ergeht aber immer noch ohne Öffnungsklausel in Art. 17 der DS-GVO.

Immerhin ist das One-Stop-Prinzip der Aufsicht von der europäischen Ebene auf die nationale übertragen worden: auch bei den Landesaufsichtsbehörden bestimmt jetzt die Hauptniederlassung des für die Verarbeitung Verantwortlichen die Zuständigkeit (§ 40 Abs. 2). Ansonsten behält das Gesetz die bisherigen Regelungen zum Beschäftigtendatenschutz, zum Datenschutzbeauftragten oder zum Scoring mit geringen Abweichungen bei.

In einigen für die Praxis und die Umsetzung der DS-GVO wichtigen Punkten herrscht nun Klarheit, etwa bei der Aufsichtsstruktur oder den Datenschutzbeauftragten. Das „neue BDSG“ ist allerdings erkennbar von dem Gedanken getragen, die DS-GVO entgegen den Betroffeneninteressen zu entschärfen. Letztere könnten der rekordverdächtigen Verabschiedungsgeschwindigkeit zum Opfer gefallen sein.

Volatility automatisiert

Volatility, das bewährte Werkzeug der Speicherforensik, lässt nur sehr wenige Wünsche offen. Einer davon ist mit dem am 06.04.2017 veröffent-

lichten robusten Volatize-Script in Erfüllung gegangen. Die kommandozeilenbasierte Ergänzung erlaubt es, mit automatischer Windows-Profilerkennung die wichtigen Aspekte der Bereiche Dump, Plugins, Strings, Timeline, VAD und Yarascan ohne weitere Interaktion für ein Hauptspeicherabbild abzuarbeiten.

Sehr hilfreich ist die automatische Erstellung der zentralen .volatilityrc-Konfigurationsdatei, die zeitsparende Umgebungsvariablen z. B. bei den Plugin-Aufrufen bereitstellt, und die dann von Volatility via Volatize für Performancesteigerungen von 30%-40% genutzt werden kann. Erzeugt man z. B. für eine große Zahl an Hauptspeicherabbildern vorab alle .volatilityrc-Konfigurationsdateien und skriptet den Volatize-Aufruf, kann man über den Playbook-Modus spezifische Datendumps direkt an die Virustotal-API übergeben.

Da Volatize quellcodeoffen ist, lassen sich damit auch Playbooks für spezifische Incident-Szenarien erstellen. In Kombination mit der yarascan-Option kann über eine große Anzahl von konvertierten hiberfil.sys-Hauptspeicherauslagerungsdateien mit der Signaturregel zur Equation Group vom 20.04. 2017 die Historie analysiert werden. Welches Unternehmen wüsste nicht gerne, ob es schon einmal Opfer eines erfolgreichen Angriffs war?

Vorbeigefahren

Bereits am 30.03.2017 hat der Bundestag das Gesetz zur Änderung des Straßenverkehrsgesetzes beschlossen. Ziel des Gesetzes ist es, einen gesetzlichen Rahmen für den Einsatz automatisierter Systeme in Fahrzeugen zu schaffen. Das Gesetz konzentriert sich zunächst auf die Regelung der Verantwortung, Sanktionen und Pflichten der Fahrzeugführer.

Bereits der Bundesrat hatte darauf hingewiesen, dass Verbraucherinteressen nicht ausreichend berücksichtigt, die Zulassungsvoraussetzungen für die Systeme nicht konkretisiert und dass vor allem Sicherheitsanforderungen bezüglich möglicher Angriffe von außen nicht geregelt würden.

Geregelt wurden dagegen Datenschutzfragen der Aufzeichnungen im Fahrzeug. Zwar wurde die Löschfrist von drei Jahren auf ein halbes Jahr verkürzt; dennoch blieben umfangreiche Zugriffsbefugnisse der Verkehrsbehörden bestehen. Der Schutz der Daten vor unbefugtem Zugriff, die diesbezügliche Verantwortung, eine ausreichende grundsätzliche Zweckbeschränkung und der erlaubte Umfang der Datenerhebung wurden dagegen nicht geregelt.

Insgesamt verfehlt das Gesetz das Ziel, einen verlässlichen Rahmen zu schaffen, da es letztlich nur einen Teil des Regelungsbedarfs aufgreift. Daher würde es nicht überraschen, wenn der Bundesrat nun den Vermittlungsausschuss anriefe.

Secorvo News

Secorvo Seminare

Vom **19. bis 23.06.2017** bieten wir Ihnen die nächste Möglichkeit, Ihre Kenntnisse und Erfahrungen in der Informations- und IT-Sicherheit mit einem T.I.S.P.-Zertifikat zu krönen. Zur Vorbereitung auf das einwöchige Intensivseminar mit anschließender Zertifizierung erhalten Sie vorab das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Sollte Ihnen eine Teilnahme an diesem Termin nicht möglich sein, bieten sich Ihnen am **25.** bis **29.09.2017** und am **27.11.** bis **01.12.2017** zwei weitere Gelegenheiten.

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

SECORVENTION 2017

Was bedeutet eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden - und lohnt sich dieser? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen?

Antworten auf diese und ähnliche Fragen gibt es auf der SECORVENTION am **30.** und **31.05.2017** in der Buhlschen Mühle in Ettlingen. Das vollständige Programm finden Sie auf unserer Webseite www.secorvention.de.

9. Tag der IT-Sicherheit

Der „Karlsruher Tag der IT-Sicherheit“, eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative mit der IHK Karlsruhe und dem Cyber-Forum e.V., beschäftigt sich in diesem Jahr zum neunten Mal mit aktuellen Herausforderungen der IT-Sicherheit für Unternehmen. Als Keynote-Speaker konnten wir Herrn Dr. Stefan Brink, den frisch gekürten Landesbeauftragten für den Datenschutz in Baden-Württemberg gewinnen. Fachvorträge behandeln die Themen Risikomanagement, Aufbau eines DIN ISO 27001 orientierten ISMS und Social Engineering. Schließlich zeichnet das BSI ein aktuelles Lagebild der Cybersicherheit.

Gelegenheit zum fachlichen Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern gibt es am Buffet. Die Veranstaltung findet statt am **28.06.2017** im Saal Baden der IHK Karlsruhe. 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

Mai 2017	
03.-04.05.	OWASP Middle East Cyber Security Conference 2017 (OWASP, Dubai/AE)
04.05.	BvD Verbandstag 2017 (BvD, Berlin)
08.-12.05.	OWASP AppSec EU 2017 (OWASP, Belfast/NIR)
09.-12.05.	European Identity & Cloud Conference 2017 (KuppingerCole Ltd., München)
16.-18.05.	15. Deutscher IT-Sicherheitskongress (BSI, Bonn)
17.-18.05.	18. Datenschutzkongress (EUROFORUM, Berlin)
22.-24.05.	Entwicklertag 2017 (VKSI, GI, ObjektForum, Karlsruhe)
30.-31.05.	SECORVENTION (Secorvo, Ettlingen)
Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.06.	9. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)

Fundsache

Am 26.04.2017 veröffentlichte das SEI CERT (Software Engineering Institute der Carnegie Mellon University) eine sehr umfassende Liste von C++ Secure Coding Standards.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, 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

Mai 2017

Fragile IT-Sicherheit

Am 13.05.2017 wirbelte der Kryptotrojaner ‚WannaCry' die IT weltweit durcheinander. Von oft reißerischen Presseberichten getrieben beschäftigte der Vorfall Security-Verantwortliche auf der ganzen Welt. Mit etwas Abstand können wir heute den Fall genauer unter die Lupe nehmen: Was können wir daraus lernen?

WannaCry war weder ein besonders neuartiger noch ein besonders gut gemachter Angriff – im Gegenteil: Die Autoren machten Fehler, die frühere Kryptotrojaner schon nicht mehr enthielten. Eine Neuerung war die Verwendung eines der von der NSA gesammelten Exploits, die im April von Hackern veröffentlicht worden waren. So verbreitete sich der Trojaner sowohl via E-Mail (und die Schwachstelle Mensch) als auch über eine Wurmkomponente, die alle erreichbaren Rechner attackierte, die die vom Exploit ausgenutzte Windows-Schwachstelle aufwiesen. Wie andere Kryptotrojaner verschlüsselte er alle Dateien, auf die der betroffene Nutzer oder Rechner Zugriff hatte.

Vor derartiger Schadsoftware schützen nur aufeinander abgestimmte präventive und Schaden begrenzende Maßnahmen wirkungsvoll. Der Virenschutz hilft, bekannte Schädlinge aus dem Netz und vom Rechner fernhalten – gegen neue Schadsoftware hilft er selten. Daher gilt es, Benutzer zu sensibilisieren – und für den Fall der Fälle den Schaden einzudämmen und die Verbreitung zu begrenzen. Eine restriktive Berechtigungsvergabe und systematische Netzwerksegmentierung tragen ebenso dazu bei wie ein funktionierendes Backup- und Recovery-Konzept, ein sorgfältiges Patch-Management und der professionelle Umgang mit Vorfällen.

Das Zauberwort zur sinnvollen Abstimmung von Schutzmaßnahmen heißt übrigens Informationssicherheitsmanagement. Kombinierte Angriffe wie WannaCry werden zukünftig der Standard sein. Daher sollte man WannaCry als Weckruf verstehen, das eigene ISMS einmal auf den Prüfstand zu stellen.

Inhalt

secorvo
security consulting

Security News

Virus per Virenscanner

Im Schatten der allgemeinen Aufregung über die Schadsoftware WannaCry wurde im Mai eine kritische Schwachstelle in Microsofts Defender entdeckt: Am 05.05.2017 publizierte Travis Ormandy via Tweet die Entdeckung der gefährlichsten Windows-Schwachstelle seit langem. Sie steckte in der NScript-Komponente des Windows Defender, die mit erhöhten Rechten und ohne Sandbox-Mechanismen dynamische Analysen von JavaScript-Code durchführt, und lässt sich mit wenigen Zeilen JavaScript-Code beispielsweise in einer Website, E-Mail oder Datei platzieren. Der Angreifer kann darüber das komplette System übernehmen. Betroffen sind die meisten Windows-Versionen, allerdings ist die Ausnutzung bei neueren Versionen (Windows 10 und 8.1) durch zusätzliche Schutzmechanismen erschwert. Microsoft reagierte schnell und lieferte am 08.05.2017 ein Update aus, das die Schwachstelle behebt. Keine acht Tage später fanden Google-Forscher am 16.05.2017 via Fuzzing die nächste kritische Schwachstelle im Defender – für die Microsoft am 25.05.2017 einen Bugfix außerhalb des Update-Zyklus' lieferte.

Da signaturbasierte Ansätze heute praktisch wirkungslos sind, setzen Virenscanner verstärkt auf die dynamische Analyse von Inhalten. Dabei werden die Daten interpretiert oder ausgeführt. Solche Analysen sind riskant, denn wie bei jeder anderen Software muss man auch hier mit Schwachstellen rechnen – dank erhöhter Rechte und fehlendem Sandboxing eine heikle Angelegenheit. Daher ist die Frage berechtigt, ob Virenscanner inzwischen nicht mehr schaden als nützen.

Sichere Passwörter revisited

Am 02.05.2017 beendete das National Institute of Standards and Technology (NIST) die Diskussion des Entwurfs der Richtlinie für Digitale Identitäten. (NIST Special Publication 800-63B). Bemerkenswert sind der Wegfall der Empfehlung von Komplexitätsvorgaben und die Verankerung der Sicherheit von Passwörtern vor allem an deren Länge.

Die Begründung des Standards deckt sich mit unseren Erfahrungen – schon seit 2009 weisen wir auf Fehlsteuerungen durch die gängigen Hinweise zur Gestaltung von Passwörtern hin.

Anfängerfehler

Intels Active Management Technology ist ein Fernwartungsverfahren mit Webinterface. Mitte Februar 2017 wurde darin eine Sicherheitslücke entdeckt, die es einem Angreifer ermöglicht, damit ausgestattete Geräte fernzusteuern. Die besondere Brisanz dieser Schwachstelle liegt in der Möglichkeit, die Authentifizierung als Administrator zu umgehen.

Am 05.05.2017 wurden weitere Details öffentlich. Ursache war ein Fehler, dem ein Ehrenplatz in Lehrbüchern für Softwaresicherheit gebührt: Für den Vergleich zweier MD5-Hashwerte verwendeten die Programmierer die C-Funktion `strncmp()` – und übergaben als String-Länge die Angabe des Clients. Behauptete dieser, die Länge sei null, lieferte der Vergleich – Sie ahnen es – als Ergebnis „ok". Dabei ist der Fehler spätestens seit der Entdeckung des OpenSSL-Bugs Heartbleed im April 2014 (SSN 4/2014) ein Klassiker: Ein Server darf sich nie ungeprüft auf (nicht authentisierte) Längenangaben des Clients verlassen.

Interessenkollision

Am 05.05.2017 ist das Videoüberwachungsverbesserungsgesetz in Kraft getreten, das § 6b BDSG für die Überwachung öffentlich zugänglicher großflächiger Anlagen oder von Fahrzeugen und Einrichtungen des öffentlichen Personenverkehrs um eine Vorgabe für die Abwägung zwischen Betroffenen- und Überwachungsinteressen ergänzt: Der Schutz von Leben, Gesundheit oder Freiheit von Personen im Überwachungsbereich gilt danach als besonders wichtiges Interesse.

Der so entstandene § 6b BDSG ist auch bereits in dem (nun ebenfalls verabschiedeten) Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG) enthalten. Ausdrückliches Ziel ist es, die Sicherheit der Bevölkerung präventiv zu erhöhen, auch durch private Videoüberwachung.

