Secorvo Security News

April 2025

Erpressbar

Drei Jahre ist es her, da erschrak Deutschland anlässlich des russischen Angriffs auf die Ukraine ob der Einsicht, dass rund 55% der Gaslieferungen aus Russland stammten – und 25% der deutschen Gasspeicher dem Energiekonzern Gazprom gehörten: Wir waren erpressbar. Die Verringerung dieser über Jahrzehnte gewachsenen Abhängigkeit gelang – und hat ein Vermögen gekostet. Doch seit über zehn Jahren stürzen wir uns – noch blauäugiger – in eine Abhängigkeit, die weit dramatischere Auswirkungen haben kann: die Nutzung amerikanischer Cloud-Anbieter für zentrale IT-Services. Nach dem Cloud-Report 2024 des Bitkom verfolgen 40% der deutschen Unternehmen eine „Cloud-only"- oder „Cloud-first"-Strategie. Hauptmotiv: Kostensenkung (62%). Dass das zum Bumerang wird, spüren gerade immer mehr Unternehmen – die Cloud-Anbieter drehen an der Preisschraube. Denn der Weg zurück ist den Firmen versperrt, die Cloud ein Oneway Ticket: Anbieter nehmen ihre On-Premise-Produkte vom Markt, und der interne Know-How-Verlust bei gleichzeitigem IT-Fachkräftemangel macht eine Rückkehr zum Eigenbetrieb zum riskanten Gewaltakt.

Weniger als 20% der Unternehmen setzten 2024 noch auf „On-Premise"-Lösungen – Tendenz: fallend. Und nun hat Amerika einen Präsidenten, dem fast jede Drohung recht ist, wenn sie der Durchsetzung seiner Interessen dient. So wird aus dem betrieblichen Risiko der Cloud-Abhängigkeit ein volkswirtschaftliches – und damit politische Erpressbarkeit: Ein Exportverbot für amerikanische Software-Dienstleistungen würde in Europa die Lichter ausgehen lassen.

Diese Befürchtung hat Jürgen Hill bereits kurz nach der Wahl Trumps geäußert. Am 30.03.2025 brachte Max Schrems seine Besorgnis in einem Interview mit der Süddeutschen Zeitung zum Ausdruck. Passiert ist bisher wenig. Vielleicht hat Max Muth recht, wenn er (in einem Essay der Süddeutschen vom 19.04.2025) schreibt: „Es wäre naiv zu glauben, dass Deutschland aus seinen Fehlern lernt."

Security News

Angriff aus dem toten Winkel

Das IT-Sicherheits-Unternehmen SecurityScorecard hat am 24.02.2025 die Analyse eines riesigen Botnets veröffentlicht. Es umfasst mehr als 130.000 kompromittierte Geräte, die großangelegte Passwort-Spray-Angriffe auf Microsoft 365-Konten ausführen; mutmaßlich stammt es aus China.

Die Bots nutzen Protokolle wie POP, IMAP und SMTP, die meist eine reine Passwort-Authentifizierung (Basic Authentication) verwenden. Von Entra ID werden sie

als „Non-interactive Sign-ins“ gewertet. In dieselbe Kategorie fallen jedoch auch automatisierte Reauthentifizierungen bei modernen Token-basierten Verfahren, die oft den Großteil der Anmeldeereignisse ausmachen – und deshalb von vielen Überwachungssystemen ausgeblendet werden. Die Aktivitäten des Bot-Netzes werden daher leicht übersehen. Zwar kann man die Erfassung erweitern – doch besser ist es, die Nutzung von Basic Authentication wo immer möglich zu beenden und abzuschalten.

Wege ins Paradies

Jeder zweite Login-Versuch im Internet nutzt kompromittierte Zugangsdaten, wie eine Studie von Cloudflare vom 17.03.2025 zeigt. Über 95% dieser Versuche erfolgen automatisiert. Besonders betroffen sind WordPress-Installationen: Hier führen in 76% der Fälle gestohlene Passwörter zu einem erfolgreichen Login. Der Sophos Active Adversary Report 2025 vom 02.04.2025 bestätigt diese Analyse: In 41% der untersuchten Fälle gelang Angreifern der Erstzugriff über gestohlene Anmeldedaten.

Auch wenn Managed-Detection-and-Response-Systeme (MDR) Angriffe schneller erkennen, beseitigt das nicht die Hauptursache: fehlende oder unzureichende Mehrfaktor-Authentifizierung. Sophos betont, dass Angreifer in vielen Fällen bereits binnen weniger Stunden die vollständige Kontrolle über ein Netzwerk erlangen, insbesondere dank „Altlasten“ wie ungeschützte VPN-Zugänge.

