Secorvo Security News

Februar 2024

Schöne neue Welt

Wie wunderbar haben wir uns damals die Zukunft vorgestellt: digitale Dokumente statt ressourcenfressender Papierberge, Online-Erledigungen statt Ämterwarteschlangen und ortsunabhängig verfügbare Warenvielfalt in digitalen Riesenkaufhäusern.

Lange sah es so aus, als ob diese Digitalisierungsträume tatsächlich in Erfüllung gehen: Einheitliche Dateiformate (PDF, mp3, jpg) machen Texte, Musik und Bilder universell austauschbar, mobile Endgeräte erlauben ein „Always on" ohne nennenswerte Technik-Kenntnisse und zahlreiche Dienste erleichtern das tägliche Leben – wie Online-Shops, Navigation oder Videokommunikation.

Doch nach und nach drängen die Schattenseiten dieser Entwicklung ins Licht: Während der Papierverbrauch pro Kopf nur marginal sinkt (2000 waren es 232 kg je Bundesbürger, 20 Jahre später immer noch 228 kg) steigt unser Energieverbrauch enorm: Jeder Smartphone-Nutzer verursacht jährlich im Schnitt einen Stromverbrauch von rund 50 kWh in Rechenzentren – zuzüglich Energie und Rohstoffen bei der Produktion des Geräts. Derweil lassen Online-Shops die Zahl der Pakettransporte explodieren und die Innenstädte veröden. Und die exzessive Nutzung von „sozialen" Medien schafft ein neues Prekariat: Anstatt den Zugang zu Wissen zu demokratisieren bekommt Konzentrationsfähigkeit Seltenheitswert, nehmen Depressionen zu und weicht der Respekt im zwischenmenschlichen Umgang zunehmender Grobheit. Und obendrein lässt sich der Wahrheitsgehalt von Informationen (Fake News, Bilder, Filme) immer schwerer beurteilen.

Datenschutz, ursprünglich ein Abwehrrecht gegen staatliche Überwachung, kämpft heute vornehmlich gegen die Begehrlichkeiten von Werbetreibenden und soziale Übergriffe wie Doxing (am 19.02.2024 sogar ein Thema in der Tagesschau). Einziger Trost: Solange die „Digitalstrategie Deutschland" im Konzeptmodus verharrt, müssen wir uns wenig Sorgen um staatliche Kontrolle machen.

Security News

Ene mene muh

Im 20. Jahrhundert war die Domänenwelt noch in Ordnung: Es gab Top-Level-Domänen (TLD) wie .com oder .gov und länderspezifische wie .de oder .at. Dann übernahm 1998 die neu gegründete ICANN die Domänenherrschaft und begann weitere, so genannte „generische" TLD (gTLD) einzuführen. Seit 2012 kann jeder, der 185.000 $ übrig hat, eine gTLD kaufen; inzwischen gibt es über 1.200.

Einige Hersteller nutzen unregistrierte TLDs für die einfache Erreichbarkeit ihrer Produkte in internen Netzen. So z. B. die Router von AVM (fritz.box) und O2

(o2.box). Doch seit dem 11.11.2016 (sic?) gibt es die gTLD .box – und am 22.01.2024 wurde die Domäne fritz.box registriert. Wer seitdem die Namensauflösung nicht von seinem Router vornehmen ließ, landete beim Aufruf der Admin-Oberfläche auf einer externen Webseite. inzwischen erscheint ein „Suspended"-Hinweis.

Dasselbe Risiko droht bei internen TLDs. Bereits seit 2020 diskutiert die ICANN daher über die Einführung von Private Use TLDs und hat anlässlich dieses Vorfalls am 24.01.2024 angekündigt, zumindest .internal zu schützen. Betroffene Hersteller könnten natürlich auch ihre intern genutzte Domäne extern registrieren. Wer weiterhin nicht registrierte gTLDs nutzt, sollte allerdings die Liste der registrierten gTLDs im Auge behalten.

Post-Quantum-Einsatz

Noch ist kein Quantencomputer bekannt, der klassischen Public-Key-Verfahren gefährlich werden könnte. Doch könnte ein Angreifer Kommunikation mitschneiden und sie in 10 oder 20 Jahren mit einem hinreichend mächtigen Quantencomputer entschlüsseln. Als eines der ersten Unternehmen hat Apple auf diese Bedrohung reagiert und kündigte am 21.02.2024 in einem Blogartikel an, solche Angriffe auf iMessage mit dem neuen Schlüsselaustauschverfahren PQ3 zu verhindern. Der hybride Schlüsselaustausch (von der NSA abgelehnt, siehe SSN 1/2024) besteht aus einem klassischen (P-256 ECDH) und einen Post-Quantum-Schlüsselaustausch (Kyber-1024). Die beiden Teilschlüssel bilden zusammen den Sitzungsschlüssel. Ein „store-now–decrypt-later"-Angreifer muss so beide Verfahren brechen können, um an den Schlüssel zu gelangen.

