secorvo
security consulting

Secorvo Security News

Oktober 2024

Parkinson reloaded

Wer seit Jahrzehnten in der IT zu Hause ist, erinnert sich sicherlich noch an die Euphorie, mit der in den 90er Jahren die Digitalisierung herbeigesehnt wurde: endlich einfache, schnelle, bürokratie- und medienbruchfreie, von jedem Ort und zu jeder Zeit nutzbare Dienste.

Die Wirklichkeit entpuppt sich zunehmend als das erschreckende Gegenteil. Das liegt nicht allein daran, dass die Fortschritte in der Digitalisierung der öffentlichen Verwaltung oder hochregulierten Bereichen wie dem Gesundheitswesen eher in homöopathischen Dosen erfolgen – dank IT wachsen Zahl und Umfang von Papierdokumenten noch immer. Der Gesetzgeber bremst derweil durch detailliert regulierende Eingriffe, wie z. B. die Spezifikation der E-Rechnung, die keine reine PDF-Datei mehr sein darf: Viel Umstellungsaufwand ohne nennenswerte Verbesserung der Abläufe, denn zahlreiche Buchhaltungssysteme werten PDF-Dateien bereits heute automatisch aus.

Nicht zuletzt sind es Sicherheitsmechanismen, die zur wachsenden Komplexität eigentlich einfacher Prozesse beitragen: Kaum noch ein wichtiger Account, der nicht durch eine Zwei-Faktor-Authentifizierung geschützt wird – hier mit einem Chip-TAN-Generator, dort mit einem FIDO-Token, da mit einer SMS oder einem Telefonanruf, dann wieder mit einer Authenticator-App und schließlich mit einem photoTAN-Gerät. Und wehe, man wechselt einen Anbieter oder gar das defekte Smartphone – dann ist man Tage damit beschäftigt, sich neue Initialisierungsbriefe zusenden zu lassen oder seine Identität zu bestätigen, denn der hinterlegte Personalausweis ist wahrscheinlich zwischenzeitlich abgelaufen.

Offenbar schlägt da eine Variante des Parkinsonschen Gesetzes zu: „IT breitet sich in genau dem Maß aus, wie Geld für ihre Erweiterung zur Verfügung steht." Wenn wir so weitermachen, brauchen wir jedenfalls eines nicht mehr fernen Tages ein „IT-Abbau-Gesetz".

Inhalt

secorvo
security consulting

Security News

Drum prüfe... öfter

Apple schlug dem CA/Browser-Forum am 08.10. 2024 vor, die maximale Gültigkeitsdauer von öffentlichen TLS-Serverzertifikaten schrittweise auf 45 Tage zu begrenzen – Google war 2023 mit einem ähnlichen Vorhaben gescheitert. Dadurch soll die Bedeutung von Sperrmechanismen abnehmen, denen Browser-Hersteller ohnehin skeptisch gegenüberstehen. Das Risiko durch überflüssige oder gar kompromittierte, aber nicht gesperrte Serverzertifikate würde sinken. Technisch würde das ACME-Protokoll weiter an Bedeutung gewinnen: Damit können Zertifikatsverlängerungen automatisiert alle 30 bis 40 Tage erfolgen und dabei jeweils die DNS-Namen validiert werden.

Gleichzeitig soll die „Cache"-Zeit für validierte OV/EV-Angaben auf 366 Tage, für DNS-Namen oder IP-Adressen sogar auf 10 Tage verkürzt werden. Bisher dürfen Trustcenter einmal validierte Unterlagen wie Handelsregisterauszüge bis zu 825 Tage lang wiederverwenden und sich so bei Verlängerungen eine aufwändige erneute Prüfung sparen.

Die Umstellung würde die Position der Browser-Hersteller gegenüber problematischen Trustcentern stärken (SSN 07/2024): Nach einem Vertrauensentzug stünden deren Kunden noch schneller ohne gültige Zertifikate da. Wer zahlreiche öffentliche Serverzertifikate nutzt, ist daher gut beraten, einen Zweitlieferanten in petto zu haben. Darüber hinaus könnte die kürzere Gültigkeit den Übergang zu Post-Quantum-Cryptography-Zertifikaten erleichtern, der ab etwa 2030 zu erwarten ist.

Patientengeheimnis

Am 04.10.2024 hat der Europäische Gerichtshof (EuGH) mit der „Lindenapotheken-Entscheidung" wichtige Grundsätze zu Gesundheitsdaten festgelegt. Sie liegen vor, sobald Informationen Rückschlüsse auf den Gesundheitszustand einer Person zulassen. Daten wie Name und Adresse, die normalerweise nicht zu den besonderen Kategorien personenbezogener Daten zählen, können als Gesundheitsdaten gelten, wenn sie mit Gesundheitsfragen in Verbindung stehen. Dieser Grundsatz gilt für alle besonderen Kategorien personenbezogener Daten.

