Secorvo Security News

März 2023

Von Bäumen und Wäldern

Es gab eine Zeit in der IT-Sicherheit, da galten einfache, klare Regeln. So erforderte eine gute Authentifikation ‚Wissen' und ‚Besitz' und wurden Daten, die von außen durch die Firewall gelangten, grundsätzlich als ‚potentiell gefährlichen Inhalts' eingestuft.

Das war einmal. Nicht, dass diese Prinzipien in Frage stünden. Wohl aber kippt immer öfter die praktische Umsetzung. Drei Beispiele: Für den bequemen Zugriff vom Mobilgerät auf E-Mails oder die Unternehmens-Cloud verlässt man sich zunehmend auf die Authentifikation des Nutzers am Gerät – die nicht selten auf schwachen Wischcodes oder leicht zu täuschenden Fingerabdruck-Scannern beruht. „Moderne" Zahlungssysteme lassen sich gänzlich ohne Transaktions-Authentifikation nutzen – um keine Kunden an andere Anbieter zu verlieren, geht das inzwischen sogar mit der EC-Karte (bis 50 € und fünfmal in Folge) und über Apple oder Google Pay. Und damit wir unseren Terminkalender nicht mehr pflegen müssen, werden per E-Mail zugesandte Einladungen ungefragt von Outlook eingetragen.

Der Preis, den wir für diese Bequemlichkeiten zahlen, ist hoch. So werden schwache Authentifikationen durch immer ausgefeiltere Datenerhebungen und Profilbildungen kompensiert (entsprechen Höhe und Empfänger der Zahlung den Gewohnheiten? kommt sie von demselben Endgerät – und aus dem richtigen Land?) – mit den unvermeidlichen Begleiterscheinungen gelegentlicher Sperrungen durch „false positives" und einer Verhaltensanalyse, die selbst George Orwells Vorstellungsvermögen überstiegen hätte. Zugleich eröffnet die dadurch anwachsende Komplexität der IT immer wieder unerwartete Angriffsflächen – vom „Denial of Service" auf das Konto bis zur Outlook-Attacke via Termineinladung (siehe „Termin-Hack").

Dagegen helfen würde mehr Einfachheit: ein „Stopp" bei vermeidbarer Komplexität, sodass neben den Bäumen der Wald wieder in den Blick käme. Aber das wäre wahrscheinlich – kompliziert.

Security News

Termin-Hack

Am 14.03.2023 hat Microsoft eine kritische Lücke (CVE-2023-23397) in allen Outlook-Versionen gepatched, über die ein Angreifer mit einer präparierten E-Mail ohne Zutun des Empfängers den Net-NTLMv2-Hash des Nutzers abgreifen konnte. Die Schwachstelle existiert offenbar schon eine Weile – und wurde nachweislich schon seit April 2022 ausgenutzt. Am 20.03.2023 wurde ein Proof of Concept auf Github veröffentlicht. Man sollte übrigens Microsofts Empfehlung folgen und den Port TCP 445/SMB (ausgehend) an

der Firewall sperren – die Lücke ist offenbar noch ausnutzbar.

Die Details der Schwachstelle sind delikat. Wer einen Outlook-Kalendereintrag erzeugt, kann diesem Termin eine selbst gewählte Sound-Datei für den Erinnerungsalarm zuordnen. Wird der Termin an einen (externen) Teilnehmer geschickt, öffnet dessen Outlook zum Zeitpunkt des Alarms diese Sound-Datei. Verlinkt der Angreifer hier auf einen externen Server, dann versucht der Outlook-Client des Empfängers, sich mit dessen Credentials dort anzumelden…

Die Schwachstelle ist das Ergebnis einer Software-Entwicklungsstrategie, die automatisiertes „Eindringen" in eine fremde Infrastruktur zur Regel macht: Outlook trägt jede Terminänderung ohne Freigabe des Empfängers beim Eintreffen der E-Mail automatisch in dessen Kalender ein. Verwunderlich ist daher nicht die Schwachstelle, sondern die Tatsache, dass Spammer und Phisher diesen Mechanismus nicht schon längst nutzen – denn was macht ein Empfänger wohl mit einem Link in einem Termin, den er nicht zuordnen kann?