Dass es sich hierbei um eine geeignete Maßnahme handelt wird von Aufsichtsbehörden und Datenschützern bezweifelt. Auf die Einordnung in das System der Datenschutz-Grundverordnung, etwa das Verhältnis zur hierfür verlangten Datenschutz-Folgenabschätzung oder die herangezogene Öffnungsklausel, wird im DSAnpUG nicht eingegangen.

Für Unternehmen, die ihr Gelände oder ihr Hausrecht durch eine Videoüberwachung schützen möchten, ändert sich durch das Gesetz wenig. Die Abwägungsvorgabe ist jedoch eine weitere Abwertung der Betroffeneninteressen. Ungeachtet der Intention ist die Bezugnahme auf Leben, Gesundheit und Freiheit jedoch paradox, denn auch die informationelle Selbstbestimmung ist ein Freiheitsgrundrecht. Daher wäre der Formulierung nach auch dem Betroffeneninteresse, unbeobachtet zu bleiben, besonderes Gewicht beizumessen.

secorvo
security consulting

Phishing mit Unicode-Domains

Namen von Unicode-Domains können so gewählt werden, dass eine gefälschte URL visuell praktisch nicht vom Original unterschieden werden kann – eine Steilvorlage für Phisher. Neu ist das nicht, aber durchaus unterhaltsam – siehe den Blogeintrag von Xudong Xheng vom 14.04.2017. Danach zeigt der Firefox-Browser mit Standardeinstellungen die URL apple.com (bitte mit Firefox öffnen) mit grünem Schloss-Symbol an. Nur wer sich das Zertifikat genauer ansieht (wofür eigentlich kein Anlass besteht) wird erkennen, dass die Website eigentlich www.xn--80ak6aa92e.com heißt.

Gegen solche Angriffe hilft, URLs „vertrauter" Domains manuell oder via Symbolleiste auszuwählen und nicht auf angebotene Links zu klicken. Alternativ setze man in den erweiterten Einstellungen (`about:config`) von Firefox den Parameter `network.IDN_show_punycode` auf `true`: Die URL wird dann als „echte" Adresse angezeigt. Die aktuelle Version 58 des Chrome-Browsers ist für solche Unicode-Angriffe nicht (mehr) anfällig.

Secorvo News

PKI-Policy-Rahmenwerk

Im Mai 2017 wurde das – in einer ersten Fassung bereits 2007 veröffentlichte – Secorvo White Paper zum Policy Rahmenwerk einer PKI überarbeitet und auf einen aktuellen Stand gebracht. Es enthält praxiserprobte und konkrete Hinweise zur Gestaltung von *Certificate Policies* (CP), *Certification Practice Statements* (CPS) und *PKI Disclosure Statements* (PDS). Im Anhang ist zusätzlich die deutsche Übersetzung des Gliederungsrahmens für eine PKI-Policy nach RFC 3647 enthalten.

Zertifizieren Sie Ihr Know-how

Kurzentschlossene können sich noch einen Platz auf dem nächsten T.I.S.P.-Seminar vom **19. bis 23.06.2017** sichern. Im Anschluss können Sie Ihre Fachkenntnisse und Erfahrungen in der Informationssicherheit zertifizieren lassen. Zur Vorbereitung erhalten Sie gleich nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit" zugesandt. Programm, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

9. Tag der IT-Sicherheit

Auf dem neunten 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 aufgezeigt und Präventionsmöglichkeiten vorgestellt. Diesjähriger Keynote-Speaker ist Dr. Stefan Brink, Landesbeauftragter für den Datenschutz in Baden-Württemberg. Anschließend behandeln Fachvorträge die Themen Risikomanagement, Aufbau eines an der DIN ISO/IEC 27001 orientierten ISMS und Social Engineering.

Die Veranstaltung findet am **28.06.2017** 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.

ISMS für alle

Wie viel kostet ein DIN ISO/IEC 27001-konformes Sicherheitsmanagement-System? Die (realistische) Antwort auf diese Frage hat schon die eine oder andere Geschäftsleitung erblassen lassen. Die Etablierung eines wirksamen Risiko-Managements und die Definition der für die systematische Organisation der Informationssicherheit erforderlichen Rollen, Regelwerke, Prozesse, Berichte und Dokumentationen – auch als Nachweise für eine Zertifizierung – sind unvermeidlich mit Aufwand verbunden.

Dabei unterscheiden sich ISM-Systeme in der Praxis meist nur geringfügig – Prozesse, Dokumentationen und oft sogar Regelwerke gleichen sich sogar über Branchengrenzen hinweg. Warum also das Rad jedes Mal neu erfinden?

Aus unseren über 15 Jahren Erfahrung mit dem Aufbau und der Zertifizierung von ISM-Systemen haben wir ISMS ready2go entwickelt – eine Lösung, die die Einführung eines ISMS mit sehr überschaubarem Aufwand und geringen Anpassungen in sehr kurzer Zeit ermöglicht und den Anforderungen und Vorgaben der DIN ISO/IEC 27001 genügt. Die ersten Kunden äußern sich begeistert. Zwei Beispiele:

„ISMS ready2go folgt dem Need-2-Have-Prinzip: Mehr braucht es nicht, weniger auch nicht. Ein übersichtliches, individuell anpassbares und schlankes CMS, der ideale Begleiter für Ihr ISMS-Projekt."
(Detlef Pouw, Stiftung Kirchliches Rechenzentrum Südwestdeutschland)

„Automatische Auswertungen auf Knopfdruck, ein hierarchischer Workflow, so haben wir unser Risikomanagement sicher im Griff!"
(Markus Hotz, 3iMedia GmbH).

Sollten Sie ebenfalls am Aufbau eines ISMS arbeiten, setzen Sie sich gerne mit uns in Verbindung.

Veranstaltungshinweise

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

Juni 2017	
07.-08.06.	Annual Privacy Forum 2017 (ENISA, EC DG Connect, Universität Wien, Wien/AT)
19.-23.06.	Audit Challenge 2017 (ARC Institute, Frankfurt)
19.-23.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.06.	9. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
19.-20.07.	DuD 2017 (COMPUTAS, Berlin)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)

Fundsache

Ein Forscherteam der Universität Braunschweig um Konrad Rieck fand in mehr als 200 Android-Apps Ultraschall-Seitenkanäle zum „Cross Device Tracking“ (SSN 01/2016). Eine (nicht nur) für Datenschützer beunruhigende Entwicklung – auch wenn sich die Zahl der betroffenen Apps mit 0,015% (noch) deutlich unterhalb der Relevanzschwelle bewegt.

Impressum

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

ISSN 1613-4311

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

Juni 2017

In der Matrix

Der Wirtschaftsnobelpreisträger Daniel Kahnemann („Schnelles Denken – Langsames Denken“) hat nicht nur dem Bild des rationalen „homo oeconomicus“ den Todesstoß versetzt, sondern deutlich gemacht, dass unsere vermeintlich vernünftigen Entscheidungen allzu oft das Ergebnis „kognitiver Verzerrungen“ sind: Wir schätzen Risiken falsch ein, werden von irrelevanten Relationen abgelenkt und lassen uns durch „Anker“ z. B. bei Käufen auf Preise festlegen.

Zwar sind uns solche Wirkungen grundsätzlich vertraut: Wir kennen den Trick der Lebensmittelläden, neben der Kasse Schokolade in Kinderaugenhöhe zu platzieren. Wir wissen aus Blindtests, dass Marken unser Geschmacksempfinden beeinflussen. Und uns ist klar, dass die „Wird-oft-zusammen-gekauft“-Vorschläge des Online-Shops nicht philanthrop gemeint sind, sondern der Umsatzmaximierung dienen. Dennoch bilden wir uns ein, auf diese Einflüsse souverän zu reagieren – schließlich können wir auch anders entscheiden.

Unter der Oberfläche ist die Technik dank Big Data aber schon viel weiter. Shops lernen, ab welchem prozentualen Preisnachlass wir zugreifen, sie können aus unserem Einkaufsverhalten prognostizieren, wann wir in Spendierlaune sind, und passen ihre Angebote an unsere IT-Umgebung an: Für Mac-Nutzer ist das Leben meist teurer. Google-Remarketing sorgt für individualisierte Online-Anzeigen, die sich aus früheren Seitenbesuchen ableiten – da kann auch mal ein Shop dabei sein, der uns an einen abgebrochenen Kaufvorgang erinnert. Die virtuelle Welt wird bereits für uns zurechtgebastelt.

Und jetzt kommt die Wirklichkeit an die Reihe: Plakatwände, die uns wiedererkennen und die Werbung anpassen oder Läden, die unser Surfverhalten am WLAN-Hotspot auswerten und Preisvergleiche unterbinden, sind nicht mehr fern. Alles anonym, natürlich, und somit kein Datenschutzproblem.

Heimlich, still und unbemerkt sind wir auf dem Weg in die Matrix.

Inhalt

secorvo
security consulting

Security News

Blackout real

Pünktlich zum fünfjährigen Jubiläum des Bestsellers Blackout haben Sicherheitsexperten von ESET am 12.06.2017 die detaillierte Analyse einer Schadsoftware veröffentlicht, die sie „Industroyer" getauft haben. Die Autoren spekulieren, dass die Software für den weitreichenden Stromausfall in Kiew am 17.12.2016 verantwortlich war – die technischen Fähigkeiten dafür besitzt sie offenbar. Die auf 17 Seiten dokumentierten technischen Details machen deutlich, dass es Angreifer gibt, die sich mit viel Know-how und Ressourcen industriellen Zielen widmen. Die dort verbreiteten Protokolle IEC 101 und IEC 104 sind zwei der Angriffspunkte, die über dynamisch aktivierbare Module attackiert werden.

Die erschreckende Vision von Marc Elsberg ist leider wohl (noch immer) näher an der Realität als Mancher es wahrhaben möchte. Für Betreiber von KRITIS-Infrastrukturen ist eine Absicherung nach dem Stand der Technik im Sinne des IT-SiG spätestens jetzt überfällig.

Spyware as a Service

Am 09.06.2017 erschienen erste Berichte zu einer neuen Spyware, die es auf Macs abgesehen hat. Das Besondere daran: Sie wird über das Darknet als Service verkauft. Gegen eine Gebühr von 30 Bitcoins (derzeit etwa 75.000 €) kann man den Service als Franchisenehmer weiterverkaufen. Die Spyware ermöglicht einem Angreifer, Bildschirmfotos, Umgebungsgeräusche und Tastaturanschläge aufzuzeichnen, Browserdaten auszulesen, iCloud-Fotos zu kopieren und die Zwischenablage zu sichern. Seit dem 15.06.2017 erkennen die gängigen Antivirenprogramme die Schadsoftware. Etwa zum gleichen Zeitpunkt erschien mit MacRansom ein Kryptotrojaner „as a Service" für MacOS.

Aufgrund seiner wachsenden Verbreitung zieht MacOS immer mehr Aufmerksamkeit von Hackern und Kriminellen auf sich. „Macs sind sicher" – so einfach ist die Welt mittlerweile nicht mehr.

Kritische Infrastrukturen, Teil 2

Das Bundeskabinett hat am 31.05.2017 den Referentenentwurf für den zweiten Korb der Verordnung zur Bestimmung Kritischer Infrastrukturen verabschiedet. Damit wird in Kürze auch für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr feststehen, welche Betreiber den Regelungen für Kritische Infrastrukturen unterfallen.

Die Änderungsverordnung bedarf keiner Zustimmung des Bundesrats, so dass noch im Juni mit einer Veröffentlichung im Bundesgesetzblatt gerechnet werden kann. Die nun erfassten Betreiber haben anschließend ein halbes Jahr Zeit, ihre Kontaktstelle für Meldungen (§ 8b Abs. 3 BSIG) einzurichten und zwei Jahre, um die nach § 8a BSIG geforderten Sicherheitsmaßnahmen umzusetzen.

Die Änderungsverordnung ergänzt zudem die bereits erlassenen Anhänge und Kataloge um Definitionen der Anlagen und passt einige Schwellenwerte an. Auch bei den neuen Sektoren wird die Kritikalität nach Versorgungs- oder Kapazitätsschwellenwerten festgestellt.

Während das Finanz- und Versicherungswesen bereits heute einer vergleichsweise strengen Regulierung in Sachen IT-Sicherheit unterliegt, kommen auf die Gesundheitsbranche und die Transport- und Verkehrsbetriebe vielfach neue Anforderungen zu, die bei den betroffenen Unternehmen und Einrichtungen für erheblichen Beratungs- und Dokumentationsbedarf sorgen werden.

Anonymes Internet 3.0

Wie werden Surfer im Internet identifiziert? Früher (und manchmal noch heute) geschah dies mit Hilfe von Cookies oder der IP-Adresse. Aber auch wer Cookies vermeidet und über mobile Netze surft, kann über weitere Merkmale identifiziert werden. Durch eine Korrelation der über den Browser zugänglichen Informationen wie Browserversion, Betriebssystem oder die installierten Plugins kann ein Benutzer „wiedergefunden" werden.

Wer dies vermeiden möchte, verwendet dedizierte Browser für einen anonymeren Zugang wie den am 07.06.2017 in Version 7.0 veröffentlichten Tor-Browser. Darin wird eine Identifikation des Nutzers durch Härtung des Browsers hinsichtlich der preisgegebenen Informationen erschwert und die Analyse der Internetnutzung durch Verwendung des Tor-Netzwerks verhindert. Wem dieses Maß an Privatheit noch nicht reicht, dem sei nahegelegt, sich die Mitte Juni angekündigte runderneute Version von Tails anzusehen. Tails 3.0 bietet eine - in der Regel von einem USB-Stick gestartete – Plattform an, welche ebenfalls das Tor-Netzwerk und den Tor-Browser nutzt. Durch die Nutzung dieser allgemeinen Plattform und Vermeidung individueller Informationen wird eine persönliche Zuordnung des Nutzers weiter erschwert.

