Secorvo Security News

November 2024

Nicht mehr allein

In den 90er Jahren benutzten Kinder noch ganz konventionelle Zahlungsmittel: Kevin McCallister entnahm die Ersparnisse seines Bruders Buzz einem Vorratsglas. In Teil 2 bezahlte Kevin Zimmer und Service im Plaza in New York schon mit der Kreditkarte seines Vaters, nachdem er seine Familie am Flughafen verloren hatte.

2024 sollen Minderjährige nach Auffassung von Google Kinder-Smartwatches wie das Fitbit Ace LTE als Zahlungsmittel verwenden, das seit dem 07.08.2024 in den USA Tap-to-pay unterstützt. Ab 2025 will Google mobiles Bezahlen für Kinder über die Google Wallet App ermöglichen, wie der Konzern am 30.10.2024 ankündigte. Eltern können ihren Kindern dann das Taschengeld über mit „Family Link" verwaltete Android-Smartphones in die virtuelle Geldbörse überspielen. Damit bekämen Eltern zugleich die Möglichkeit, das Ausgabeverhalten ihrer Kinder zu überwachen.

Nun darf ernsthaft bezweifelt werden, dass Kinder den besonnenen Umgang mit Geld mit einem digitalen „Wallet" besser erlernen als mit Bargeld. Auch sind Zweifel angebracht, dass aus überwachtem Kaufverhalten der Kinder später Souveränität erwächst.

Noch größere Zweifel muss man allerdings daran hegen, dass erzieherische Fragen bei diesem Angebot überhaupt eine Rolle spielen. Denn selbstverständlich kennt das Zahlungs- (und damit Konsum-) Verhalten der Kinder auch der Anbieter des Zahlungssystems: Google. Dabei fallen Daten von unschätzbarem Wert an: Die konsumbeeinflussende Wirkung von Online-Werbung oder Product Placements durch Influencer in sozialen Medien wird so unmittelbar messbar.

Dass aus jahrelanger systematischer „Verhaltensdressur" von Kindern und Jugendlichen nur in Ausnahmefällen Mündigkeit erwächst, dafür hält die Geschichte genügend Beispiele bereit. Ernüchternd, dass ein solches Angebot keinen Aufschrei provoziert.

Security News

Neue Berichte, alte Erkenntnisse

Am 12.11.2024 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den jährlichen Bericht zur Lage der IT-Sicherheit 2024 in Deutschland. Danach bleibt die IT-Sicherheitslage in Deutschland auch 2024 angespannt: Cyberkriminelle verfeinerten ihre Methoden, besonders bei Erpressungstrojanern (Ransomware) und Angriffen durch Überlastung (DDoS-Angriffe), Schwachstellen in IT-Systemen, vor allem bislang unbekannte Sicherheitslücken (Zero-Day) würden immer häufiger ausgenutzt und Angriffe auf kritische Infrastrukturen und Cloud-

Dienste nähmen weiter zu. Gleichzeitig würden die Abwehrmaßnahmen durch internationale Zusammenarbeit und neue gesetzliche Vorgaben wie NIS-2 und den Cyber Resilience Act gestärkt. Die digitale Bedrohungslage erfordere einen intensiveren Schutz in Unternehmen und Behörden, um Cyberangriffe abzuwehren und Schäden zu begrenzen.

Etwa zeitgleich aktualisierten MITRE und CISA am 20.11.2024 die Liste der 25 schlimmsten Schwächen bei der Software-Entwicklung. Erschreckenderweise finden sich auch alle hartnäckigen Schwachstellen unverändert noch immer in dieser Liste.

Keine bahnbrechenden neuen Einsichten – aber die Gewissheit, dass noch in vielen Einrichtungen an vielen Stellen „Hausaufgaben" zu erledigen sind.

Umsetzung des CRA

Das BSI hat am 20.09.2024 die Technische Richtline (TR) 03183 aktualisiert. Sie enthält die Anforderungen an Hersteller und Produkte, die sich aus dem Cyber Resilience Act (CRA) ergeben und ist nun in drei Teile gegliedert: generelle Anforderungen, Anforderungen an Software-Stücklisten (Software Bill of Materials, kurz: SBOM) und Vorgaben für Schwachstellenberichte und -meldungen.