Auskunftskosten

Am 05.02.2024 verurteilte das Amtsgericht Lörrach einen Telefonvertrieb, die vorgerichtlichen Anwaltskosten für ein Auskunftsersuchen zu einer rechtswidrigen Verarbeitung zu erstatten. Denn juristischen Laien sei es nicht zumutbar, den Auskunftsanspruch selbst durchzusetzen. Das Urteil hat jedoch keine Bindungswirkung über den Fall hinaus, daher müssen Verantwortliche nicht widerspruchslos geforderte Kosten übernehmen. In der Regel dürften Auskunftsersuchen zumutbar sein, da Auskunftssuchenden zahlreiche Mustervorlagen der Aufsichtsbehörden zur Verfügung stehen.

Neues Website Audit Tool

Der Website Evidence Collector des europäischen Datenschutzbeauftragten sammelt auf Webseiten Nachweise für die Speicherung und den Transfer von personenbezogenen Daten (SSN 10/2023). Am 28.01.2024 hat der Europäische Datenschutzausschuss ergänzend das Website Auditing Tool veröffentlicht. Es besitzt eine grafische Oberfläche mit integriertem Chromium-Browser, was die manuelle Prüfung von Webseiten deutlich erleichtert. So lassen sich beispielsweise Datenübertragungen vor und nach einer Einwilligung einfacher prüfen als mit dem Website Evidence Collector. Auch das Website Audit Tool kann Prüfberichte erstellen; außerdem lassen sich

gespeicherte Webseiten zur erneuten Prüfung importieren. Das Tool ist Open Source (EUPL 1.2) und kostenlos; es kann von der EU-Webseite code.europa.eu heruntergeladen werden.

Private Key

In einer (später noch ergänzten) Meldung räumte die AnyDesk Software GmbH am 02.02.2024 die Kompromittierung ihrer produktiven Systeme ein. Da auch Zertifikate für die Codesignatur zügig gesperrt wurden, drängt sich der Verdacht auf, dass die Angreifer deren Private Keys erbeutet haben.

Zwar belegt eine Codesignatur nicht, dass die signierte Software korrekt und frei von Schadsoftware ist – sie soll nachweisen, dass die Software vom Hersteller freigegeben und nach der Auslieferung nicht mehr verändert wurde. Wer jedoch den Private Key für die Codesignatur kennt, kann modifizierte Software im Namen des Herstellers signieren.

Daher sollte der Private Key zu einem Codesignatur-Zertifikat in sicherer Hardware (Smartcard, HSM o. ä.) gespeichert werden, um einen Schlüsseldiebstahl zu erschweren und aufdecken zu können. Auch lässt sich ein Hardware Key einfacher an einen neuen Codesignierer übergeben.

Genau dies fordert das CA/Browser-Forum seit dem 01.06.2023 verbindlich für öffentliche Codesignatur-Zertifikate. Daher dürften AnyDesks neue Keys besser geschützt sein als deren kompromittierte Vorgänger.

HackGPT

Beim KA-IT-Si-Event am 22.02.2024 demonstrierte Dr. Swantje Westpfahl vom Institute for Security and Safety GmbH, wie man ChatGPT zur Vorbereitung eines Cyberangriffs verwenden kann. Wenige Tage zuvor hatte OpenAI berichtet, dass in Zusammenarbeit mit Microsoft Threat Intelligence fünf den Geheimdiensten von China, Russland, Nordkorea und des Iran nahestehende Gruppen identifiziert und gesperrt worden waren, die ebenfalls versucht hatten, OpenAI-Tools unter anderem für die Vorbereitung von Phishing-Angriffen zu nutzen.

