secorvo
security consulting

Secorvo Security News

Juni 2019

Der Wert des Flüchtigen

Wenn ich dieses Editorial verfasse weiß ich nicht nur, dass es viele Menschen lesen werden. Ich weiß auch, dass ich nicht wissen kann, wer genau es lesen wird – oder anders herum: Ich muss damit rechnen, dass es jeder Mensch lesen könnte. Auch Menschen, die mich nicht kennen, meine Äußerungen nicht in den Gesamtkontext einordnen werden oder können, vielleicht Sätze aus dem Zusammenhang reißen. Daher werde ich mich besonders um Unmissverständlichkeit bemühen, um die korrekte Verwendung von Begriffen und die Klarheit meiner Überlegungen. Das muss nicht gelingen – aber vor der Veröffentlichung werde ich überzeugt sein, dass ich es nicht klarer und unmissverständlicher schreiben konnte. Umgekehrt wird jeder Leser genau das wissen. Und mir daher jeden Satz und jede Äußerung auch zurechnen. Einmal in der Welt lässt sich ein solcherart veröffentlichter Gedanke nicht mehr zurücknehmen. Das ist auch bedeutsam, denn erst diese Ernsthaftigkeit verleiht ihm das nötige Gewicht.

Daneben (besser: davor und dahinter) gibt es aber auch das nichtöffentliche, gesprochene Wort: Dem kann dieses Gewicht nicht beigemessen werden. Und darf es nicht. Es muss zurücknehmbar bleiben, vorläufig und flüchtig. Dieser Schutz vor unerwarteter oder unerwünschter Kenntnisnahme durch Dritte ist essentiell: Denn wir benötigen den Raum des Vorläufigen und Flüchtigen, damit Gedanken und Überzeugungen im Diskurs reifen können. Der öffentliche Umgang mit privaten Äußerungen von Politikern (die hinsichtlich aller ihrer Äußerungen natürlich in einer besonderen Verantwortung stehen) macht manchmal vergessen, wie bedeutsam diese Flüchtigkeit für eine freie Gesellschaft ist.

Wer daher den Zugriff auf Daten von Sprachassistenten fordert, hat nicht nur den Datenschutz und die Unverletzlichkeit der Wohnung, sondern auch das Fundament einer freiheitlichen Ordnung nicht verstanden.

Inhalt

secorvo
security consulting

Security News

Magische Technologien

Ransomware ist derzeit eine der größten digitalen Gefahren für Unternehmen und Behörden. Sind die Daten erst einmal verschlüsselt, hilft in der Regel nur eine gelebte Disaster-Recovery-Strategie. Oft fehlt sie – und die Opfer wenden sich verzweifelt an Datenwiederherstellungs-Experten. Doch ohne bekannte Schwachstellen in der Ransomware hilft auch das nicht, denn die verwendeten starken Verschlüsselungsalgorithmen können nicht gebrochen werden. Mehrere US-amerikanische Data-Recovery-Firmen verfügen jedoch nach eigenen Angaben über „proprietäre Technologien", um die Daten zu entschlüsseln – wie kann das sein?

Wie Pro Publica am 15.05.2019 publizierte, besteht die magische „proprietäre Technologie" darin, unter der Hand das Lösegeld zu bezahlen... Die Firmen bieten den Opfern einen risikofreien Weg aus der Ransomware-Falle. Ransomware-Entwickler umwerben diese Firmen offenbar als vertrauenswürdige Mittelsmänner und bieten ihnen Vergünstigungen, Rabatte und Verlängerungen von Deadlines an. Lesson learned: „Magische Technologien" mag es geben – allerdings nicht in der Kryptografie.

Dem Trustcenter ausgeliefert

Auch Schadsoftware kann mit einer gültigen Code-Signatur versehen werden. Forscher veröffentlichten am 22.05.2019 eine auf den Daten von VirusTotal basierende Top-25-Liste der Trustcenter, mit deren Zertifikaten mutmaßliche Malware signiert wurde. Ganz oben: die Comodo CA. Deren neuer Betreiber Sectigo sperrte daraufhin am 24.05.2019 127 betroffene Zertifikate.