Der neue erste Teil (Community Draft) konkretisiert die grundlegenden Anforderungen aus Anhang I des CRA; außerdem werden Untersuchungskriterien für Prüfer definiert. Im überarbeiteten zweiten Teil wird festgelegt, dass die SBOM-Formate SPDX oder CycloneDX in XML oder JSON verwendet werden. Eine Anleitung beschreibt, wie die Felder korrekt auszufüllen sind, z. B. welche Bezeichnung für eine Produktkomponente zu wählen ist.

Der ebenfalls neue dritte Teil (Community Draft) verpflichtet Hersteller zur Verwendung einer mit OpenPGP signierten security.txt-Datei nach RFC 9116. Außerdem wird ein Prozess zur Schwachstellenbehandlung definiert. Unternehmen sollen getrennte Verantwortlichkeiten für Product Security Incident Response Team (PSIRT) und Computer Security Incident Response Team (CSIRT) einrichten. Weiterhin werden Elemente für eine Unternehmensrichtlinie zum koordinierten Melden von Schwachstellen vorgegeben.

Die Richtlinie enthält zahlreiche konkrete Vorgaben zur Erfüllung der CRA-Anforderungen. Sie soll in die europäische Standardisierung eingehen. Die Kommentierungsphase für die Teile eins und drei endet am 24.11.2024.

EUCLEAK-Nachwehen

Schon bei der Publikation der EUCLEAK-Schwachstelle war klar, dass nicht nur YubiKeys betroffen sind, sondern auch andere Produkte, die Infineon-Sicherheitschips mit der ursächlichen Firmware-Bibliothek einsetzen (SSN 09/2024).

Die meisten der möglicherweise betroffenen Hersteller schweigen sich bislang darüber aus, ob ihre Produkte anfällig sind. Immerhin hat Infineon selbst im Oktober drei gefixte Firmware-Versionen für ihre TPM-Chips nach den Common-Criteria-Standards vom BSI rezertifizieren lassen. Für Endanwender ist das jedoch

nur begrenzt hilfreich, solange sie nicht wissen, ob der eigene PC eines der betroffenen TPM-Modelle enthält und wie sich die neue Firmware installieren lässt. Hier sind die PC-Hersteller in der Pflicht für Klarheit zu sorgen.

Der Fall zeigt außerdem, dass auch die akkreditierten Prüfer der Zertifizierungsstandards nicht dagegen gefeit sind, komplexe Schwachstellen zu übersehen. Ein Sicherheitszertifikat ist keine Garantie für schwachstellenfreien Code.

Vertrauen ist gut...

Der Ratschlag aus den SSN 10/2024, vorsorglich einen Zweitlieferanten für öffentlich gültige Zertifikate in der Hinterhand zu haben, hat sich schneller als erwartet als praxisrelevant erwiesen.

Ein für die Nutzer öffentlich gültiger Zertifikate folgenreicher Vertrauensverlust in der Beziehung zwischen einem Trustcenter und dem CA/Browser-Forum als Aufsichtsorgan ereignete sich vor wenigen Monaten, als Google Entrust und AffirmTrust das Vertrauen entzog (siehe SSN 07/2024).

Aber auch im Verhältnis zwischen Zertifikatsnutzern und ihren Lieferanten kann es – wie bei jedem Vertrag – zu Streitigkeiten über die Auslegung kommen. Wie am 13.11.2024 bekannt wurde, hat das Trustcenter Sectigo den Rahmenvertrag mit GÉANT, dem Zusammenschluss der europäischen Forschungsnetzwerke vorzeitig gekündigt. Die Konsequenzen beschäftigen nun unter anderem 450 deutsche Forschungseinrichtungen und Universitäten, die sich mit der unerwarteten Herausforderung konfrontiert sehen, dass Sectigo voraussichtlich ab dem 10.01.2025 über den GÉANT-Rahmenvertrag keine Zertifikate mehr liefert.

Geht doch!

Am 27.10.2024 hat die Sächsische Datenschutz- und Transparenzbeauftragte mitgeteilt, dass sie bei einer Kontrolle von 1.500 Webauftritten tatsächlich Verbesserungen in Sachen Datenschutz festgestellt hat. Im Frühsommer wurden 30.000 Webauftritte überprüft; davon wurden 2.300 beanstandet. In 1.500 Fällen konnte im Oktober 2024 festgestellt werden, dass es keine unzulässige Verwendung von Cookies oder Diensten wie Google Analytics mehr gab. Neben dem Kontrolldruck hat offenbar auch die Bereitschaft der Aufsichtsbehörde geholfen, die Verantwortlichen zu beraten, wie Webauftritte überarbeitet und „in legale Bahnen“ gelenkt werden können.