OpenVPN erwischt

Wieder hat es ein Open-Source-Produkt erwischt: Am 21.06.2017 gab Guido Vranken in seinem Blog die Entdeckung von vier schwerwiegenden Sicherheitsschwächen bekannt – die zuvor von zwei un-

abhängigen Sicherheitsaudits nicht entdeckt und durch ein Code-Hardening nicht beseitigt worden waren. Aufdecken konnte er die Fehler durch Fuzzing, eine bereits 1989 entwickelte Analysemethode, der wir inzwischen die Entdeckung zahlreicher Bugs in unterschiedlichsten Anwendungen verdanken. OpenVPN-Nutzer sollten umgehend auf die Versionen 2.3.17 bzw. 2.4.3 wechseln.

Der Fall macht deutlich, dass eine Standardisierung der Methoden zur Code-Auditierung überfällig sind: zu häufig blieben kritische Schwachstellen unentdeckt, obwohl Verfahren zu deren Aufspürung existieren.

Grenzwertiges Marketing

Bereits am 30.05.2017 wurde Amazon ein Patent für ein von Miles J. Ward entwickeltes Verfahren erteilt, mit dem der Einzelhandel einen Internet-Preisvergleich der Kunden über das Laden-WLAN registrieren und unterbinden kann. Zwar muss man in Europa vorläufig nicht mit dem Einsatz dieser Lösung rechnen: Eine Sperrung des Zugriffs auf Vergleichsportale und andere Anbieter über das WLAN-Angebot ist rechtlich zulässig, nicht aber eine Auswertung der WLAN-Nutzung – das wäre ein rechtswidriger Eingriff in das Telekommunikationsgeheimnis.

Derzeit testen die Deutsche Post in rund 100 und Real in 40 Filialen im Rahmen eines Feldversuchs eine vom Fraunhofer-Institut in Erlangen entwickelte Analysesoftware, mit der sich die Inhalte von Werbetafeln über eine Auswertung von Videoaufzeichnungen der Betrachter steuern lassen. Dabei bestimmt die integrierte Gesichtserkennung Alter, Geschlecht und Verweildauer des Kunden.

Die Rechtmäßigkeit dieser Videoanalysen wurde vom Bayerischen Landesamt für Datenschutzaufsicht bestätigt. Auf die Videoüberwachung werde hingewiesen, und die Analyse erhebe keine personenbezogenen Daten.

Die beiden Beispiele zeigen, dass die Grenzen des datenschutzrechtlich Erlaubten nicht nur in der Online-Werbung sondern auch bei Ladenbesuchen zunehmend ausgereizt werden. Bei den Videoanalysen mit Gesichtserkennung treffen dabei durchaus plausible Anonymisierungskonzepte auf das Problem mangelnder Transparenz und Vertrauenswürdigkeit. Dabei wird zweifellos bei den Betroffenen ein Überwachungsdruck erzeugt, dessen datenschutzrechtliche Berücksichtigung allerdings umstritten ist.

Diskrete Anpassung

Weitgehend unbeachtet von der Öffentlichkeit treibt der Gesetzgeber die Anpassung des Datenschutzrechts an die Europäische Datenschutz-Grundverordnung voran. Die jüngsten Änderungen von immerhin 12 Gesetzen verstecken sich in einem am 01.06.2017 verabschiedeten Artikelgesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften.

Darin behandelt werden vor allem Betroffenenrechte in Bezug auf öffentliche Register, bspw. das Handelsregister, das Patent- und Markenregister oder das Register vergriffener Werke, sowie die Verarbeitung von Daten durch die Finanzbehörden (Änderungen der AO). Hier ist besonders die Regelung zur Auftragsdatenverarbeitung von Steuerdaten hervorzuheben: Die hier vorgenommenen strengen Einschränkungen bilden einen Gegensatz zu den Planungen bzgl. der Dienstleister anderer Berufsgeheimnisträger. Beschränkt werden das Auskunftsrecht, Mitteilungspflichten gegenüber dem Betroffenen und Berichtigungsansprüche.

Bei den vorgenommenen Beschränkungen kann sich der Gesetzgeber auf Art. 23 DSGVO stützen. Dieser lässt allerdings Einschränkungen der Betroffenenrechte nur zu spezifischen Zielen im öffentlichen Interesse zu, nicht zur Aufwandsbegrenzung der Behörden. Zudem gibt Abs. 2 Kompensationen vor. Hier hat der Gesetzgeber den Gestaltungsspielraum der DSGVO womöglich überschritten.

Secorvo News

Secorvo Seminare

Nach dem T.I.S.P. ist vor dem T.I.S.P. – gerade erst haben sich zwölf Teilnehmer unseres T.I.S.P.-Seminars erfolgreich auf die Zertifizierung vorbereitet, und schon läuft die Vorbereitung des nächsten T.I.S.P.-Seminars vom **25. bis 29.09.2017**. Die Sommerpause ist die beste Zeit zur Vorbereitung: Nach Ihrer Anmeldung erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ zugesandt. Die letzte Gelegenheit zur T.I.S.P.-Zertifizierung im Jahr 2017 bieten wir Ihnen vom **27.11. bis 01.12.2017**.

Für unser PKI-Seminar vom **06. bis 09.10.2017** gibt es bereits zahlreiche Anmeldungen, daher empfehlen wir allen Interessenten an einem vertieften Einblick in Public Key Infrastrukturen eine baldige Buchung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

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

Juli 2017	
03.-05.07.	EssoS 2017 – International Symposium on Engineering Secure Software and Systems (EssoS, Bonn)
12.-14.07.	SOAPS 2017 – 13th Symposium on Usable Privacy and Security (USENIX, Santa Clara/US)
18.-21.07.	PETS 2017 – 17th Privacy Enhancing Technologies Symposium (Univ. of Minnesota, Minneapolis/US)
26.-27.07.	Blackhat USA 2017 (Blackhat, Las Vegas/US)
27.-30.07.	DEF CON 25 (DEFCON, Las Vegas/US)
August 2017	
06.-09.08.	DFRWS USA 2017 - Digital Forensic Research Workshop (DFRWS, Austin/US)
16.-18.08.	26th USENIX Security Symposium (Usenix, Vancouver/BC)
20.-24.08.	Crypto 2017 (IACR, Santa Barbara/US)

Fundsache

Bereits am 18.11.2016 hat die Group Privacy der Deutschen Telekom eine erste Fassung von konzernweit gültigen „Binding Interpretations" der DSGVO verfasst. Das hilfreiche, gut 100 Seiten starke Dokument ist online zugänglich.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Kai Jendrian, 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

Juli 2017

EDA-Daten

Ein beliebter Fehler in Kostenrechnungen sind die übersehenen EDA- (oder „Eh-da“-) Kosten: Fixkosten für Personal, Infrastruktur oder bereits verfügbare IT-Systeme. Sie erzeugen keine unmittelbaren Kosten – sind (oder waren) aber natürlich irgendwann einmal fällig. Würde man sie konsequent berücksichtigen, wären zahlreiche Projekte und Maßnahmen erheblich teurer als kalkuliert, und viele davon unwirtschaftlich. Genau deshalb sind sie bei Projektleitern so beliebt wie bei Controllern verhasst: Wer EDA-Kosten geschickt zu verstecken weiß, kann die Durchsetzung eines Lieblingsprojekts mit Wirtschaftlichkeitsargumenten forcieren.

Was dem Controller die EDA-Kosten sind dem Datenschützer die EDA-Daten: Mit jeder neuen Anwendung fallen sie an. Meist sind es Log-Daten, die ursprünglich zur Fehlersuche dienten. Für viele dieser Daten lassen sich zahlreiche andere Nutzungen finden: Verknüpft man Login- und Logout-Zeiten eines Administrators mit seinen Urlaubszeiten, lassen sich Unregelmäßigkeiten entdecken; leitet man aus den E-Mail-Logfiles die Intensität von Kommunikationsbeziehungen ab, kommt man womöglich Insidergeschäften auf die Spur.

Aber die Begehrlichkeiten machen bei Compliance- und Sicherheitsanwendungen nicht halt. Gewöhnt haben wir uns an die Auswertung unseres Online-Verhaltens, auch wenn uns vielleicht nicht klar ist, was diese Spuren alles enthüllen: Schon wenige hundert Likes erlauben Kaufprognosen, die so zuverlässig sind wie die Einschätzung unseres Lebenspartners. Auch Microsoft hat die Möglichkeiten der EDA-Daten entdeckt und bietet in Office 365 einen Dienst zur Analyse des Mitarbeiterverhaltens. Und der Hersteller des Mäh- und Staubsaugerroboters iRobot, Roomba, deutete kürzlich an, er wolle die über Wohnungen und Grundstücke erhobenen Daten verwerten.

Dabei gibt es – anders als bei EDA-Kosten – ein sehr einfaches und probates Mittel gegen EDA-Daten: Löschen.

Inhalt

secorvo
security consulting

Security News

WhatsApp illegal

Das Amtsgericht Bad Hersfeld hat sich in einem unterhaltsamen Sorgerechtsbeschluss vom 20.03. 2017 detailliert zur Legalität der Nutzung von WhatsApp geäußert und die Eltern zum Einholen von Einwilligungen aller im Adressbuch des Sohnes geführten Personen oder zur Deinstallation verpflichtet. Daneben stellte es eine Pflicht der Eltern zur Aneignung digitaler Kompetenz fest.

Der 12-jährige Sohn hatte vorgetragen, sein Vater habe ihn „auf WhatsApp blockiert". Das Gericht sah sich daraufhin veranlasst, Anordnungen zur Abwehr von Gefahren für das Kind zu treffen. Durch den Upload des Adressbuchs zur – nach den Geschäftsbedingungen – undefinierten weiteren Nutzung durch WhatsApp werde das Recht auf informationelle Selbstbestimmung (!) der geführten Personen verletzt, wodurch der Sohn möglichen Abmahnungen und Unterlassungsbegehren nach § 823 BGB ausgesetzt sein könne. Eine genauere Betrachtung der Rechtsgrundlagen des BDSG und der Verantwortlichkeiten erfolgte allerdings nicht.

Dass der Upload des Adressbuchs unter Vorbehalt undefinierter Nutzungszwecke rechtlich problematisch ist, ist zutreffend und führt zu Recht auch zu entsprechenden Warnungen bzgl. der WhatsApp-Nutzung im Unternehmensumfeld. Die hier verlangte Einwilligung kann dies allerdings mangels Bestimmtheit nicht heilen. Für das private Umfeld ist die Begründung des Amtsgerichts schlicht unzureichend. Als Beleg für die (durchaus vertretbare) Rechtswidrigkeit der WhatsApp-Nutzung ist das Urteil trotz seines klaren Tenors deshalb leider gänzlich ungeeignet.

Trau, schau, wem!

Die NSA hat Ende Juni die Liste ihrer Tools, die im Rahmen des NSA Technology Transfer Program (TTP) der Open Source Community zugänglich gemacht wurden, aktualisiert. Die Liste umfasst mehr als 30 Einträge, darunter WELM, GRASSMARLIN, SHB und LOCKLEVEL.

WELM extrahiert die in Windows Binaries eingebetteten Definitionen für Windows Event-Log-Einträge und konvertiert diese in besser auswertbare Formate wie JSON oder CSV. Um die Topologien von ICS- (*Industrial Control System*) bzw. SCADA- (*Supervisory Control and Data Acquisition*) Netzwerken zu analysieren, kann auf GRASSMARLIN zurückgegriffen werden. SHB (*Secure Host Baseline*) oder LOCKLEVEL beschäftigen sich mit der Härtung von Windows-Betriebssystemen.

Die Tools erfüllen den vorgesehenen Zweck – dennoch ist ein gesundes Misstrauen gegenüber den NSA-Tools zweifellos angebracht.

Schöne neue Arbeitswelt

Microsoft plant Analysetools anzubieten, die es ermöglichen sollen, das Zeitmanagement der Mitarbeiter bspw. bei der E-Mail-Nutzung oder Terminplanung sowie die Ressourcennutzung und Zusammenarbeit zu analysieren und auszuwerten. Workplace Analytics soll als Teil von Office 365 angeboten werden.

Workplace Analytics ist seit dem 05.07.2017 bereits als Add-On für Kunden der O365-Suite verfügbar. Der Deutsche Gewerkschaftsbund hat bereits reagiert und die spätestens durch dieses Angebot eingetretene betriebliche Mitbestimmungspflichtigkeit der O365-Einführung postuliert.

Dass es sich bei diesem Angebot um einen gut überlegten Schritt von Microsoft handelt, darf bezweifelt werden. Mit dem neuen Angebotsbestandteil werden die dem bisherigen Einsatz zugrunde liegenden datenschutzrechtlichen und betriebsverfassungsrechtlichen Erwägungen hinfällig. Unternehmen, die bereits O365 einsetzen, werden ihre Entscheidung nachbessern müssen – mit Blick auf die Mitbestimmung mit ungewissem Ausgang. Aus Datenschutzsicht ist der neue Dienst hinsichtlich der Rechtsgrundlagen und Datenschutzanforderungen kritisch zu prüfen; danach sind mindestens neue Prozesse und Regelungen zum Umgang mit diesem Dienst zu schaffen.