Zugleich hat der EuGH klargestellt, dass Wettbewerber wettbewerbsrechtlich gegen Unternehmen vorgehen können, die gegen Vorgaben der DSGVO verstoßen – dafür sind keine vorausgehenden Maßnahmen der Datenschutzaufsichtsbehörden erforderlich. Die Vernachlässigung des Datenschutzes kann also neben hohen Bußgeldern auch kostspielige Streitigkeiten zur Folge haben.

Selbst ist der Versicherte

Ab dem 15.01.2025 sollen alle gesetzlich Versicherten mit der Einführung der elektronischen Patientenakte (ePA) von den Vorteilen der Digitalisierung des Gesundheitssystems profitieren.

Der Hamburgische Beauftragte für den Datenschutz und die Informationsfreiheit hat am 17.10. 2024 darauf hingewiesen, dass die Nutzung der ePA freiwillig ist und ihr (im Voraus) widersprochen werden kann.

Die ePA kann nicht nur über die ePA-App auf Mobilgeräten genutzt werden. Auch in Arztpraxen oder Apotheken wird die ePA eingesehen und bearbeitet. Trotz technischer und organisatorischer Maßnahmen besteht daher das Risiko, dass Unbefugte Zugang zu diesen besonderen personenbezogenen Daten erhalten.

Allerdings können Versicherte selbst festlegen, welche Dokumente sie freigeben und welchen Leistungserbringern sie Zugriff gewähren. Der Grundsatz „data privacy by design" wurde berücksichtigt, allerdings ohne „data privacy by default": Ohne Widerspruch sind standardmäßig fast alle Dokumente allen Leistungserbringern zugänglich.

Gut Ding...

Am 27.09.2024 hat die irische Datenschutzaufsicht DPA ein seit 2019 laufendes Verfahren gegen Meta Ireland mit einem Bußgeld von 91 Mio. € beendet. Die Bemühungen des European Data Protection Boards, die Anforderungen der DSGVO auch gegenüber den großen Technologieunternehmen mit Sitz in Irland durchzusetzen, tragen langsam Früchte: Die Anzahl der Beschäftigten bei der DPA hat sich innerhalb der fünf Jahre, die das Verfahren dauerte, fast verdoppelt (2019: 110, 2023: 210).

Rechte und Freiheiten müssen auch in Zukunft gegenüber den Technologieriesen geschützt und verteidigt werden. Das gelingt nur, wenn die Aufsichtsbehörden EU-weit personell und finanziell ausreichend ausgestattet sind. Nur dann können Betroffene und Verantwortliche darauf vertrauen, dass ihre Anfragen bei den Behörden nicht in bürokratischen Schwarzen Löchern verschwinden.

Test-Phishing

Am 26.10.2024 wurde bekannt, dass Abgeordnete und Mitarbeiter des Bundestages im Rahmen eines Pentests mit unangekündigten Phishing-E-Mails „getestet" wurden. So sinnvoll Trainings mit Phishing-E-Mails auf den ersten Blick sein mögen –

sie verstellen manchmal den Blick auf das eigentliche Problem. Denn woran sollte der Empfänger einer solchen E-Mail verlässlich erkennen, ob ein unbekannter Link in einer E-Mail vertrauenswürdig ist – oder eben gerade nicht?

Viele Unternehmen markieren daher schon lange externe E-Mails durch farbige Balken oder Hinweise (z. B. in Office 365) und leiten in der E-Mail enthaltene Links, die auf externe Quellen verweisen, auf einen Proxy-Server um, der eine Warnung vorschaltet und den Link testet. Ein solcherart erzwungenes „Innehalten" kann zumindest verhindern, dass im HTML-Code einer E-Mail verschleierte Links in spontanem Vertrauen gedankenlos angeklickt werden.

Consumer Respect Act?

Am 10.10.2024 hat der Rat der EU dem Cyber Resilience Act (CRA) zugestimmt. Der CRA verpflichtet Hersteller von Soft- und Hardwareprodukten, die mit einem Netz oder einem anderen Gerät verbunden werden, zur Einhaltung von Cybersicherheitsvorgaben. Die Produkte müssen bestimmte Anforderungen an die Cybersicherheit erfüllen, und die Hersteller müssen Schwachstellen und Vorfälle behandeln und beheben.