Rapid7 ergänzt das Bild in einem Blog-Beitrag vom 10.04.2025 mit aktuellen Zahlen: Über eine Million Brute-Force-Versuche mit Tools wie FastHTTP wurden im ersten Quartal 2025 beobachtet. Zwar führten 73% dieser Versuche zu Account-Sperrungen und weitere 26% scheiterten an falschen Passwörtern. Oft reichen jedoch wenige kompromittierte Konten, um schwere Sicherheitsvorfälle auszulösen.

Die Studien zeigen: Wer auf MFA verzichtet oder veraltete Systeme offen lässt, macht es Angreifern leicht. Einmal kompromittiert, bleibt den Unternehmen oft nur wenig Zeit, um den Schaden zu begrenzen. Sichere, einmalige Passwörter und verpflichtende MFA für exponierte und kritische Dienste, gezielte Zugangsbeschränkungen und aktives Monitoring sind heute Kernelemente eines wirksamen Schutzes.

Trau, schau, wem!

Troy Hunt, Betreiber von „Have I Been Pwned?“, berichtete am 25.03.2025 über eine raffinierte Attacke, bei der ein Angreifer Zugriff auf seine Mailingliste erlangte. Mittels einer überzeugenden Phishing-E-Mail brachte er Hunt dazu, seine Zugangsdaten einschließlich OTP händisch einzugeben – obwohl der Passwort-Manager die URL nicht erkannte und die Zugangsdaten daher nicht automatisch eintrug. Der Angreifer verschaffte sich damit vollen Zugriff auf Hunts Account.

Der Fall zeigt, dass auch Multi-Faktor-Authentifizierung (MFA) keinen perfekten Schutz garantiert: Gibt man die Zugangsdaten an der falschen Stelle preis, kann ein Angriff trotz MFA gelingen. Ein zunehmender Wildwuchs bei Domänennamen erschwert die

Zuordnung von DNS-Namen zu Diensten und damit deren Verwaltung in Passwort-Managern stark. Ständige Wachsamkeit bleibt daher ein wichtiges Element der IT-Sicherheit.

Konsolidierung

Viele Anbieter nutzen für ihre Online-Dienste unterschiedliche Domänennamen. Das erschwert es Nutzern, Phishing-Angriffe an der URL zu erkennen. Woran soll man auch festmachen, ob z. B. die URL login.microsoftonline-p.com zu Microsoft gehört? Sie gehört – und ist bei weitem nicht die einzige (siehe Microsoft 365-URLs und-IP-Adressbereiche).

2023 beschloss Microsoft, alle Clouddienste in cloud.microsoft zusammenzuführen – schrittweise und mit Redirects, um Seiteneffekte zu minimieren. Seit Juni 2024 werden Monat für Monat wichtige Anwendungen wie Excel, Word, PowerPoint und Outlook unter Microsofts eigene Top-Level-Domäne migriert, was vor Domain-Spoofing wie z. B. homographischem Phishing schützt. Ein Beispiel, das Schule machen sollte.

Lizenz zum Signieren

Die Gültigkeit eines Deutschlandtickets bestätigt eine digitale Signatur, die der Aussteller oder sein Dienstleister beim Kauf erzeugt. Sie bindet das Ticket an einen Gültigkeitsmonat sowie an Namen und Geburtsdatum des Inhabers.

Da der Code kopiert werden kann, gilt das Ticket nur zusammen mit einem amtlichen Ausweis. Dennoch entstehen den Verkehrsbetrieben durch Rückbuchungen bei Zahlungsvorgängen und Kopien Millionenschäden – die nun durch Ticket-Sperrlisten und Kontoverifikationen eingedämmt werden sollen, wie der Interessenverband der privaten Verkehrsunternehmen mofair am 23.04.2025 mitteilte.

Doch auch beim Schutz der Signierschlüssel hapert es zuweilen: Am 12.02.2025 ging durch die Presse, dass Käufer, die beim Fahrkartenshop D-Ticket.su ein Deutschlandticket erworben hatten, unvermittelt zu Schwarzfahrern geworden waren – der zur Prüfung benötigte Public Key war gesperrt worden. Offenbar war der Betreiber von D-Ticket.su, die RouteVibe Ltd, in den Besitz des (zwischenzeitlich gewechselten) Signierschlüssels des für das Wittenberger Busunternehmen Vetter GmbH ausgestellten und vom Dienstleister MoPla Solutions GmbH genutzten Schlüsselpaars gekommen: Es war wohl nicht in einem Hardwaremodul (HSM) gespeichert. Für öffentlich gültige Codesignaturen schreibt das CA/Browser-Forum das schon seit 2023 zum Schutz der Signierschlüssel vor.