Berufsgeheimnisträger

Am 29.06.2017 hat der Deutsche Bundestag das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen verabschiedet. Das Gesetz beendet die Strafbarkeit der Auslagerung von IT-Dienstleistungen durch Berufsgeheimnisträger, die eintritt, sobald der Dienstleister Einblick in geschützte Daten erhält (§ 203 StGB). Im Ausgleich regelt es Voraussetzungen der Dienstleistereinbindung und das Zeugnisverweigerungsrecht des Dienstleisters (§ 53 StPO-neu).

Die Pflichten des Auftraggebers regelt das Gesetz in Änderungen der einschlägigen Berufsordnungen. Daher profitieren vor allem Ärzte zunächst noch nicht, da hier Landesregelungen angepasst werden müssen. Berufsgeheimnisträger müssen die Möglichkeit des Dienstleisters, auf vertrauliche Daten zuzugreifen, auf das Erforderliche beschränken, den Dienstleister sorgfältig auswählen und in einem schriftlichen Vertrag auf Verschwiegenheit verpflichten.

Die Strafbarkeit der Geheimnisoffenbarung wird auf die mitwirkenden Personen erstreckt; das Versäumen der Verpflichtung wird ebenfalls unter Strafe gestellt. Das Erfordernis von Auftragsdatenverarbeitungen bleibt unberührt.

Das Gesetz schafft eine überfällige Rechtsgrundlage vor allem für die zahlreichen IT-Dienstleistungen, deren Berufsgeheimnisträger bedürfen; diesbezüglich kann es nur begrüßt werden (SSN 1/2017). Der Schutz der Geheimnisse wird jedoch unweigerlich erheblich geschwächt.

Ende der Störerhaftung

Mit dem Dritten Gesetz zur Änderung des Telemediengesetzes hat der Bundestag nach der zaghaften Einschränkung vom 21.07.2016 nun in § 8 Abs. 1 TMG-neu die Haftung auf Schadensersatz oder auf Unterlassung von WLAN-Anbietern für rechtswidriges Nutzerverhalten ausgeschlossen. Das Gesetz wurde am 30.06.2017 verabschiedet, der Bundesrat muss nicht mehr zustimmen.

Mit der Abschaffung reagiert der Gesetzgeber auf das EuGH-Urteil zur WLAN-Haftung vom 15.09.2016. Für WLAN-Anbieter wird durch den Ausschluss der Störerhaftung ein wesentliches Rechtshindernis beseitigt, sodass Internetanschlüsse nun ohne Identifizierungserfordernisse oder Belehrungen der Nutzer Dritten zur Verfügung gestellt werden können. § 7 TMG-neu ermöglicht den Rechteinhabern allerdings, von den Anbietern Sperrungen von Inhalten zu verlangen. Die Kosten einer solchen Anordnung können jedoch nicht mehr dem Anbieter auferlegt werden.

Der Abmahnindustrie wird durch die Neuregelung weiter Boden entzogen. Für Anbieter und Internetnutzer handelt es sich trotz der verbliebenen Sperrthematik um eine lange erwartete gute Nachricht.

Secorvo News

SSN-Jubiläum

Am 04.07.2002 erschien die erste Ausgabe der Secorvo Security News. Seit nunmehr 15 Jahren versorgen wir Sie monatlich mit Hintergrundinformationen und Einschätzungen zu den (nach unserer Bewertung) wichtigsten Security-Ereignissen des jeweiligen Monats. 180 Ausgaben mit insgesamt 720 Seiten – trotz der von uns angestrebten inhaltlichen „Verdichtung“ ein kolossales Werk.

Wir danken Ihnen für Ihre Lese-Treue, mit der Sie dazu beigetragen haben, dass die SSN heute zu den wichtigsten Informationsquellen zur IT- und Informationssicherheit in Deutschland zählen.

Frisches aus der Hackerküche

Nach der Sommerpause werden Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) beim KA-IT-Si-Event am **21.09.2017** zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Anschließend stellen Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

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

Secorvo-Publikationen

Webanwendungen sind eines der beliebtesten Einfallstore von Angreifern. Systematische Analysen und Penetrationstests können oft das Schlimmste verhüten. Wie man dabei vorgehen sollte, stellt Dr. Safuat Hamdy in Ausgabe 04/2017 der iX vor.

Und wer bloggen möchte, aber die Sicherheitsrisiken dynamischer Content-Management-Systeme (CMS) scheut, findet in Ausgabe 08/2017 der iX hilfreiche Hinweise von Kai Jendrian auf Alternativen.

Secorvo-Seminare

Die Sommerpause ist eine perfekte Gelegenheit zur Vorbereitung auf Ihre T.I.S.P.-Zertifizierung: Nach Ihrer Anmeldung für das T.I.S.P.-Seminar vom **27.11. bis 01.12.2017** erhalten Sie das Begleitbuch „Zentrale Bausteine der Informationssicherheit“ von uns.

Für unser PKI-Seminar vom **06. bis 09.10.2017** gibt es bereits zahlreiche Anmeldungen, daher empfehlen wir allen Interessenten an einem vertieften Einblick in Public Key Infrastrukturen eine baldige Buchung.

Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

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

August 2017	
06.-09.08.	DFRWS USA 2017 - Digital Forensic Research Workshop (DFRWS, Austin/US)
16.-18.08.	26th USENIX Security Symposium (Usenix, Vancouver/BC)
20.-24.08.	Crypto 2017 (IACR, Santa Barbara/US)
September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landes-zentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
26.-28.09.	Future Security 2017 (Fraunhofer VVS, Nürnberg)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, 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

August 2017

Neuland

Am 19.06.2013 äußerte Bundeskanzlerin Angela Merkel in einer Pressekonferenz mit Barack Obama, dass das Internet „für uns alle Neuland“ sei – und musste für diese Formulierung viel Hohn und Spott einstecken. Dabei ging ihr Satz weiter: Das Internet „ermöglicht auch Feinden und Gegnern unserer demokratischen Grundordnung mit völlig neuen Möglichkeiten und völlig neuen Herangehensweisen unsere Art zu leben in Gefahr zu bringen.“

Die Äußerung fiel zwar im Kontext der NSA-Überwachung, doch brachte Frau Merkel damit (wenn auch womöglich unwillentlich) eine empfindliche Wahrheit auf den Punkt: Nach wie vor treiben Hersteller mit einer erschütternden Naivität die Digitalisierung ihrer Produkte voran und schaffen mit unausgereiften und offenbar unzureichend getesteten Lösungen gefährliche neue Angriffspunkte.

Solange es sich dabei um via Internet zugängliche Überwachungskameras handelt, mag das noch als handwerkliche Ungeschicklichkeit mit Spaßfaktor durchgehen. Inzwischen erfasst die von Sicherheitsaspekten unbelastete Digitalisierung allerdings immer mehr Produkte, bei denen Angriffe eine unmittelbare Gefahr für Leib und Leben darstellen. Blieb der Angriff auf ein motorisiertes Skateboard noch eher unbeachtet, sorgte die von einem Journalisten im Selbstversuch dokumentierte Attacke auf einen Chrysler Cherokee im Juli 2015 immerhin für etwas Wirbel. Gelernt haben daraus allerdings noch lange nicht alle, wie der am 18.07.2017 bekannt gewordene Angriff auf einen Segway MiniPro zeigt.

Jeder Sicherheitsgurt, jeder Reifen und jede Stoßstange muss einen Sicherheitstest absolvieren. Aber IT-Schnittstellen, bei denen Fehler zu wesentlich dramatischeren Eingriffen in die Fahrzeugsicherheit führen können, dürfen ohne vertiefte Prüfung verbaut werden. Es fehlen sogar anerkannte, standardisierte Testverfahren, mit denen wir solche Systeme verlässlich prüfen könnten. Neuland eben.

Inhalt

secorvo
security consulting

Security News

Wie gut ist mein Passwort?

In den SSN 05/2017 haben wir über die geänderten Empfehlungen des NIST zur Wahl geeigneter Passwörter berichtet. Unter anderem wird empfohlen, Passwörter mit Listen kompromittierter Passwörter abzugleichen. Der Sicherheitsforscher Troy Hunt, bekannt durch die Bereitstellung von Listen gehackter Accounts, bietet seit dem 03.08.2017 die Online-Prüfung von Passwörtern gegen ca. 320 Millionen bekanntermaßen kompromittierter Passwörter an. Sie kann per Formular oder via API erfolgen.

Hunt warnt selbst davor, solche Webdienste mit Passwörtern zu nutzen, die in Gebrauch sind – was den Nutzwert des Angebots deutlich reduziert. Immerhin bietet er die Passwörter auch als SHA1-Hashes zum Download an. Mit etwas Programmierung (Stichwort: binäre Suche) lässt sich damit schnell ein Werkzeug erstellen, mit dem man seine Passwörter lokal überprüfen kann.

Einheitlicher Beschäftigtendatenschutz

Bereits am 08.06.2017 hat die Art. 29 Gruppe unter anderem eine Stellungnahme zum Beschäftigtendatenschutz (WP 249 – Opinion 2/2017 on data processing at work) verabschiedet. Diese aktualisiert die Stellungnahmen WP 48 und 55 aus den Jahren 2001 und 2002, ausgehend noch von der Datenschutzrichtlinie, aber mit Bezug auf die künftige Datenschutz-Grundverordnung und den aktuellen Entwurf der ePrivacy-Verordnung.

Der Beschäftigtendatenschutz wird durch die Öffnungsklausel in Art. 88 DS-GVO den Mitgliedsstaaten zur eigenständigen Regelung überlassen. Die Stellungnahme fasst Verhältnismäßigkeitserwägungen zu typischen Verarbeitungskontexten zusammen. Allgemein werden Anforderungen an die Ausfüllung von Art. 88 DS-GVO formuliert, die deutlich über den deutschen § 26 BDSG-neu (vorher § 32 BDSG) hinausgehen.

Es wird klargestellt, dass Arbeitgeber Arbeitnehmer nicht ausschließlich auf vorgegebene Social-Media-Profile verpflichten können, auch nicht, wenn diese öffentlich das Unternehmen vertreten. Es wird die Erforderlichkeit von Transparenz und dokumentierten Datenschutzrichtlinien bei IT-Nutzungsüberwachungen betont. Bezüglich Mobile Device Management Lösungen wird generell eine Datenschutz-Folgenabschätzung für erforderlich gehalten.

Gesichtserkennungstechnologien im Beschäftigungskontext werden abgelehnt. Für Einwilligungen und berechtigte Interessen des Arbeitgebers als Rechtsgrundlage wird nur ein sehr eingeschränktes Anwendungsfeld gesehen. Die Stellungnahme stellt eine hilfreiche Zusammenfassung und Orientierungshilfe dar, zumal viele aktuelle und praktische Problemstelllungen angesprochen und mit Szenarien erläutert werden.

Meinungswandel

Ob eine juristische Person (bspw. eine Firma) als externer Datenschutzbeauftragter bestellt werden kann, ist eine in der Praxis durchaus relevante, aber bislang umstrittene und nicht entschiedene Frage. Der Hessische Datenschutzbeauftrage empfiehlt nun in einem Informationspapier zum betrieblichen Datenschutzbeauftragten nach der Datenschutz-Grundverordnung vom 29.06.2017, die Bestellung einer juristischen Person bis zu einer endgültigen Klärung durch den Europäischen Datenschutzausschuss mit der zuständigen Aufsichtsbehörde lediglich abzusprechen.

Die sich abzeichnende Kehrtwende der Aufsichtsbehörden zu dieser durch den Gesetzeswortlaut weiter offenen Frage geht auf ein bereits im Dezember 2016 veröffentlichtes Arbeitspapier (WP 243) der Art. 29 Datenschutzgruppe zurück. Die Europäischen Aufsichtsbehörden halten darin die Bestellung einer juristischen Person ausdrücklich für möglich. Voraussetzung ist, dass die für die juristische Person handelnden Mitarbeiter die Qualifikationsvoraussetzungen erfüllen. Dabei wird ausdrücklich anerkannt, dass die Kombination der Qualifikationen mehrerer Einzelpersonen einer Firma die Wirksamkeit der Tätigkeit in der Praxis steigern kann.

Auch wenn eine endgültige Anerkennung des Modells noch abzuwarten bleibt, öffnet sich damit der Weg für eine praxistauglichere Bestellpraxis, die die bisherigen mühsamen Konstrukte zur persönlichen Bestellung externer Datenschutzbeauftragte überflüssig macht. Bisherige Appelle in diese Richtung waren bislang bei den Aufsichtsbehörden eher auf Ablehnung gestoßen.

Suricata extended

Bereits am 27.07.2017 erschien das robuste Network Intrusion Detection/Prevention/Security Monitoring System Suricata nach ca. 18 Monaten in der Version 4.0.0-stable. Eine wesentliche Neuerung ist die Integration der Programmiersprache RUST, dank der neben deutlich gesteigerter Geschwindigkeit auch eine sicherere Speicherverwaltung und Threats ohne Race Conditions möglich wurden.

Technisch neu sind bei TLS die Dekodierung und das Logging von STARTTLS für SMTP und FTP sowie von

TLS Session Resumptions. Hinzugekommen ist die Unterstützung für das NFS-Protokoll, welches im kommerziellen Umfeld nach wie vor eine wichtige Rolle spielt. Hinzugekommen ist mit der Implementierung des Extensible Event Format (EVE) die Möglichkeit, bei gekapseltem Netzwerkverkehr (encapsulated traffic) auch die innere und äußere IP-Adresse inklusive der zugehörigen Ports auszuwerten.

Alexas lokale Überwachung

Am 01.08.2017 stellte Mark Barnes einen Angriff auf Amazons Echo vor, der das Gerät in eine Abhörstation verwandelt. Auf der Unterseite des Geräts kann über die dortige Kontaktleiste eine SD-Karte angeschlossen werden, mit der das Gerät gebootet werden kann. Anschließend lassen sich über geeignete Skripte das interne Laufwerk ansprechen und die Firmware modifizieren. Auf diesem Weg ist es beispielsweise möglich, Mikrofon-Aufzeichnungen von Echo unbemerkt an einen Dritten zu übermitteln.