Secorvo News

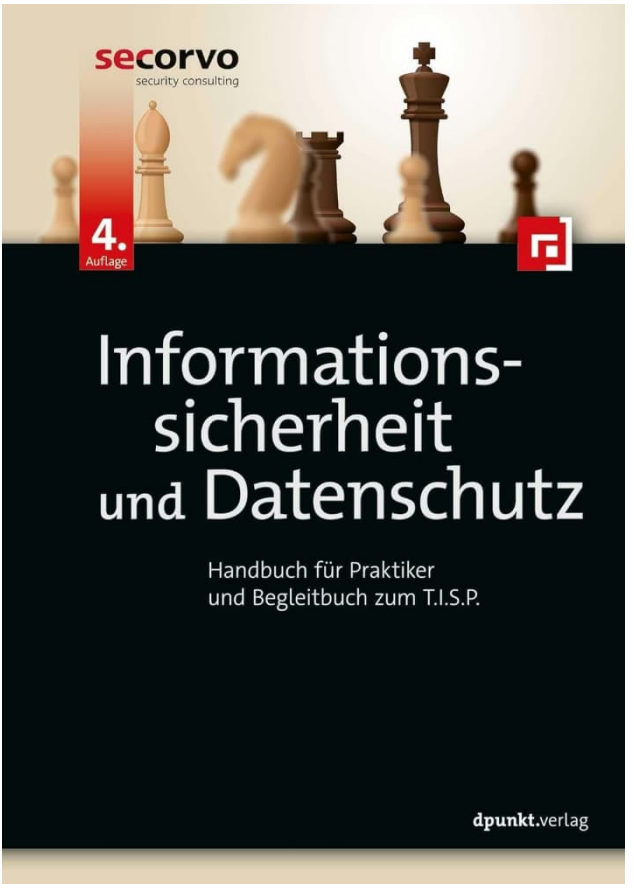
Vierte Auflage

Vor 17 Jahren fassten wir den schon damals verwegenen Beschluss, die wichtigsten Grundlagen der selten um neue Themen verlegenen Informationssicherheit zu verschriftlichen. Vier Jahre später erschien tatsächlich das „Secorvo-Buch“ mit dem Titel „Zentrale Bausteine der Informationssicherheit“ als Begleitbuch zum T.I.S.P. In die drei Jahre später erschienene zweite Auflage nahmen wir 2014 weitere wichtige Themen wie „Rechtliche Aspekte“, „IPv6“ und „Incident-Management“ auf; das Werk wuchs dadurch auf 26 Kapitel. Die dritte, gründlich überarbeitete und aktualisierte Auflage erschien dann 2019 unter dem Titel „Informationssicherheit und Datenschutz“ im dpunkt-Verlag.

Seit dem 07.03.2024 ist nun die vierte, aktualisierte und ergänzte Auflage erhältlich. Sie ist auf über 900

Seiten und 32 Kapitel angewachsen, räumt dem Datenschutz mehr Raum ein und wurde um einige aktuelle Themen wie „Cloud Security“ ergänzt.

Auch diese Ausgabe eignet sich sowohl zum Selbststudium als auch für die systematische Vorbereitung auf die T.I.S.P.-Zertifizierung – ein Qualifikationsnachweis, den inzwischen mehr als 2.000 Informationssicherheitsexperten erworben haben.



Wir freuen uns über Ihre Rückmeldungen, Kommentare und Rezensionen – und hoffen, Ihnen mit der Neuauflage des Handbuchs einige wertvolle Erkenntnisse und Einsichten zu bieten.

Seminare

In der Woche vom **15. bis 18.04.2024** bieten wir das Seminar PKI – Grundlagen, Vertiefung, Realisierung an, das von unserem PKI-Experten Hans-Joachim Knobloch geleitet wird.

Und vom **22. bis 25.04.2024** dreht sich beim im vergangenen Jahr neu konzipierten und aktualisierten TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) alles um sichere Software-Entwicklung – mit der Möglichkeit einer anschließenden T.P.S.S.E.-Zertifizierung.

Die nächste Möglichkeit zur Vorbereitung auf die T.I.S.P.-Zertifizierung bieten wir Ihnen vom **24. bis 28.06.2024**.

Es gibt noch freie Plätze: Sichern Sie sich den Frühbucherrabatt. Die Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

No risk, no fun

Im Zentrum des Informationssicherheits-Managements stehen die Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Kai Jendrian (Secorvo) wird in seinem Vortrag auf dem KA-IT-Si-Event am **11.04.2024** Einblicke in seine Erfahrungen aus 18 Jahren Beratungstätigkeit zur Informationssicherheit geben – mit einem besonderen Augenmerk auf der Bewertung von Risiken und der Abschätzung von Eintrittswahrscheinlichkeiten. Freuen Sie sich auf praxiserprobte Ideen für die Bewältigung der Herausforderungen beim Risikomanagement – und den Erfahrungsaustausch beim anschließenden „Buffet-Networking".

Wir freuen uns auf Sie beim Fraunhofer IOSB – und empfehlen bei Interesse eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover)
11.-15.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	GI Sicherheit 2024 (Gesellschaft für Informatik, Worms)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
22.-24.05.	25. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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