Nachlässigkeiten

Adam Chester (SpecterOps) hat am 08.04.2025 aufgedeckt, wie wenig Sorgfalt die Entwickler von ADSelfService Plus (ManageEngine) walten ließen: Der Master-Key seiner Datenbank wird mit einem Beispiel-Passwort aus der Microsoft-Dokumentation „geschützt". Mehr noch: Die Installationsanleitung verwendet einen Domänenadministrator-Account als Dienstekonto. Zwar beschreibt der Hersteller im Berechti-

gungsleitfaden die Verwendung eines eingeschränkten Dienstekontos („Principle of Least Privilege“) – da die Berechtigungen jedoch für die gesamte Domäne gelten, bringt das keinen Sicherheitsgewinn. Die erforderliche Einschränkung auf bestimmte Organisationseinheiten wird nicht erwähnt.

Kein Wunder, wenn Angreifer bei solchen Herstellerempfehlungen leichtes Spiel haben.

Nachtigall, ick hör dir trapsen

Am 27.02.2025 hat Microsoft den Abschluss des „EU Data Boundary“ verkündet. Das Unternehmen wirbt mit mehr Datenresidenz und Transparenz: Europäische Kunden sollen sich sicher(er) sein können, dass ihre Daten innerhalb der EU und nicht etwa in den USA verarbeitet würden. Grundsätzlich ein guter Ansatz, auch vor dem Hintergrund, dass das Data Privacy Framework zunehmend auf tönernen Füßen steht. Allerdings werden dadurch nicht die durch den CLOUD Act verursachten Risiken aus der Welt geschafft (SSN 03/2019 und SSN 09/2019): Die US-Geheimdienste behalten die Befugnis, auch in europäische Datenbestände Einblick zu nehmen. Derzeit besteht kaum Zweifel, dass die USA davon auch Gebrauch machen würden.

Tatsächlich helfen kann nur, Produkte und Dienste rein europäischer Anbieter zu nutzen. Mehr digitale Souveränität in der EU wäre die bessere Lösung.

Das Buch zum Tool

1998 startete Bernhard Esslinger das Open-Source-Projekt „CrypTool“, um seine Kollegen bei der Deutschen Bank für IT-Sicherheit zu sensibilisieren. Es gelang ihm, daraus eine „Bewegung“ zu machen – hunderte engagierte Studenten, Krypto-Experten und -Begeisterte beteiligten sich in den vergangenen 25 Jahren an der Programmierung, der Dokumentation und der Entwicklung des didaktischen Materials. Das Projekt wurde vielfach ausgezeichnet und wird heute in Unternehmen, Schulen und Hochschulen eingesetzt. Im November 2024 hat Professor Esslinger nun das „CrypTool-Buch“ veröffentlicht – eine 750 Seiten füllende Einführung in kryptografische Verfahren und Protokolle an Beispielen mit CrypTool, dazu ein 250 Seiten starker Anhang mit Anleitungen und Leseempfehlungen.

Secorvo News

Kettenregeln

In der Softwareentwicklung bedient man sich heute zahlreicher Bibliotheken aus Open-Source-Software oder von Zulieferern. Dadurch wird es schwieriger, die große Zahl direkter und indirekter Abhängigkeiten zu überblicken und auf einem aktuellen Stand zu halten. Beim KA-IT-Si-Event am **15.05. 2025** im dm-dialogicum zeigt Christian Kühn (dmTECH), wie man automatisiert Transparenz über bekannte Schwachstellen in den verwendeten Bibliotheken sowohl im Entwicklungsteam als auch in der zentralen Sicherheitsorganisation herstellen kann. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch

beim „Buffet-Networking“. Es gibt noch einige wenige freie Plätze (zur Last-Minute-Anmeldung).

Secorvo Seminare

Wie Sie Public Key Infrastrukturen erfolgreich aufbauen und nutzen, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **23. bis 26.06.2025**. Und vom **22. bis 26.09.2025** bereiten Sie die Autoren des T.I.S.P.-Buchs auf die T.I.S.P.-Zertifizierung vor. Alle unsere Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2025	
12.-15.05.	PKC 2025 (IACR, Roros/NO)
13.-15.05.	26. Datenschutzkongress (EURO-FORUM, Berlin)
15.05.	Kettenregeln (KA-IT-Si, Karlsruhe)
19.-20.05.	CIO Cybersecurity Summit 2025 (CIO, München)
20.-22.05.	Datenschutztage 2025 (WEKA, Frankfurt)
26.-28.05.	BvD Verbandstage 2025 (BvD, Berlin)
26.-28.05.	OWASP 2025 Global AppSec (OWASP Foundation, Barcelona/ES)
Juni 2025	
02.-04.06.	DuD 2025 (COMPUTAS, Potsdam)
02.-04.06.	Entwicklertag 2025 (VKSI, GI, ObjektForum, Karlsruhe)
04.-05.06.	Security Forum Congress 2025 (Security Forum, Barcelona/ES)
23.-26.06.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
23.-26.06.	ACNS 2025 (LMU, ForDaySec, München)
30.06.-04.07.	10th IEEE European Symposium on Security and Privacy (IEEE, Venedig/IT)

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

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