Auch wenn Barnes' Angriff nur für bis 2016 verkaufte Geräte nachweislich funktioniert und in neueren Geräten ab 2017 unterbunden wurde, sollte man die Gefahr durch Abhör-Angriffe über manipulierte Geräte mit Mikrofon nicht gering schätzen: Zwar benötigt der Angreifer Zugang zum Gerät, aber die Kosten sind vernachlässigbar.

Selbst führende Hersteller sind sich dieser Gefahr offenbar wenig bewusst, wenn sie von außen zugängliche Daten-Schnittstellen am Gerät vorsehen. Aber auch ein hermetisch verschlossenes Gerät birgt ein Restrisiko: Dass der Hersteller die mitgeschnittenen Worte nicht selbst zu anderen als den im Prospekt versprochenen Zwecken nutzt, darauf müssen Sie in jedem Fall vertrauen.

Rekall's Agent

Pünktlich zum jährlichen Rekall-Workshop auf der DFRWS 2017 ist seit dem 07.08.2017 die Version 1.7 für Windows, Linux und OSX verfügbar. Neben vielen Weiterentwicklungen bei den Plugins (z. B. iexport für NTFS-Dateiextraktion via $MFT) und der Ausweitung auf ca. 2.000 vordefinierte, spezifische Kernelprofile steht die Agenten-Komponente im Mittelpunkt, die sich nun als dauerhafter Service (Daemon) auf Endsystemen installieren lässt.

Mit diesem Release wandelt sich Rekall von einer Stand-Alone-Installation zu einem eigenständigen forensischen Client-Server Incident Response Framework und bietet Unterstützung für Echtzeitforensik auf Client-Systemen. Praktisch ist u. a. die Ausführung von WMI-Queries in Live-Systemen, um Erkenntnisse jenseits eines reinen Hauptspeicherabzugs zu erhalten.

Der Agent stößt außerdem eine spannende Entwicklung an: Client-side Plugins. Dies wird bereits durch das neue vfs_ls-Plugin ermöglicht, mit dessen Hilfe nun „Remote Timelines" auf Clients erstellt werden können – fast in Echtzeit und mit hoher Aussagekraft.

Secorvo News

BSIG-Prüfverfahrens-Kompetenz

Vier Berater und Auditoren von Secorvo haben inzwischen erfolgreich die Prüfverfahrens-Kompetenz nach § 8a (3) BSIG erworben. Sie ist Eignungsvoraussetzung für die Prüfung Kritischer Infrastrukturen und weiterer vom IT-Sicherheitsgesetz betroffener Unternehmen und Institutionen – und hilfreich beim Aufbau geeigneter Informationssicherheits-Management-Systeme.

Frisches aus der Hackerküche

Am **21.09.2017** startet die KA-IT-Si in die zweite Jahreshälfte. Benjamin Lipp und Timon Hackenjos (Fraunhofer IOSB) zeigen, wie ein im September 2016 veröffentlichter Angriff auf Windows-Anmeldeinformationen in abgewandelter Form auch heute noch funktioniert. Benny Görzig und Florian Loch (ebenfalls Fraunhofer IOSB) stellen Angriffe auf das Netzwerkauthentifizierungsprotokoll WPA2-PSK vor, das die meisten von uns in ihren privaten WLAN-Netzen benutzen. Wird die Authentifikation von einem Angreifer mitgeschnitten, liefert sie einen Hashwert, den der Angreifer für einen Angriff auf das WLAN-Passwort verwenden kann.

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

Secorvo-Seminare

Interessenten an unserem PKI-Seminar vom **06. bis 09.10.2017** mit einem vertieften Einblick in Public Key Infrastrukturen empfehlen wir eine baldige Buchung. Und vom **16. bis 19.10.2017** bieten wir Software Engineers das T.P.S.S.E.-Seminar mit der Möglichkeit zur anschließenden Zertifizierung als *TeleTrusT Professional for Secure Software Engineering*.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir Ihnen mit dem T.I.S.P.-Seminar vom **27.11. bis 01.12.2017**; das Begleitbuch „Zentrale Bausteine der Informationssicherheit" erhalten Sie vorab zur Vorbereitung.

Programme, Online-Anmeldung und weitere Termine: secorvo.de/seminare.

Veranstaltungshinweise

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

September 2017	
05.-06.09.	D • A • CH Security (GI, OCG, TeleTrusT, München)
18.09.	Sommerakademie 2017 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
19.-22.09.	OWASP AppSec USA 2017 (OWASP Foundation, Orlando/US)
21.09.	Frisches aus der Hackerküche (KA-IT-Si, Karlsruhe)
26.09.	Anwendertag IT-Forensik (Fraunhofer-Institut SIT, Darmstadt)
Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.10.	IDACON 2017 (WEKA-Akademie, München)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

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

ISSN 1613-4311

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

September 2017

Sie haben die Wahl...

Am 07.09.2017 sorgte der Chaos Computer Club (CCC) kurz vor der Bundestagswahl für Aufregung: Er hatte zahlreiche Schwachstellen in der Software ‚PC-Wahl' identifiziert. Diese Software dient zwar nur zur Ermittlung des vorläufigen Endergebnisses, dennoch könnte dessen Manipulation zu einem Chaos und einer Verunsicherung der Bevölkerung führen. Ein derartiger Vorfall dürfte auch das Vertrauen in den Wahlvorgang nachhaltig erschüttern.

Das Thema Wahlcomputer und Online-Wahlen hielten viele nach dem Urteil des Bundesverfassungsgerichts (BVerfG) im Jahr 2009 für abgeschlossen. Dennoch brachte BSI Präsident Arne Schönbohm in einem Interview vom 11.09.2017 das Thema Online-Wahlen für die nächste Legislaturperiode ins Gespräch. Mit seiner Kritik an der Briefwahl schlägt Prof. Dr. Müller-Quade – Gewinner des deutschen IT-Sicherheitspreises für das Bingo-Voting-Verfahren – in eine ähnliche Kerbe.

Alle denkbaren kryptografischen Wahlverfahren basieren jedoch auf der Grundannahme, dass die Sicherheit des unterliegenden Wahl-Clients gewährleistet sein muss. Das ist gerade bei Online-Wahlen eine wohl kaum umsetzbare Voraussetzung, zumal viele Wahlberechtigte erreicht werden müssen. Dies ist ein bekanntes Problem der IT-Sicherheit: Immer neue Angriffe auf das Online-Banking zeigen, dass es den Banken trotz Jahrzehnten Erfahrung bisher nicht gelungen ist, eine für den Anwender benutzbare und von der Sicherheit des Client unabhängige Online-Banking-Anwendung zu entwickeln. Das lässt sich auf Online-Wahlen übertragen. Komplexe technische Lösungen behindern zudem die vom BVerfG geforderte Überprüfbarkeit der Wahl durch den Bürger – ohne besondere Sachkenntnis – und lösen daher das grundlegende Problem nicht.

Inhalt

secorvo
security consulting

Security News

Vertrauen entzogen

In der März-Ausgabe (SSN 3/2017) berichteten wir von dem Zertifikatsdesaster von Symantec. Bereits damals waren die Google-Chrome-Entwickler entschlossen, den von Symantec ausgestellten SSL/TLS-Zertifikaten das Vertrauen zu entziehen. Nach längeren Diskussionen und Verhandlungen verkündete Google nun am 11.09.2017 in seinem Security Blog den genauen Zeitplan für diesen in der PKI-Geschichte einmaligen Vorgang. Ausgelöst von Googles Vorstoß hatte Symantec bereits am 02.08.2017 den Verkauf seiner Trustcenter-Sparte an den Mitbewerber DigiCert bekanntgegeben.

Spätestens zum 01.12.2017 sollen Zertifikate für Kunden der (Ex-)Symantec-Marken über DigiCerts Trustcenter-Infrastruktur erstellt werden. Sollten nach diesem Stichtag noch Zertifikate von Symantecs jetziger Infrastruktur ausgestellt werden, wird Chrome diesen nicht mehr vertrauen. Vorhandene Zertifikate, die von Symantecs Trustcenter-Marken (u. a. VeriSign, Thawte und GeoTrust) vor dem 01.06.2016 ausgestellt wurden, verlieren mit dem Erscheinen der Chrome-Version 66 ihre Gültigkeit (geplant für den 15.03.2018). Symantec-Zertifikaten, die zwischen dem 01.06.2016 und dem 01.12.2017 erstellt wurden, soll spätestens mit Erscheinen der Chrome-Version 70 das Vertrauen entzogen werden (geplant für den 13.09.2018).

Mozilla hat bereits angekündigt, sich diesem Zeitplan (bis auf wenige Tage Abweichung aufgrund der Release-Zyklen des Firefox-Browsers) anzuschließen. Betroffene Serverbetreiber sollten sich daher frühzeitig um neue Zertifikate von Symantec/DigiCert oder anderen Anbietern kümmern.

BlueBorne

Insgesamt acht kritische Lücken in den Bluetooth-Stacks entdeckten Sicherheitsforscher von Armis Labs und publizierten diese am 12.09.2017 in ihrem Blog. Vier dieser Schwachstellen erlauben einem Angreifer, Schadcode auf allen gängigen Android-, Linux-, Windows- und iOS-Geräten (mit iOS Versionen bis einschließlich 9.3.5) auszuführen: Zwei ermöglichen das Extrahieren sensibler Informationen unter Linux und Android, die beiden anderen Man-in-the-middle-Angriffe unter Windows und Android.

Das Fatale an den gefundenen Schwachstellen ist die Möglichkeit, ein Gerät anzugreifen, ohne es zuvor mit dem Gerät des Angreifers zu koppeln. Es genügt, eine eingeschaltete Bluetooth-Schnittstelle beim Opfer. Unsichtbare Bluetooth-Geräte sind ebenfalls nicht wirksam geschützt. Zwar konnten Microsoft, Google und die Linux-Foundation im September passende Patches für alle betroffenen Geräte bereitstellen; ob diese jedoch von den Herstellern zügig verbreitet werden, ist vor allem bei Android unsicher. Die Bluetooth-Schnittstelle sollte daher deaktiviert werden, bis eine entsprechende Aktualisierung erfolgt ist.

Malware mit Brief und Siegel

Am 18.09.2017 wurde bekannt, dass das beliebte Festplatten-Bereinigungstool CCleaner etwa vier Wochen lang mitsamt einem Trojaner ausgeliefert wurde. Besonders pikant daran ist zum einen, dass kurz zuvor CCleaner-Hersteller Piriform vom Antiviren-Unternehmen Avast übernommen worden war. Zum anderen trugen die befallenen Softwarepakete gültige Code-Signaturen von Piriform. Dennoch braucht der Hersteller wohl keine Welle an Schadenersatz-Klagen aufgrund einer irgendwie gearteten Produkthaftung zu befürchten, was auch die am 19.09.2017 abgewiesene Klage FTC gegen D-Link unterstreicht.

Entdeckt wurde die Schadsoftware unabhängig voneinander in Kunden-Installationen zweier Unternehmen, die aufwändige neuere Ansätze beim Malwareschutz verfolgen. Der klassische, signaturbasierte Virenschutz dagegen gelangte wieder einmal an seine Grenzen: Selbst nach dem Bekanntwerden vergingen noch ca. drei Tage, bevor ein Großteil der unter VirusTotal versammelten Virenscanner den befallenen Installer nicht mehr als „Clean“ meldete. Die Aufarbeitung des Vorfalls folgt eher dem herkömmlichen Muster: Nach ersten Beschwichtigungen, eine Sekundärinfektion wäre unwahrscheinlich, ergab die forensische Analyse des beschlagnahmten C&C-Servers doch knapp zwei Dutzend auf eben diese Weise angegriffene Unternehmen. Inzwischen ist von APT, bekannten Angriffsmustern und asiatischen Netzwerken die Rede – gäbe es die sprichwörtlichen ‚Chinesischen Hacker' nicht, man müsste sie als Synonym für „höhere Gewalt“ erfinden.

Angesichts der Zunahme von „Supply Chain Attacks“ ist jedoch der Blick nach vorn wichtiger als die Suche nach Entschuldigungen. Ein erster Schritt könnte sein, dass Softwarehersteller im Freigabeprozess ihre Softwarepakete zunächst eine Weile mit neueren, bspw. verhaltensbasierten Anti-Malware-Methoden prüfen, ehe sie per Code-Signatur die – wenn schon nicht justiziable, so doch moralische – Verantwortung für ihren so versiegelten Code übernehmen.

Neues vom Privacy Shield

Seit dem 01.08.2016 ist das Europäisch-US-amerikanische Privacy Shield eine Alternative zu den übri-

gen Wegen, die ein gleichwertiges Schutzniveau bei der Verarbeitung personenbezogener Daten sicherstellen sollen. Teil des Abkommens ist eine Beschwerdemöglichkeit, zu deren Unterstützung mehrere deutsche Datenschutzaufsichtsbehörden nun ein Beschwerdeformular publiziert haben.

Das Formular erfragt die erforderlichen Informationen zur Überprüfung der Datenübermittlung ab. Die Beschwerde kann dann von einer unabhängigen Stelle bearbeitet werden. Führt dies nicht zu Abhilfe bleibt dem Betroffenen die Beschwerde bei den eigenen lokalen Datenschutz-Aufsichtsbehörden.