Produkthaftung für Software

Die National Cybersecurity Strategy der US-Regierung vom 01.03.2023 listet auf 35 Seiten, strukturiert in fünf „Säulen" (Schutz kritischer Infrastrukturen, Bekämpfung von Angreifern, Stärkung der Widerstandskräfte des Marktes, Investitionen in Widerstandsfähigkeit und Internationale Zusammenarbeit), zahlreiche Maßnahmen und Vorgaben zum Schutz digitaler Infrastrukturen. (Allein die kompakte Darstellung ist beispielgebend – die Cybersicherheitsstrategie der Bundesregierung vom 08.09.2021 benötigte 142 Seiten, davon allein vier für das Inhaltsverzeichnis.) Folgenreich könnte die Zuweisung der Verantwortlichkeit von Software-Unternehmen für Sicherheitsmängel sein: "*Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers*." Daraus lässt sich eine Haftung bei Pflichtverletzungen ableiten: Wer gegen Best Practices verstößt oder typische Fehler wiederholt, muss für daraus entstehende Schäden gerade stehen.

In Deutschland hält sich bisher die Auffassung, dass Software – juristisch – kein Produkt ist: Der Käufer erwirbt lediglich ein Nutzungsrecht. Ein Schritt zu mehr Herstellerverantwortung war die Einführung einer Aktualisierungspflicht zum 01.01.2022 (in § 475b und § 327f BGB). Mit dem EU Cyber Resilience Act vom 15.09.2022 will die EU-Kommission nun die Anforderungen an die Sicherheit von Software und den Umgang mit Schwachstellen stärker regulieren. Im Entwurf der neuen Produkthaftungsrichtlinie gilt Software als Produkt. Damit unterläge Software der Produkthaftung – eine gute Nachricht für Unternehmen, die sich schon heute um Software-Sicherheit kümmern.

Die Forderungen an die Hersteller im Anhang des Richtlinienentwurfs sind äußerst konkret: „*Products with digital elements shall be delivered without any known exploitable vulnerabilities*, (…) *with a secure by*

default configuration, (...) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data')."

Don't roll your own crypto

Die Implementierung von Krypto-Algorithmen ist fehleranfällig (SSN 12/2022). So darf beispielsweise die Zufallszahl, die der ECDSA für die Signatur einer Nachricht benötigt, nicht erneut verwendet werden. Daher wird diese Zahl auch „Nonce" (= number used only once) genannt. Eine am 06.03.2023 veröffentlichte Untersuchung von Kudelski Security zeigt eine weitere Angriffsmöglichkeit: Wird für ECDSA ein schlechter Pseudozufallszahlengenerator verwendet, dessen Ausgabewerte in einem polynomiellen (oder sogar linearen) Zusammenhang stehen, kann unter speziellen, aber plausiblen Umständen der private Schlüssel rekonstruiert werden. Als die Autoren ihr Verfahren an den Signaturen in der Bitcoin Blockchain ausprobierten, konnten sie den privaten Schlüssel von 762 Wallets (im Wert von rund 9,4 Mio. US$) rekonstruieren – dank fehlerhafter ECDSA-Implementierungen, die Nonces wiederverwendeten. Daher sollte – wo immer möglich – auf Standard-Krpyto-Bibliotheken und -Protokolle zurückgegriffen werden.

TrustPid freigegeben

Mit TrustPid sollen Mobilgeräte-Nutzer zukünftig nicht mehr durch Cookies oder Browser Fingerprinting, sondern durch ihre Internet-Provider getrackt werden (SSN 06/2022). Die Einwilligung der Nutzer wird über die Webseite verwaltet. Nach erfolgreicher Durchführung des Machbarkeitstests soll TrustPID nun europaweit eingesetzt werden; dafür hat die EU-Kommission am 10.02.2023 die wettbewerbsrechtliche Freigabe erteilt. Als technische Plattform für digitale Werbung in Europa haben die europäischen Mobilfunkanbieter Orange, Telefónica, Vodafone und Telekom ein Gemeinschaftsunternehmen mit Sitz in Belgien gegründet.

Trotz seiner Unzuständigkeit hat sich Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, zu TrustPid geäußert: Zwar erfolge der Einsatz auf der Grundlage einer Einwilligung der Nutzer, dennoch sei die besondere Vertrauensstellung, die Telekommunikationsanbietern zukommt, „nur schwer mit einem Tracking ihrer Nutzerinnen und Nutzer vereinbar". Außerdem müssten potenzielle Gefahren wie die Zusammenführung von pseudonymen Kennungen mit Login-Daten bei Webdiensten, die eine Re-Identifikation und die Verknüpfung von Tracking-Daten ermöglichen, verhindert werden. Fazit: Besser deaktivieren.