Wie am 30.05.2019 bekannt wurde, war darunter jedoch mindestens ein Code-Signing-Zertifikat eines legitimen Sectigo-Kunden, dessen CAD-Software von fünf der 70 Virenscanner fälschlich als Malware klassifiziert wurde. Nach der Sperrung beschwerten sich Anwender zuhauf beim Hersteller, dass ihre CAD-Software nicht mehr lief. Sectigo hat formal korrekt gehandelt: Nach Kapitel 4.9.1 der Baseline Requirements des CA/Browser-Forums muss ein Trustcenter ein Zertifikat nach spätestens fünf Tagen sperren, wenn „*The CA obtains evidence that the Certificate was misused*". Wie sorgfältig die Indizien zu prüfen sind, ist nicht genauer spezifiziert. Eine Haftung für fälschliche Sperrung ist nicht vorgesehen. Zwar hätten fünf Tage wohl gereicht, um den Sachverhalt mit dem betroffenen Kunden zu klären – das aber ist in diesem Fall offenbar unterblieben. Wer Zertifikate für geschäftskritische Zwecke nutzt, sollte also besser regelmäßig selbst den Sperrstatus der eigenen Zertifikate prüfen.

Crypto Wars 2.0

Verwendet man TLS mit Perfect Forward Secrecy (PFS) ist es auch bei Kenntnis des privaten Schlüssels unmöglich, aufgezeichnete TLS-Sitzungen nachträglich zu entschlüsseln. Aus Compliance-Gründen (Network Monitoring in internen Netzen) unterstützt das vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelte ETS-Protokoll (vormals eTLS) PFS nicht. MITRE listet es daher seit dem 26.02.2019 auf Betreiben der Electronic Frontier Foundation (EFF) offiziell als Schwachstelle (CVE-2019-9191). Der Bankensektor, insbesondere die Industriegruppe BITS, versuchte schon während der Standardisierung TLS 1.3 durch die Entfernung von PFS zu schwächen. Webbrowser können ETS und TLS 1.3 nicht unterscheiden, da ETS PFS mit statischen Diffie-Hellman-Schlüsselpaaren realisiert.

Eine von derzeit vielen Bestrebungen, Krypto-Protokolle zu schwächen. So sollen beispielsweise Messenger-Dienste gesetzlich verpflichtet werden, Strafverfolgungsbehörden in Verdachtsfällen einen Zugriff auf die entschlüsselte Kommunikation zu ermöglichen. Keine neue Diskussion – und es gilt noch immer, was auch der Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) am 12.06.2019 publizierte: Backdoors schwächen nicht nur das Vertrauen der Nutzer in IT-Systeme, sondern können auch missbräuchlich genutzt werden. Keine gute Idee.

Certificate Transparency

Damit Zertifikate von Google Chrome als gültig anerkannt werden, müssen öffentlichen Zertifizierungsstellen diese seit dem 30.04.2018 vor der Ausstellung als *Precertificate* in mehrere öffentliche Certificate-Transparency-Protokolle schreiben. Ein echter Sicherheitsgewinn für die Web-PKI, denn nun kann jeder diese Protokolle durchsuchen – beispielsweise durch die Website crt.sh –, fehlerhafte Ausstellungen erkennen, melden und eine rasche Sperrung veranlassen.

So wurde am 16.04.2019 aufgedeckt, dass die französische Zertifizierungsstelle Certinomis unter anderem Zertifikate für nicht registrierte Domains und solche mit ungültigen Object Identifiers (OIDs) ausgestellt hatte. Wegen mehreren Verstößen gegen Baseline Requirements wird sie nun aus dem Root-Programm von Mozilla Firefox Version 69 entfernt; Certimonis-Zertifikate sind damit nicht mehr vertrauenswürdig. Auch die Zertifizierungsstellen Sectigo, SECOM und DigiCert sind betroffen: Sie haben Extended-Validation-Zertifikate (EV), die nur nach besonders sorgfältiger Überprüfung des Antragstellers ausgestellt werden dürfen und daher im Browser mit einer „grünen Adressleiste" belohnt

werden, teilweise mit „Default City“ als Städtenamen oder „Some-State“ als Staatsnamen ausgestellt. Die betroffenen Zertifikate wurden gesperrt.

Vielleicht gelingt es ja auf diesem Weg, das angekratzte Vertrauen in die Web-PKI zu kitten.

Private Videoüberwachungen

Das Bundesverwaltungsgericht hat am 27.03.2019 bestätigt, dass die Regelung zur Videoüberwachung im neuen § 4 BDSG mangels Reichweite der Öffnungsklausel der DSGVO nicht für private Stellen gilt. Private Videoüberwachungen sind allein nach Art. 6 Abs. 1 f) DSGVO (Rechtsgrundlage) und insbesondere Art. 13/14 DSGVO (Informationspflichten) zu beurteilen.