Das Formular ist eine Erleichterung zur Wahrung der Betroffenenrechte. Ob das Instrument jedoch tatsächlich zu einem verbesserten Schutz der personenbezogenen Daten führt, ist zweifelhaft: Nur wenige Betroffene werden überhaupt von der Möglichkeit zur Nachforschung wissen, geschweige denn den dafür erforderlichen Aufwand treiben.

Weitere IT-Sicherheitspflichten

Am 30.06.2017 ist weitgehend unbemerkt das Umsetzungsgesetz zur Richtlinie EU 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (kurz: NIS-Richtlinie) in Kraft getreten. Die Neuregelungen für Anbieter digitaler Dienste gelten ab dem 10.05. 2018. Das Gesetz nimmt auch zahlreiche Änderungen an den durch das IT-Sicherheitsgesetz eingeführten Bestimmungen vor.

Kern ist die Erweiterung des BSI-Gesetzes um einen § 8c, der die Anbieter zum Ergreifen verhältnismäßiger technischer und organisatorischer Maßnahmen verpflichtet, eine Meldepflicht für erhebliche Vorfälle einführt und das BSI zur Prüfung sowie zum Erlass von Anordnungen ermächtigt. Mit ‚digitalen Diensten' sind Dienste der Informationsgesellschaft gemeint, einschließlich Online-Marktplätzen, Suchdiensten und Cloud-Diensten.

Die sonstigen Befugnisse des BSI werden um Regelungen zu Mobilen Incident Response Teams (MIRTs) ergänzt, die andere Stellen nach Sicherheitsereignissen bei der Wiederherstellung ihrer Systeme unterstützen sollen. Auch in Bezug auf die digitalen Dienste wird eine Mitwirkungspflicht von Anwendungsherstellern eingeführt. Die Erweiterungen bezüglich der Betreiber Kritischer Infrastrukturen beziehen sich hauptsächlich auf die Behandlung grenzüberschreitender Belange.

Mit dem Umsetzungsgesetz wird ab Mai 2018 ein weiterer Anbieterkreis gesetzlich zur IT-Sicherheit verpflichtet. Nach den bisherigen Erfahrungen mit dem IT-Sicherheitsgesetz wird sich die Begeisterung bei den betroffenen Unternehmen wohl in Grenzen halten.

Secorvo News

Secorvo Seminare

Noch vier Gelegenheiten zur Weiterqualifikation bieten wir Ihnen in diesem Herbst:

- das T.P.S.S.E.-Seminar zur sicheren Software-Entwicklung (**16.–19.10.2017**),
- unser PKI-Seminar (**06.–09.11.2017**),
- IT-Sicherheit heute (**21.–23.11.2017**) und
- das T.I.S.P.-Seminar (**27.11.–01.12.2017**)

Alle Seminare sind bereits gut gebucht – wir empfehlen daher eine schnelle Anmeldung und freuen uns auf Ihre Teilnahme. Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

CyberWehr-Gipfel in Karlsruhe

Um den wachsenden Schäden durch Cyberangriffe zu begegnen, plant Innenminister Strobl den Aufbau einer CyberWehr Baden-Württemberg. Auf Einladung des Wirtschafsrats wird er das Konzept am **11.10.2017** in einer Keynote auf dem in Zusammenarbeit mit der KA-IT-Si veranstalteten CyberWehr-Gipfel im ZKM | Karlsruhe vorstellen und sich anschließend mit weiteren Experten der Diskussion stellen (Teilnahme frei; zur Anmeldung).

Watching. You.

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **19.10.2017** zum Filmevent in die Karlsruher Schauburg. Bei der Eröffnungsveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Oscar-prämierte Film „Citizenfour" von Laura Poitras gezeigt, der einen persönlichen Blick auf das Leben von Edward Snowden gibt. Wolfgang Petroll wird eine Einführung in den Film geben; im Anschluss folgt eine Diskussion mit Dr. Oliver Raabe (Zentrum für Angewandte Rechtswissenschaft), Prof. Dr. Caroline Robertson-von Trotha (ZAK), Dr. Dirk Achenbach (Kompetenzzentrum IT-Sicherheit) und Jan Linders (Badisches Staatstheater Karlsruhe).

Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
11.10.	Wehrhafte IT-Sicherheit: Cyberwehr-Gipfel in Karlsruhe (Wirtschaftsrat Deutschland/ Wirtschaftsjunioren Karlsruhe/KA-IT-Si, Karlsruhe)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
18.10.	Swiss Cyber Storm 2017 (Swiss Cyber Storm Association, Luzern/CH)
19.10.	Watching. You. (Partner der IT-Sicherheitsregion Karlsruhe/ZAK, Karlsruhe)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick (Editorial), Fabian Ebner, 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

Oktober 2017

Die Schildkröte

Eine meiner Lieblingsparadoxien ist die von Achilles und der Schildkröte. Überliefert von Aristoteles und zugeschrieben Zenon von Elea lautet sie etwa wie folgt:

Achilles, Sohn des Peleus und der Nymphe Thetis, Held der Griechen beim Kampf gegen Troja und schneller Läufer, tritt im Wettlauf gegen eine Schildkröte an. Um das Rennen fairer zu gestalten, räumt er ihr einen Vorsprung ein – und verliert.

Denn während er die Strecke des der Schildkröte gewährten Vorsprungs durchläuft, ist diese bereits weiter gekrabbelt – und hat sich einen neuen, wenn auch kleineren Vorsprung erarbeitet. Holt er diesen auf, hat die Schildkröte wiederum etwas Strecke gut gemacht, und passiert er auch die, ist sie wieder ein Stück weiter – Achilles wird sie daher, so schnell er auch laufen und so unendlich nah er ihr auch kommen mag, niemals überholen.

Mathematiker werden jetzt einwenden, dass unendliche Reihen auch endliche Summen haben können. Aber das rettet uns nicht aus der Denkfalle – denn als Sicherheitsexperte erkennen wir uns in Achilles wieder: Fühlen wir uns nicht oft wie er, wenn wir durch präventive Maßnahmen, Patches oder Policies Angriffsfläche reduzieren – dabei aber feststellen müssen, dass wir Angreifern nachjagen, die sich derweil wieder mit neuen Angriffsmethoden oder unter Ausnutzung neu entdeckter Sicherheitslücken erneut einen kleinen Vorsprung erarbeitet haben.

Dabei widerspricht Zenons Paradoxon unserer Erfahrung. Und tatsächlich ist es die Perspektive, die uns täuscht: Wenn wir uns selbst als hinter Angreifern her hechelnden Achilles sehen, der ständig die von jenen aufgerissenen Löcher stopft, werden wir die Aufholjagd nicht gewinnen können.

Deshalb sollten wir die Perspektive wechseln und uns klarmachen: Für Resignation gibt es keinen Grund. Denn wenn wir schneller sind als die Schildkröte werden wir sie auch überholen.

Inhalt

secorvo
security consulting

Security News

Deterministischer Zufall

Am 18.10.2017 wurde eine Schwachstelle in Infineons Firmware-Bibliothek für Smartcard- und TPM-Chips veröffentlicht – gleich mit GitHub-Archiv. Sie steckt in einem Beschleunigungsalgorithmus für die RSA-Schlüsselerstellung: Er testet nicht einfach Zufallszahlen, bis zwei Primzahlen gefunden sind, sondern konstruiert stattdessen zufallsabhängig Kandidaten, die nicht durch kleine Primzahlen teilbar und somit wahrscheinlicher prim sind.

Hier zeigt sich wieder die Schwierigkeit, Sicherheit als Qualitätsmerkmal nachzuweisen: Die inkriminierte Firmware-Bibliothek wurde u. a. vom BSI nach Common Criteria zertifiziert. Jahre später griffen nun tschechische Forscher auf eine Angriffsmethode zurück, die bei heutiger Schlüssellänge eigentlich nicht mehr relevant ist. Von Infineon-Chips konstruierte 2048 bit lange RSA-Schlüssel aber kann man damit in der Amazon-Cloud für ca. $ 40.000 binnen Tagen brechen. Ob der eigene RSA-Schlüssel betroffen ist, lässt sich übrigens mit Hilfe verschiedener Testtools prüfen.

Als etwas hilflose Panik-Reaktion muss man wohl die Beschränkung des Zugriffs auf die öffentlichen RSA-Schlüssel 750.000 estnischer Ausweiskarten bewerten: das Nicht-Veröffentlichen öffentlicher Schlüssel ist nicht nur eine Contradictio in Adiecto, sondern zudem wirkungslos, denn schon zwei digitale Signaturen können ausreichen, um daraus den öffentlichen Schlüssel zu ermitteln – zumindest wenn dafür wie üblich das traditionelle RSA-Padding-Verfahren (PKCS#1 v1.5) anstelle des seit gut 15 Jahren empfohlenen PSS-Verfahrens verwendet wird.

WLAN-Ü-Ei

In postfaktischen Zeiten benötigt eine Schwachstelle einen griffigen Namen, ein Logo und eine eigene Webseite. Daneben vereint die am 16.10.2017 veröffentlichte KRACK-Attacke drei Dinge auf einmal: Angriff, Ansatzpunkt und Theorie.

Zunächst deckt sie einen in Linux und Android weit verbreiteten Bug auf, der es Angreifern ermöglicht, Nutzer betroffener Geräte unbemerkt und ohne Social Engineering in ein Evil-Twin-Netz umzuleiten. Dahinter steckt eine im WLAN-Standard begründete Schwäche, über die die unterste Ebene der Schlüsselableitung angegriffen werden kann: der pseudozufällige Schlüsselstrom einzelner Datenpakete. In Kombination mit geratenen oder bekannten Inhalten lassen sich so einzelne Pakete in einem per AES-CCMP gesicherten WPA2-Netz entschlüsseln oder wiedereinspielen. Dies ist meist noch nicht schwerwiegend, jedoch ein potenter Ansatzpunkt für weitere Angriffsschritte. Und schließlich erhellt KRACK unser Verständnis vom Wert theoretischer Sicherheitsbeweise: Der Angriff auf das Kryptoprotokoll widerlegt nicht die formalen Beweise, sondern bewegt sich haarscharf außerhalb deren Gültigkeitsbereichs.

Eilige Warnungen, deswegen auf Online-Banking per WLAN zu verzichten, sind jedoch unangemessen: Dass anstelle von leicht aus der Ferne zu dirigierender Man-in-the-Browser-Malware jetzt Flotten von Kleintransportern mit WLAN-Man-in-the-Middle-Ausrüstung in deutsche Wohnviertel ausschwärmen, ist wohl eher unwahrscheinlich. Handlungsbedarf ergibt sich dagegen aus dem Schlaglicht, das KRACK auf das zu erwartende Schwachstellenmanagement im Internet-of-Things wirft: Man beachte, welche Hersteller und Geräte *nicht* in den Listen verfügbarer Patches auftauchen.

Versteckte Minenarbeiter

Seit Mitte September erfreuen sich JavaScript-Miner immer größerer Beliebtheit. Ursprünglicher Zweck solcher Bitcoin-Miner war es, Webseitenbetreibern eine – im Vergleich zu Werbung – beständigere und effizientere Möglichkeit der Finanzierung zur Verfügung zu stellen. Dabei sollte der Nutzer den eingebetteten Miner selbst starten und während des Webseitenbesuchs laufen lassen. Seiten wie „The Pirate Bay“ erweiterten dieses Konzept jedoch und lieferten einen Miner aus, der sofort mit seiner Arbeit beginnt – auch ohne Einverständnis des Nutzers und meist sogar ohne dessen Wissen. Nun haben die Entwickler des JavaScript-Miner reagiert und erzwingen ein Opt-In.

Wer sicher gehen will, dass sein Endgerät nicht für Fremde Bitcoins schürft, sollte JavaScript im Browser blockieren – z. B. mittels Erweiterungen wie NoScript. Alternativ kann man einzelne Seiten auch über den Dienst „Who runs Coinhive?“ prüfen.

Nutzungsanalyse

Das am 13.10.2017 von Harlan Carvey veröffentlichte PlugIn recentapps für das forensische RegRipper Toolset erlaubt die Gewinnung zusätzlicher Informationen über Benutzeraktivitäten unter Windows 10 (und ergänzt damit den UserAssist-Registry-Key). Dazu zählen zum Beispiel die ‚Last-Write Time‘ des Application GUID Subkeys, die unabhängig von der ‚LastAccess Time‘ im NTFS-Dateisystem gespeichert wird. Diese Zeitinformation stellt eine wertvolle Möglichkeit zur Validierung von Programmaufrufen eines Benutzers dar, sogar wenn die Zeitangaben im Dateisystem selbst und in der Master-Dateitabelle manuell verändert wurde.

Praktischerweise liefert das Plugin seine Ergebnisse im Timeliner-Format *.TLN, womit es die forensische Timeline eines Benutzerkontos ergänzt und z. B. Informationen darüber liefert, welche Programme eine Schadsoftware in diesem Benutzerkontext aufgerufen hat.

Zielgruppenansprache à la Facebook

Das Bayerische Landesamt für Datenschutzaufsicht führt in einem Bericht vom 04.10.2017 aus, ob und unter welchen Voraussetzungen der Facebook-Dienst „Custom Audience" den Datenschutzanforderungen des BDSG und der DS-GVO entspricht.

Gemeinsam ist den nach Anwendungsfällen unterschiedenen Varianten des Werbedienstes die zielgenaue Ansprache von Facebook-Nutzern. Dazu erhält Facebook von seinem Auftraggeber entweder eine Adressatenliste oder es wird ein Facebook-Pixel auf der Auftraggeber-Website eingebunden.