90-Tage-Zertifikate

Am 03.03.2023 hat das Chromium-Projekt von Google erneut eine drastische Verringerung der Gültigkeiten von Browser-Zertifikaten vorgeschlagen (und angekündigt, dies ggf. direkt im Chrome-Root-Programm zu verankern): Root-Zertifikate sollen maximal sieben, CA-Zertifikate bis zu drei Jahre und öffentliche TLS-Sever-Zertifikate nur noch 90 Tage gültig sein (bei Let's Encrypt ist das schon lange Praxis). Mit diesem Schritt

sollen CAs dazu gebracht werden, etwa alle fünf Jahre ihre Infrastruktur auf den aktuellen Stand der Technik zu bringen – und die Server-Betreiber, automatisierte Protokolle wie ACME zur Zertifikatsaktualisierung zu verwenden. Sollte sich der Vorschlag durchsetzen, wäre das der Anfang vom Ende des Geschäftsmodells der kommerziellen Zertifikatsanbieter. Zugleich könnte er die Entwicklung von ACME-Clients für Plattformen jenseits der verbreiteten Betriebssysteme und Webserver (wie Hypervisor, Appliances oder IoT-Schnittstellen) beschleunigen – und so die überfällige Automatisierung der Zertifikatsaktualisierung zum Standard machen.

Kontrolle ist besser

Für großes Erstaunen, nicht nur bei der Landesbeauftragten für den Datenschutz Niedersachsen, Barbara Thiel, hat die Entscheidung des VG Hannover vom 09.02.2023 zur ununterbrochenen Überwachung von Mitarbeitern mit Handscannern bei Amazon gesorgt (10 A 6199/20). Obwohl beim EuGH (Rechtssache C-34/21) gerade die Frage der DSGVO-Konformität des § 26 BDSG zur Entscheidung ansteht, ist das VG Hannover überzeugt, dass das berechtigte Interesse des Unternehmens hier die Interessen der Arbeitnehmer überwiegt. Die von Amazon geltend gemachten Zwecke zur Steuerung der Logistik und der Mitarbeiterqualifizierung sowie zur Schaffung objektiver Bewertungsgrundlagen für Feedbackgespräche seien (ge)wichtiger als der permanente Überwachungsdruck auf die Arbeitnehmer. Diese wüssten um die Überwachung und müssten angesichts der großen Anzahl offener Stellen auch keine Angst vor Arbeitsplatzverlust haben, wenn sie sich dieser Überwachung nicht aussetzen wollten. Zwar seien einige Punkte wie etwa die Speicherdauer grenzwertig, aber letztlich könne man sich der Argumentation von Amazon anschließen.

Unternehmen, die Überwachungsmaßnahmen planen, sollten ihre Motivation plausibel darlegen und dokumentieren – und sich in Niedersachen ansiedeln. Allerdings prüft die LfDI Niedersachsen gerade den Gang in die nächste Instanz.

Secorvo News

Secorvo Seminare

Machen Sie den ersten Schritt zum BSI Vorfall-Experten mit unserem Seminar „BSI Vorfall-Experte – Aufbauschulung“ vom **09. bis 11.05.2023.** Oder krönen Sie Ihre Qualifikation mit dem T.I.S.P.-Zertifikat: Beim vorbereitenden T.I.S.P.-Seminar vom **19. bis 23.06.2023** sind noch Plätze frei.

Das Seminarprogramm und weitere Informationen finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

AD = Anno Domini?

Wie realistisch ist es für Angreifer, mit frei verfügbaren und öffentlichen Informationen Domain-Administrator auf einem fremden System zu werden? Beim KA-IT-Si-Event am **04.05.2023** in der *Church* (CyberForum e.V.) zeigen die Ethical Hacker von aramido in ihrem Vortrag „In 30 min. zum Domain-Admin“ anhand von

realen Bedrohungen, wie ein Angreifer auf interne Systeme zugreifen und anschließend die gesamte Infrastruktur übernehmen kann, indem er Domain-Admin-Privilegien erlangt. Dabei wird auch auf mögliche Abwehrmaßnahmen und Best Practices für die IT-Sicherheit eingegangen.

Anschließend gibt es natürlich wieder den fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)

Fundsache

Am 23.03.2023 hat das BSI eine neue Technische Richtlinie (TR 03145-5) mit Anforderungen an den sicheren Betrieb von Public Key Infrastrukturen für technische Sicherheitseinrichtungen veröffentlicht (26 Seiten).

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, 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