Der CRA setzt auf der CE-Kennzeichnung und deren horizontalem Ansatz auf: Es werden allgemeine Anforderungen formuliert, die für alle Arten von Produkten gelten. So müssen Produkte etwa Sicherheitsupdates unterstützen, die der Hersteller innerhalb eines festgelegten Mindestzeitraums zur Verfügung stellen muss.

Das Prüfverfahren hängt davon ab, welcher Kategorie ein Produkt angehört: Kritische Produkte müssen durch externe Prüfer nach definierten Prüfkatalogen geprüft werden; bei wichtigen Produkten gelten weniger strenge Prüfvorgaben. Sonstige Produkte können vom Hersteller selbst geprüft werden.

Ebenfalls am 10.10.2024 erweiterte der Rat der EU die Produkthaftungsrichtlinie, die nun auch Software einschließt. Hersteller haften nun gegenüber Verbrauchern auch für defekte Software(-komponenten), etwa wenn diese fehlerhaft Daten löscht.

Eine Übersicht der Anforderungen des CRA stellte Markus Toran (Secorvo) am 02.06.2024 auf der GPN22 vor (Video). In einem Round Table beim CyberForum diskutiert er am 19.11.2024 die Herausforderungen und mögliche Lösungen für Unternehmen.

RoSIg

Am 28.10.2024 hat die Deutsche Energie-Agentur (dena) die Studie „Cyber-Fit" über die Rentabilität von Cybersicherheitsmaßnahmen vorgelegt. Darin behaupten die Autoren allen Ernstes, die Ausgaben für IT-Sicherheitsmaßnahmen nach dem NIS-2-Umsetzungsgesetz seien in wichtigen Einrichtungen „bereits im ersten Jahr rentabel".

Zum Beweis entstauben sie das Modell des „Return on Security Investment" (RoSI), das Anfang des Jahrtausends eine kurze Karriere machte – und verrechnen dabei Äpfel mit Birnen: Die durch die Schutzmaßnahmen reduzierte „Verlusterwartung" wird den Kosten der Maßnahmen gegenübergestellt. Echte Kosten werden so durch virtuelle Nicht-Verluste beglichen – eine solche Geldschöpfung wünscht sich jeder Unternehmer.

Secorvo News

Kompetenzzuwachs

Seit dem 01.10.2024 verstärkt der Jurist Ion Barza unser Datenschutz-Team. Herzlich willkommen!

Secorvo Seminare

Freie Plätze für Kurzentschlossene: Eine vertiefte Einführung in die sichere Software-Entwicklung bietet das T.P.S.S.E.-Seminar **vom 25. bis 28.11.2024** mit Praxisbezug und interaktiven Workshops – und im Anschluss die Möglichkeit, sich zertifizieren zu lassen.

Planen Sie schon Ihre Weiterbildung für nächstes Jahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender 2025. Wir freuen uns auf Ihre Anmeldung!

IT-Sicherheit hinter den Spiegeln

Zu einem ganz besonderen Jahresabschluss-Event lädt die IT-Sicherheitsregion Karlsruhe (FZI, KA-IT-Si und KASTEL) am **21.11.2024** in die Karlsruher Palazzo-Halle. Mitarbeiter von aramido demonstrieren in ihrem Vortrag „**Voice Cloning – faszinierend oder erschreckend einfach?**", wie mit KI-unterstützter Stimmenfälschung Angriffe möglich sind – und wie man sich davor schützen kann. Die Veranstaltung ist bereits ausgebucht, aber es gibt eine Warteliste.

Merken Sie sich schon einmal den Termin des Jahresauftakt-Events 2025 der KA-IT-Si am 20.02.2025 vor – die Einladung folgt Ende November. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2024	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
08.11.	DORA, NIS2 und CRA als Wegweiser für Informationssicherheit (GI, Frankfurt/Main)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.11.	Round Table Cyber Resilience Act (CyberForum, Karlsruhe)
20.-21.11.	ICSP 2024 (NIT, Jamshedpur/IND)
21.11.	IT-Sicherheit hinter den Spiegeln (FZI, KA-IT-Si, KASTEL, Karlsruhe)
25.-28.11.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
Dezember 2024	
09.-13.12.	Asiacrypt 2024 (IACR, Kolkata/IND)
09.-12.12.	Black Hat Europe 2024 (Black Hat, London/UK)
11.12.	IT Sicherheitsrechtstag NRW (IHK NRW, Bonn)
19.-20.12.	CSCML 2024 (IACR, CSCML, virtuell)

Fundsache

Am 26.09.2024 haben die IT-Sicherheitsbehörden der "Five Eyes"-Staaten Australien, USA, Kanada, Neuseeland und UK einen guten Ratgeber zum Finden und Beheben von Schwachstellen im Active Directory veröffentlicht.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

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