Beim Pixel-Verfahren seien die Auftraggeber verpflichtet, Betroffene über die Datenerhebung zu informieren und ein Opt-Out-Verfahren anzubieten. Die Verantwortung für den rechtmäßigen Einsatz der „Facebook Custom Audience" obliege dabei dem jeweiligen Unternehmen. Die Übermittlung der Listendaten erfordere eine gesonderte Rechtsgrundlage, in der Regel die Einwilligung der betroffenen Personen.

Sowohl das Einwilligungserfordernis als auch die Informationspflicht über die Verarbeitung durch Facebook machen eine rechtskonforme Umsetzung faktisch unmöglich. Mit Blick auf die empfindlichen Ordnungsgelder der DS-GVO sollte daher von einer Nutzung der Dienste Abstand genommen werden.

Kopieren oder nicht kopieren...

Mit einer Änderung von § 20 Personalausweisgesetz (PAuswG) vom 07.07.2017 wurde das Kopieren von Personalausweisen unter bestimmten Voraussetzungen ermöglicht. So muss die Kopie als solche dauerhaft erkennbar sein (z. B. schwarz-weiß) und die Einwilligung des Inhabers vorliegen. Dient die Ablichtung zur weiteren Verwendung der Personalausweisdaten, so bedarf dies einer gesonderten Einwilligung; selbstverständlich sind zudem alle einschlägigen Datenschutzvorschriften einzuhalten.

Bislang war die vielfach auch in Privatunternehmen bestehende Praxis, zur Dokumentation des Identitätsnachweises den Ausweis zu scannen oder zu kopieren, durch § 14 PAuswG untersagt. Das Verbot hat sich in der Praxis nie wirklich durchgesetzt, die der neue § 20 nun legitimiert. Ein wenig wirkt dieser Interessensausgleich daher wie eine Kapitulation.

Secorvo News

Verstärkung

Im Sommer ist es uns gelungen, unser Beratungsteam zu erweitern: Seit dem 01.10.2017 verstärkt Sarah Niederer den Bereich Datenschutz. Sie bringt vieljährige Berufserfahrung aus den Bereichen Compliance, Business-Impact-Analysen, Risikomanagement und insbesondere vertieftes Datenschutz-Know-How mit.

Secorvo-Seminare

Für Schnellentscheider bieten wir in diesem Jahr noch drei Seminare an: PKI (06.-09.11.2017), IT-Sicherheit heute (21.-23.11.2017) und das T.I.S.P.-Seminar (27.11.-01.12.2017) mit anschließender Zertifizierung.

Programme, die Möglichkeit zur Anmeldung und die Seminartermine 2018 finden Sie unter www.secorvo.de/seminare.

Sicherheit auf Wolke sieben

Die Verarbeitung von Daten in der ‚Cloud' stößt immer wieder (und oft berechtigt) auf Sicherheitsbedenken. Dabei ginge es auch anders: Mit ‚Privacy & Security by Design' lassen sich Cloud-Lösungen mit hohem Sicherheits- und Datenschutzniveau realisieren. Wie das geht, zeigen wir bei unserem kommenden KA-IT-Si-Event am **23.11.2017** an Beispielen aus anwendungsnahen Forschungs- und Entwicklungsprojekten. Gastgeber ist das Karlsruher „House of Living Labs" des Forschungszentrums Informatik (FZI). Für Interessierte bieten wir vorab eine Führung durch dieses Innovationslabor an.

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

Krypto im Advent – 24 Tage, 24 Rätsel

Verschlüsseln und entschlüsseln, grübeln und Spaß haben, lösen und gewinnen: Das ist Krypto im Advent. Mehr als 2.400 begeisterte Rätselknacker begaben sich im vergangenen Advent täglich in die Welt der Kryptologie. Am 01.12.2017 geht es nun wieder los. An diesem Adventsrätsel, das in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelt wurde, können alle Schülerinnen und Schüler der **Klassen 3 bis 9** teilnehmen. Dank unseren Sponsoren gibt es wieder zahlreiche Preise zu gewinnen. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

Oktober 2017	
30.10.-03.11.	ACM CCS 2017 (ACM/SIGSAC, Dallas/US)
November 2017	
06.-09.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-15.11.	ISSE 2017 (EEMA, Brüssel/BEL)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.-28.11.	7. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Hans-Joachim Knobloch, Michael Knopp, 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

November 2017

Panoptikum

Jeremy Bentham (1748-1832), einer der großen Vordenker des Liberalismus und unseres heutigen Rechtsstaatsverständnisses, huldigte einem heute nur schwer nachzuvollziehenden Freiheitsbegriff: Er war überzeugt, dass nur ein mächtiger Staat mit strengen Sanktionen die allein auf ihren Vorteil bedachten Bürger an der rücksichtslosen Durchsetzung ihrer eigenen Interessen hindern könne. Und dass dieser Staat dafür einen umfassenden Überwachungsapparat benötige, damit aus der Erzwingung rechtskonformen Verhaltens echte Freiheit erwachse. Seine Vorstellungen kulminierten in dem Konstruktionsentwurf eines Gefängnisses, bestehend aus einem zentralen Bewachungsturm, um den die Zellen kreisförmig angeordnet und vom Turm aus durch Glaswände einsehbar sind.

Diese von ihm als Panoptikum bezeichnete Konstruktion erlaubte eine Überwachung ohne Wächter: Da der Turm von den Zellen aus nicht einsehbar war, mussten die Gefangenen ständig davon ausgehen, beobachtet zu werden. Mit dem Resultat, dass sie ihr Verhalten automatisch an die vermeintlichen Erwartungen der Überwacher anpassten. So beschreibt es auch Winston Smith in Orwells „1984“: *“You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”*

Benthams Gefängnisse konnten sich nicht durchsetzen. Dafür mutiert unsere Welt gerade zum Panoptikum: Hunderttausende Videokameras auf Straßen, in öffentlichen Gebäuden, Bussen und Bahnen, Kuscheltiere und Kinderuhren mit Mikrofon, HD-Kamera und SIM- oder SD-Karte, Spy-Tools für Smartphones und trackende Navigations-Apps – und natürlich die Kommunikationsfilter der Nachrichtendienste. Orwells Dystopie funktioniert offenbar auch gänzlich ohne „Großen Bruder“. Welchen Preis wir dafür bezahlen, werden wir vor lauter Gewöhnung womöglich nicht einmal bemerken.

Inhalt

secorvo
security consulting

Security News

Übermorgen ist morgen gestern

In den vergangenen Jahren haben sich die öffentlichen Trustcenter, die SSL-Serverzertifikate verkaufen, nicht gerade mit Ruhm bekleckert (u. a. SSN 03/2011, 09/2011 und 09/2017).

Da wäre es doch eine gute Idee, wenn der Browser reagieren könnte, falls ein HTTPS-Server plötzlich ein ganz anderes Zertifikat vorweist als erwartet, dachte man bei Google und entwarf 2011 bis 2015 den HPKP-Standard zum *Public Key Pinning*. Mit dieser HTTP-Header-Erweiterung kann ein Webserver dem Browser mitteilen, wie die Zertifikate aussehen werden, die er in den nächsten Monaten erwarten darf. Bei anderen Zertifikaten blockiert der Browser dann künftig den Zugriff auf die Seite.

Die Krux dabei ist, dass sich im schnelllebigen Internet „erwartet" und „unerwartet" nicht ganz so einfach unterscheiden lassen. Was ist, wenn bspw. der langjährige Zertifikatslieferant plötzlich vom Markt verschwindet? Ein weiteres schlagendes Argument der HPKP-Kritiker ist, dass sich dadurch ein neues Geschäftsfeld für Internet-Erpresser auftut: Wer den Besuchern eines kompromittierten Webservers manipulierte Public Key Pinning Header unterschiebt, könnte einen stolzen Preis für den passenden Private Key verlangen – selbst dann, wenn der Server HPKP eigentlich gar nicht nutzt.

Am 27.10.2017 verkündete Google nun, HPKP in Chrome zum Mai 2018 wieder abschaffen zu wollen – noch bevor Public Key Pinning eine breite Akzeptanz gefunden hat.

TeleTrusT Innovationspreis 2017

Auf dem mit rund 200 Teilnehmern sehr gut besuchten (und sehr empfehlenswerten) T.I.S.P. Community Meeting wurde am 14.11.2017 der TeleTrusT Innovationspreis 2017 an die PointBlank Security/Steen Harbach AG für eine smarte und einfallsreiche IoT-Lösung verliehen.

Man könnte meinen, der Begriff IoT-Security sei ein Widerspruch in sich, da es doch das Ziel der Hersteller (und oft auch der Nutzer) ist, Steuerungen für Alltagsgegenstände möglichst günstig zu realisieren und an das Internet anzubinden. Sicherheitsaspekte müssen dabei in der Regel zurückstehen – sie kosten Ressourcen und erfordern Know-how. Genau in diese Bresche springt die prämierte Lösung: Ein winziger Hardware-Chip ertüchtigt IoT-Geräte mit aktuellen Kryptofunktionen, der Authentisierung von Kommunikationspartnern und einer TLS-Absicherung der Kommunikationsverbindungen.

Der Chip wird in die Kommunikation eingeschleift und ermöglicht trotz der geringen Rechenleistung Kyptofunktionen auf Augenhöhe mit aktuellen PC-Systemen. Laut Herstellerangaben konnte z. B. der TLS-Handshake durch den sehr schlanken Code von ursprünglich mehreren Minuten auf 300 Millisekunden reduziert werden. Ein vielversprechender Ansatz, um einfache IoT-Geräte mit State-of-the-Art-Security-Mechanismen auszustatten. Security Made in Germany eben.

OWASP Top 10 – 2017

Seit inzwischen 13 Jahren veröffentlicht das OWASP regelmäßig die 10 wichtigsten Risiken bei Webanwendungen. Die am 20.11.2017 veröffentlichte finale Version der OWASP Top 10 2017 basiert zum ersten Mal auf Daten der Community. Erschreckend ist die große inhaltliche Übereinstimmung mit der ersten Version der OWASP TOP 10 aus dem Jahr 2004. Offensichtlich ist das Thema Sicherheit trotz vieler Bemühungen noch immer nur in Teilbereichen der Softwareentwicklung angekommen.

Sehr häufig werden die OWASP Top 10 als Standard missverstanden. Tatsächlich sind die Top 10 ein Awareness-Dokument. Für andere Zwecke bieten OWASP und auch andere Organisationen geeignetere Hilfestellungen, wie die Sicherheitsspickzettel für Entwickler, die Top 10 für Entwickler, den Application Security Verification Standard, den Testing Guide und vieles mehr.

Happy Birthday Privacy Shield

Das EU-U.S. Privacy Shield regelt seit 2016 den transatlantischen Datenverkehr personenbezogener Daten in die USA. Es ersetzte das vom Europäischen Gerichtshof für nichtig erklärte Safe-Harbor-Abkommen. Die Effizienz und Effektivität des Privacy Shield muss jährlich von der Europäischen Kommission überprüft werden. In dem am 18.10.2017 publizierten ersten Jahresbericht wurde dessen Wirksamkeit grundsätzlich bestätigt. Jedoch wurden konkrete Maßnahmen zur Verbesserung identifiziert, z. B. hinsichtlich der Kontrolle zertifizierter U.S.-Unternehmen oder der ausstehenden Ernennung eines Privacy-Shield-Ombudsmanns.

Die geforderte Umsetzung der Privacy-Shield-Vorgaben wird genau überwacht und teilweise kontrovers diskutiert. So wird beispielsweise moniert, dass EU-Datenschutzbeauftragte durch die Europäische Kommission ungenügend zur jährlichen Überprüfung einbezogen wurden, weshalb diese nun an einem eigenen Bericht arbeiten.

Inwieweit sich die Resultate mit denjenigen der Europäischen Kommission decken, bleibt abzuwarten. Falls die datenschutzrechtlichen Bedenken nicht ausgeräumt werden können, wird es zu einem wichtigen Indikator für die künftige Datenschutzausrichtung der Europäischen Kommission, wie diesem Umstand Rechnung getragen wird. Denn europäische Datenschutzbeauftragte zeigten und zeigen sich noch immer unzufrieden mit dem vom Privacy Shield vorgegebenen Datenschutzniveau.

Forensik inside

Seit dem 21.11.2017 liegen die Ergebnisse des diesjährigen Volatility Plugin Contest der Volatility Foundation vor, bei dem einige interessante und hilfreiche Erweiterungen prämiert wurden.

Besonders hervorzuheben ist darunter das Plugin SqliteFind, mit dem nun der Hauptspeicher nach jeglichen vorhandenen Table-Definitionen des „sqlite_master table" logisch und automatisiert durchsucht werden kann. In einem zweiten Schritt können dann spezifische Tables zeilenweise als Row ausgelesen werden.

Da SQLite inzwischen von sehr vielen Programmen genutzt wird und es immer seltener bei einer forensischen Analyse zu Beginn bekannt ist, wo ggf. wichtige Datenspuren vorhanden sind, schließt dieses Plugin einen wirklich blinden Fleck bei der forensischen Datenaufbereitung.

Secorvo News

Vom Rack zum RZ

In vielen Unternehmen ist die IT-Infrastruktur über die Jahre gewachsen – und manchmal sieht man ihr das auch an: Der Serverraum war eigentlich nie als Serverraum gedacht, und es sind eher die Erfordernisse des Tagesgeschäfts, die den Ausbau prägen, als eine systematische Planung. Der Sicherheit und Wartbarkeit der Infrastruktur kommt das selten zugute.

Wie aus dem gewachsenen Serverraum ein kleines Rechenzentrum werden kann, das heutigen Sicherheits- und Verfügbarkeitserwartungen genügt, zeigt Marco Müller (DC-Datacenter-Group GmbH) bei unserem kommenden KA-IT-Si-Event am **07.12.2017**, diesmal in den Räumen des Cyber-Forum. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „**Buffet-Networking**" (zur Anmeldung).