Die Entscheidung in der Sache – rechtswidrige Live-Überwachung einer Zahnarztpraxis – erging noch zur alten Rechtslage (§ 6b BDSG aF). Bei den Aussagen zu § 4 BDSG nF handelt es sich also streng genommen eher um ein *obiter dictum*: Das Gericht prüfte, ob eine Pflicht der Aufsichtsbehörde zur Überprüfung der Umsetzung besteht. Nach Überzeugung des Gerichts gelten die Öffnungsklauseln in Art. 6 Abs. 2, 3 DSGVO nur für hoheitliche Verarbeitungen. Für die Prüfung der Erforderlichkeit und Angemessenheit einer Überwachung dürfte es trotz der spezifischeren Ausführungen des § 4 BDSG weitgehend bei den bisherigen Maßstäben bleiben.

Sysmon 10

Das am 14.06.2019 aktualisierte Microsoft-Werkzeug Sysmon (v10.1) unterstützt mit 21 spezifischen EventIDs die Aufzeichnung detaillierter Logs des Laufzeitverhaltens eines Windowssystems (Server wie Clients). Für EventIDs 1 (ProcessCreate) und 7 (ImageLoad) wurde die Eigenschaft „Original FileName“ hinzugefügt, wodurch nun der aufrufende PE-Originaldateiname aufgezeichnet und nachvollziehbar wird. Die EventID 22 (DNSEvent DNS query) wurde ergänzt; sie wird erzeugt, wenn ein Prozess eine DNS-Abfrage ausführt, unabhängig davon, ob das Ergebnis erfolgreich ist oder fehlschlägt: sehr hilfreich bei der Vorfallsanalyse von Anomalien, Schadsoftware oder Datenexfiltrationen, da eine DNS-Protokollierung mit einer spezifischen Prozesszuordnung auf Urheber und Securityidentifier (SID) hinweist.

Diese Erkenntnisse gewinnt man allerdings nur, wenn Sysmon produktiv installiert ist. Mit einem eigenen Symon-Config-File lassen sich die laufenden Ereignisse (Events) in einer zentralen Logauswertung sammeln und auswerten.

Alte Antwort, neue Bedeutung

Am 13.06.2019 hat der Europäische Gerichtshof (EuGH) im Streit zwischen Google und der Bundesnetzagentur entschieden, dass GMail kein elektronischer Kommunikationsdienst nach § 3 Nr. 24 TKG bzw. RL 2002/21/EG ist. Definitionsmerkmal eines Kommunikationsdienstes sei, dass der Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Unstreitig übertragen E-Mail-Provider und andere Anbieter von vergleichbaren Internetdiensten (wie Messengerdienste) die Signale jedoch nicht selbst, sondern bedienen sich der durch Access-Provider angebotenen Infrastruktur.

Die Bedeutung der Entscheidung wird eingeschränkt durch die bevorstehenden Neuregulierungen der bereits bis Dezember 2020 umzusetzenden RL 2018/1972/EU und der ePrivacy-Verordnung. Beide Gesetzgebungen schaffen Rechtsrahmen, die direkt auf E-Mail-Dienste und vergleichbare Angebote zielen. In der Übergangszeit beschränkt das Urteil zwar einerseits u. a. staatliche Zugriffsrechte, andererseits verschärft es die Unsicherheit: Bisher wurde bezüglich des Telekommunikationsgeheimnisses und des Umgangs mit Verbindungsdaten regelmäßig Telekommunikationsrecht angewendet. Zugleich verdrängen die sehr allgemeinen DSGVO-Bestimmungen die Datenschutzbestimmungen des Telemediengesetzes – eine Situation, die der Gesetzgeber baldmöglichst klären sollte.

Secorvo News

Secorvo@itsa

Vom **08. bis 10.10.2019** ist Secorvo wieder auf der it-sa in Nürnberg vertreten. Am Stand 10.1-630 zeigen wir Ihnen u. a. ISMS ready2go und DSMS ready2go, unsere Lösungen für das Informationssicherheits- und Datenschutz-Management. Sie sind herzlich eingeladen, bereits vorab einen Termin mit uns zu vereinbaren. Gerne schicken wir Ihnen auch einen Registrierungscode, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können.

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets‘) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige 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

Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (KTH Royal Institute of Technology, Stockholm/SWE)
August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
23.-26.09.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-27.09.	heise devSec 2019 (dpunkt-Verlag, Heidelberg)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knöppler, Michael Knopp, Jannis Pinter, Jochen Schlichting, Christian Titze

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