Fortsetzung folgt...

Im Juni 2020 hatte die Datenschutzkonferenz die „Orientierungshilfe für Anbieter von Telemedien“ in überarbeiteter Version veröffentlicht (SSN 06/2020). Sie wurde am 15.11.2024 durch die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten“ ersetzt, die nun die neue Rechtslage des TDDG und des DDG berücksichtigt.

Das Dokument enthält wertvolle Hinweise: Es geht insbesondere auf die Unterschiede zwischen TDDDG und DSGVO ein und beschreibt nachdrücklich die Anforderungen an eine wirksame Einwilligung. Ab-

gerundet wird das Dokument durch die sehr konkrete Darstellung der Anforderungen an Einwilligungsbanner auf Webseiten – eine wirkliche Hilfestellung für Webseitenbetreiber.

Vorsicht: Fälschung

Die Digitalisierung von Dienstleistungen und die urbane E-Mobilität hauchen alten Betrugsmethoden (SSN 10/2011) neues Leben ein: Nach Angriffen auf Ladesäulen und Strafzetteln mit falschen QR-Codes („Quishing“) geraten nun auch Parksäulen ins Visier der Täter. So geschehen in Hannover, wie die Polizei am 12.11.2024 berichtete. Betroffen sind Kundinnen und Kunden des Parkdienstleisters easypark. Die Methode ist nicht neu (SSN 04/2022), aber effektiv: Die falschen QR-Codes führen auf eine Internetseite, die die Zahlungsdaten abfragt und nahezu identisch mit der Originalseite ist, sodass der Betrug nicht sofort auffällt. Der Parkhausbetreiber easypark und die Landeshauptstadt Hannover informieren, wie man sich vor solchen Betrugsmaschen schützen kann. Wie im analogen Leben gilt auch hier: Keine Zahlung an unbekannte Empfänger.

Secorvo News

Secorvo Seminare

Unser Seminarbetrieb geht in die Winterpause.

Falls Sie über Weihnachten Ihre Weiterbildung 2025 planen möchten, werfen Sie doch einen Blick in unseren Seminarkalender. Im März bereiten wir Sie gerne auf die T.I.S.P.- und die T.P.S.S.E.-Zertifizierung vor. Wir freuen uns auf Ihre Anmeldung.

Cyber-Versicherung im Ernstfall

Risiken kann man ignorieren, reduzieren – oder transferieren. Mit der Zunahme erfolgreicher Cyberangriffe steigt daher auch die Nachfrage nach Cyber-Versicherungen. Im Februar 2024 widmete die BaFin diesem Thema sogar einen Fachartikel.

Aber wie das so ist im Leben: Erst im Ernstfall zeigt sich, was eine Vereinbarung wert ist. Denn nicht jeder Vorfall ist automatisch auch ein Versicherungsfall – angesichts der wachsenden Vorfallszahlen und sinkender Margen im Cyber-Versicherungsgeschäft wird aus einem Vorfall schnell ein Streitfall. Welche Fragen dabei zu klären sind und was Versicherungsnehmer schon bei Vertragsabschluss beachten sollten, erläutert anschaulich und spannend an realen Beispielen Dr. Christian Förster (Bartsch Rechtsanwälte) beim Jahresauftakt-Event 2025 der Karlsruher IT-Sicherheitsinitiative am **27.02.2025** um 18:00 Uhr im Saal Baden (IHK Haus der Wirtschaft). Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking".

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

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)
Januar 2025	
20.-22.01.	Omnisecure 2025 (in TIME berlin, Berlin)
Februar 2025	
11.-12.02.	32. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg
12.-14.02.	IT-Defense 2025 (cirosec, Leipzig)
19.-20.02.	ID:SMART Workshop 2025 (CAST e.V., Darmstadt)
27.02.	KA-IT-Si-Event „Wer zahlt die Zeche?“ (KA-IT-Si, Karlsruhe)
März 2025	
10.-14.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
17.-21.03.	31st Fast Software Encryption Conference (IACR, Rom/IT)
18.-20.03.	secIT 2025 (Heise Medien, Hannover)
24.-27.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza (Editorial), 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