24 Verschlüsselungsrätsel

Am 01.12.2017 beginnt unser 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 drei Spione innerhalb von 24 Tagen davon abzuhalten, die Weihnachtsfeier der Agenten zu entlarven...

Wer alle Aufgaben 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.

www.krypto-im-advent.de

Who watches the watchmen?

Merken Sie sich schon einmal die Abschlussveranstaltung der Traumfabrik-Filmreihe „BIG BROTHER: Surveillance Cinema" am **27.02.2018** (18-21 Uhr) im Karlsruher Filmtheater Schauburg vor – einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit dem Zentrum für Angewandte Kulturwissenschaft (ZAK) am KIT. Wir zeigen den Film „The Circle" (OmU) und diskutieren anschließend 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) – eine Anmeldung ist nicht erforderlich.

Secorvo Seminare

Im kommenden Jahr bieten wir Ihnen wieder zahlreiche Gelegenheiten, Ihre Kenntnisse in der IT- und Informationssicherheit aufzufrischen, zu vertiefen und zu zertifizieren. Das nächste T.I.S.P.-Seminar findet **vom 16. bis 20.04.2018** statt – nach Ihrer Anmeldung erhalten Sie zur Vorbereitung ein Exemplar des T.I.S.P.-Begleitbuchs.

Veranstaltungshinweise

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

Dezember 2017	
04.-07.12.	Black Hat Europe 2017 (Blackhat, London/UK)
Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)

Fundsache

Mozilla wartet in diesem Jahr mit einem besonderen Weihnachtsgeschenk auf: Auf einer ansprechend gestalteten Webseite bewertet es die (US-amerikanischen) technischen „Must-Haves“ dieser Geschenkesaison nach einer einfachen Privacy-Taxonomie: Kann es mich ausspionieren? Was weiß es über mich? Und: Was kann passieren, wenn etwas schiefgeht?

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, 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

Dezember 2017

Bärendienst

Noch fünf Monate bis zum Inkrafttreten der Datenschutz-Grundverordnung. Kaum ein Magazin, das nicht mahnt und erinnert – und an prominenter Stelle mit den Sanktionen droht: bis zu 20 Mio. € oder 4 % des weltweiten Vorjahresumsatzes.

Das sind Zahlen, die jede Geschäftsleitung erblassen lassen. Stand der Datenschutz bisher abgeschlagen auf der „Da-sollte-ich-mich-vielleicht-auch-mal-drum-kümmern"-Liste, hat er es nun unter die Top 10 der „Wichtig-und-dringend"-Liste geschafft. Datenschützer frohlocken, Aufsichtsbehörden schwitzen unter den signifikant gestiegenen Beratungsanfragen und Datenschutzexperten schießen allerorts wie Pilze aus dem Boden.

Dabei gibt es für Torschlusspanik nicht den geringsten Grund, ist die DS-GVO doch wenig mehr als eine Kopie des BDSG: Kaum eine Bestimmung, die (zumindest in Deutschland) nicht bereits heute gilt. Neu sind die erweiterten Dokumentationspflichten – aber das kann auch als Ruf nach einem höheren „Reifegrad" des Datenschutz-Managements verstanden werden: Wie die Informationssicherheit wird sich zukünftig auch der Datenschutz mit Prozessen und deren Nachweisbarkeit beschäftigen müssen.

Aber diese Anpassungen rechtfertigen kaum den Handlungsdruck, der mit Blick auf den 25. Mai 2018 aufgebaut wird. Denn wie viele Besuche von Aufsichtsbehörden gab es 2017 tatsächlich? Und woher soll das Personal kommen, das diese Anzahl erhöhen könnte? Wenn aber der letzte Vorstand verstanden hat, dass die DS-GVO doch nicht so heiß gegessen wird, wie sie gekocht wurde, kann der Datenschutz schnell wieder in der Asche landen, aus der er gerade aufsteigt. Und dann könnte es sich als Fehler erweisen, dass es Ordnungsgelder waren, die ihn wichtig gemacht haben – und nicht die Einsicht, dass es beim Datenschutz gar nicht um den Schutz von Daten, sondern von Persönlichkeitsrechten geht. Vermutlich ist es nie eine gute Idee, Grundrechte einem Ablasshandel zu überlassen.

Inhalt

secorvo
security consulting

Security News

Geschenktipp 1

Nachdem am 16.12.2017 bekannt wurde, dass Firefox unerwünscht ein Plug-In installiert, das Daten über die Firefox-Nutzung erhebt, empfehlen wir, Chrome mit den folgenden Plug-Ins zu bescheren, die unerwünschte Werbung und Skripte abschalten.

Das wohl interessanteste ist Privacy Badger der Electronic Frontier Foundation, das über einen lernenden Algorithmus unerwünschte Tracker, Werbung und Cookies zu blockieren versucht. Eine ähnliche Funktionalität bietet das von Firefox bekannte Ghostery. Das Besondere: es kann Tracker verschiedener Kategorien selektiv deaktivieren. Ein klassischer Werbeblocker ist uBlock Origin, der die gängigen Listen unterstützt und nutzt. Erfahrene Anwender können zu uMatrix greifen, das ähnliche Funktionen wie NoScript für Firefox mitbringt.

Am sinnvollsten ist eine Kombination der genannten Plug-Ins: Privacy Badger oder Ghostery als Grundgerüst und als Ergänzung einen Werbeblocker wie uBlock oder uMatrix. Von allen oben genannten Plug-Ins gibt es übrigens auch eine Firefox-Version.

Geschenktipp 2

Sich selbst beschenkt haben die beiden Autodiebe, die in dem am 26.11.2017 von der West Midlands Police veröffentlichten Video die Funkstrecke zwischen dem Autoschlüssel hinter der verschlossenen Eingangstür und dem in der Einfahrt geparkten Wagen mit passender Gerätschaft verlängern.

Uns bescheren sie damit zweierlei: Einerseits eine schöne bildliche Illustration des Man-in-the-Midde Prinzips. Und andererseits die Bestätigung, dass Videoüberwachungen oft nur von beschränktem Nutzen sind – von den Dieben und dem Wagen fehlt bis heute offenbar jede Spur.

Geschenktipp 3

Am 23.11.2017 veröffentlichte Matt Edmondson in seinem Blog, wie sich ein exemplarischer Hidden Service im Tor-Netzwerk durch das Tool Burp Collaborator deanonymisieren lässt: Hidden Services erlauben es, über das Tor-Netzwerk Dienste wie Webserver anzubieten, ohne die IP-Adresse des Servers preiszugeben.

Der Burp Collaborator ist eine 2015 erschienene Erweiterung für das verbreitete Pentesting-Tool Burp Suite, das hilft, Schwachstellen durch die zeitlich versetzte Verarbeitung von Daten zu erkennen – sogenannte Out-of-Band-Angriffe. Dafür werden Hostnamen und URLs mit eindeutigen Merkmalen für jede Anfrage injiziert und danach überwacht, ob diese durch den Server oder nachgelagerte Systeme per DNS aufgelöst bzw. per HTTP angefragt werden. Mit der Erweiterung Collaborator Everywhere lassen sich solche Payloads noch flexibler und großflächiger injizieren.

Der verwundbare Hidden Service löste den HTTP-Header X-Forwarded-For auf und verriet dabei seine tatsächliche IP-Adresse. Der Angriff stellt zwar keine grundsätzliche Verwundbarkeit der Hidden Services dar, illustriert jedoch sehr gut, wie sich der Collaborator einsetzen lässt. Deshalb ist er unser diesjähriger Geschenktipp für Pentester.

Geschenktipp 4

Das Ergebnis des dreijährigen, gemeinsamen Normungsprojekts von Deutscher Bahn, Blancco, DATEV, Secorvo und Toll Collect, die Ende 2016 verabschiedete DIN 66398 („Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“) ist nun, immerhin noch vor Inkrafttreten der Datenschutz-Grundverordnung, in englischer Sprache erschienen und kann beim Beuth Verlag bezogen werden.

Für international tätige Unternehmen – insbesondere mit europäischen Tochter- oder Muttergesellschaften – gehört sie zwingend unter den Weihnachtsbaum.

Geschenktipp 5

Das Bundesarbeitsgericht hat in einem bereits am 25.04.2017 verkündeten und nun schriftlich begründeten Urteil sehr deutlich Grenzen für die Leistungs- und Verhaltenskontrolle gesetzt. Es führt beispielhaft den Abwägungsprozess zwischen Persönlichkeitsrechten und dem Interesse der Arbeitgeber anhand eines Tools zur Erstellung einer „Belastungsstatistik“ vor.

Gegenstand war ein Einigungsstellenspruch über die Auswertung der Schadensfallabwicklung in verschiedenen Außenstellen einer Versicherung. Während der Betriebsrat wegen der – allerdings nicht ausreichend dargelegten – Gesundheitsgefährdung klagte, befand das Bundesarbeitsgericht die gesamte Auswertung für unzulässig. Nach dem aufgeführten Zweck sollten Auslastungsunterschiede der Außenstellen analysiert werden. Hierzu sollte anhand von wöchentlichen bis halbjährlichen, auf den einzelnen Mitarbeiter bezogenen Kennzahlen die quantitativ gemessene Leistung erfasst und bei Abweichung von Schwellenwerten individuell untersucht werden. Das BAG sieht hierin eine unverhältnismäßige ständige Überwachung. Zuvor äußerte es bereits Zweifel an der Eignung und

Erforderlichkeit zum behaupteten, grundsätzlich anzuerkennenden Zweck.

Ausgedruckt ein perfektes Last-Minute-Geschenk für Betriebsräte – Datenschützer müssen hingegen die Kröte schlucken, dass das Bundesarbeitsgericht strikt mit dem Persönlichkeitsrecht argumentiert und weder die informationelle Selbstbestimmung noch § 32 BDSG heranzieht.

Geschenktipp 6

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) informierte am 24.11.2017 über ein interessantes Angebot: Über einen spielerischen Onlinetest können Unternehmen kostenfrei ihre DS-GVO Konformität überprüfen. Hintergrund der Sensibilisierungsaktion ist u. a., dass das BayLDA mit Anfragen zur DS-GVO überhäuft wird. Auf Basis der Online-Selbsteinschätzung wird Unternehmen die Möglichkeit gegeben, ihren aktuellen Datenschutzreifegrad bewerten zu lassen. Die Test-Ergebnisse inklusive Erläuterungen werden in Berichtsform zum Download bereitgestellt. Das perfekte Geschenk für die Geschäftsleitung, falls das Datenschutzbudget 2018 noch umstritten sein sollte...

Geschenktipp 7

Die CNIL (Commission Nationale de l'Informatique et des Libertés) hat neben den bereits veröffentlichten Leitfäden zur Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO nun ein Open-Source-Software-Tool bereitgestellt.

Das Tool führt anhand von Fragen mit Erläuterungen zu den erwarteten Antworten durch die Datenschutz-Folgenabschätzung eines Verfahrens und unterstützt deren Dokumentation. Die Erfassung ist gegliedert in die Verfahrenserfassung (Beschreibung der Verarbeitung), die Abfrage der Rechtsgrundlage und der Verhältnismäßigkeit, die ergriffenen Schutzmaßnahmen und die Bewertung der Risiken nach Eintrittswahrscheinlichkeit und Folgen für die Betroffenen. Als Risiken sind pauschal unbefugter Zugriff, unbefugte Veränderung und Datenverlust vorgegeben. Umfangreicher sind die vorgegebenen und anhand der Hinweise zu beschreibenden Schutzmaßnahmen.

Für Datenschutzbeauftragte, die nur vereinzelt Datenschutz-Folgenabschätzungen durchzuführen haben, kann diese mit dem Tool dokumentiert werden. Es bietet zudem eine gute Orientierung, wenn es auch nur wenige Anpassungen zulässt.

Secorvo News

Wie ich lernte, die Blockchain zu lieben.

Blockchain, die Technologie hinter der Kryptowährung Bitcoin, hat einen regelrechten Hype ausgelöst. Mit ihr können Transaktionen unveränderlich und für jedermann nachvollziehbar erfasst werden, und das ohne eine zentrale Vertrauensinstanz. Viele reagieren auf dieses Versprechen mit Begeisterung: So habe die Blockchain-Technologie noch ganz andere Anwendungen über elektronische Währungen hinaus: In der Musikindustrie ebenso wie zur Absicherung von Militärsystemen. Andere begegnen der Blockchain mit zurückhaltender Skepsis.

Dirk Achenbach erklärt auf dem Jahresstartevent der KA-IT-Si am **01.02.2018** die Blockchain aus kryptographischer Sicht – und stellt in seinem Vortrag dar, wie seine Skepsis der Begeisterung wich. Blockchain ist nämlich keine Universallösung, sondern eine Technologie, die spannende Fragen aufwirft. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wegen der großen Nachfrage empfehlen wir eine baldige Anmeldung.

Who watches the watchmen?

Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Vorratsdatenspeicherung, Sammlung von Nutzungs- und Bewegungsprofilen durch Internet-Dienstleister, Massenüberwachung durch Nachrichtendienste – die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger" zu machen. Doch was, wenn die Kontrolleure unkontrollierbar werden?

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg.

Bei der Abschlussveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Film „THE CIRCLE" von James Ponsoldt gezeigt. Wolfgang Petroll wird in den Film einführen; im Anschluss folgt 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). Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
01.02.	Wie ich lernte, die Blockchain zu lieben. (KA-IT-Si)
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.02.	Who watches the Watchmen? (IT-Sicherheitsregion 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)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, 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