secorvo
security consulting

Secorvo Security News

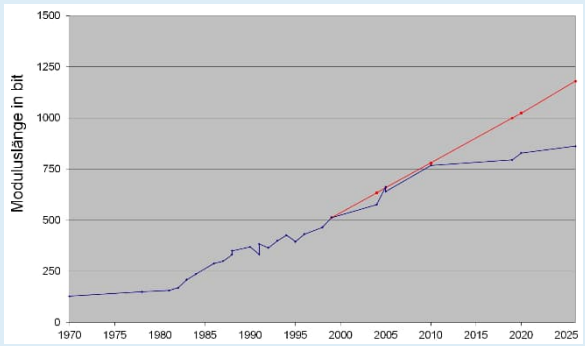
September 2026

Fakt(or)en

Am 03.09.2026 überraschte der amerikanische Forscher Eric Lu mit der Veröffentlichung der Lösung der „RSA-260-Challenge“ – der Zerlegung eines vor 25 Jahren von RSA Laboratories veröffentlichten, 862 Bit (260 Dezimalstellen) langen RSA-Moduls (öffentlichen Schlüssels) in seine Faktoren (den geheimen Schlüssel). Lu nutzte für die Faktorisierung kein neues Verfahren, sondern eine mit KI-Hilfe optimierte Implementierung des GNFS. Den Aufwand beziffert er mit 13,5 GPU-Jahren, eine Rechenleistung im Wert von rund 400 T$.

Bis zur nächsten Faktorisierung dauerte es nicht erneut 6,5 Jahre: Am 19.09.2026 veröffentlichte Stephen A. Weis die Lösung der „RSA-896-Challenge“ (270 Dezimalstellen), die er mit einer Claude-Portierung des GNFS-Algorithmus‘ auf GPUs fand. Sie dauerte 10 Tage und benötigte eine Rechenleistung von etwa 30 GPU-Jahren.

Zur Einordnung: Die Faktorisierung eines 1024-bit-RSA-Schlüssels benötigt etwa den 30fachen Aufwand; solche Schlüssel wurden vom BSI schon vor 25 Jahren für unsicher erklärt. Das Ergebnis bestätigt unsere Prognose aus dem Jahr 2002, dass niemand die RSA-1024-Challenge vor 2020 löst (SSN 5/2004, 12/2019). Es ist also weit davon entfernt, aktuelle 3072-bit-RSA-Schlüssel nach BSI-Empfehlung zu gefährden: Die Faktorisierung eines nur 2048 bit langen RSA-Keys erfordert ca. 1.200 Milliarden GPU-Jahre. In der Praxis sind Implementierungs- und Konfigurationsfehler der PKI das reale Sicherheitsrisiko.



Inhalt

Fakt(or)en

Security News

Mangelhafte Zaunpflege

Zu einfach

Immer dünneres Eis

Verdampft

Unsicheres Recycling

Secorvo News

In eigener Sache

Wissensdurst löschen

Patch me, if you can!

Veranstaltungshinweise

secorvo
security consulting

Security News

Mangelhafte Zaunpflege

Am 26.08.2026 veröffentlichten Tenable und SentinelOne eine gemeinsame Analyse von Angriffen auf Perimeter-Infrastrukturen wie Firewalls und VPN-Gateways. Dabei wurden Tenables Telemetriedaten zu verwundbaren Kundensystemen mit Erkenntnissen aus SentinelOnes Incident-Response-Einsätzen angereichert. In den betroffenen Systemen nutzten rund 39 verschiedene staatliche und kriminelle Gruppen Schwachstellen in Produkten von (u. a.) Fortinet, Citrix, Ivanti, Palo Alto Networks und Cisco aus.

Die Angreifer waren erfolgreich, weil die Betreiber ihre Systeme nicht rechtzeitig patchten. Im Median blieben Schwachstellen 122 Tage offen, besonders dringliche sogar 146 Tage. Citrix-Kunden ließen sich gar 461 Tage Zeit: In 54% der Umgebungen mit F5-Produkten fand sich mindestens eine von Angreifern genutzte Schwachstelle.

Ähnliches berichtet der diesjährige Data Breach Investigations Report von Verizon: Das Ausnutzen von Schwachstellen sei inzwischen mit 31% der häufigste initiale Zugriffsvektor bei erfolgreichen Angriffen. Auch Verizon stellt fest: Die Zeit bis zur vollständigen Behebung einer Schwachstelle stieg im Median von 32 auf 43 Tage. Organisationen mussten 16 bekanntermaßen ausgenutzte Schwachstellen (KEVs) schließen, fünf mehr als im Vorjahr. Vollständig behoben wurden nur 26%, im Vorjahr waren es noch 38%.

Abnehmende Patch-Disziplin bei gleichzeitig rapider Zunahme von mit KI-Unterstützung entdeckten Schwachstellen – das ist keine gute Entwicklung. Unsere Empfehlungen für das Einspielen von Microsoft-Patches (SSN 07/2026) gelten erst recht für sicherheitskritische Perimeter-Infrastrukturen.

Zu einfach

Rund 5.000 Dropbox-Nutzer wurden im August davon überrascht, dass unberechtigte Dritte auf ihre Daten zugreifen konnten, wie diverse Quellen am 01.09.2026 berichteten. Der Fehler lag jedoch nicht (allein) bei Dropbox: Wie viele andere Clouddienste erlaubt Dropbox bei persönlichen Konten eine Anmeldung über Identity Provider (IdP) wie Google oder Apple – ohne dass Nutzer dies explizit einrichten müssen. Auch mit einer Lenovo ID war das möglich.

Allerdings prüfte Lenovo beim Anlegen der ID nicht, ob eine registrierende Person tatsächlich Kontrolle über die angegebene E-Mail-Adresse besitzt (Double Opt-In). Ein Hinweis, dass Lenovo als IdP genutzt werden konnte, fand sich obendrein nur versteckt auf der Hilfeseite zu einer Werbeaktion. Dropbox-Team-Konten (Advanced, Business Plus, Enterprise) waren nicht betroffen: Hier muss der Administrator Single-Sign-on ausdrücklich aktivieren und dabei den IdP der Organisation hinterlegen.

Ein weiteres starkes Argument für Zwei-Faktor-Authentifizierung: Denn auch beim Dienstanbieter können sich ausnutzbare Schwächen im Anmeldeprozess verstecken.

Immer dünneres Eis

Am 29.06.2026 traf der US Supreme Court im Fall Trump ./. Slaughter eine folgenreiche Entscheidung: Der US-Präsident hatte ohne Angabe von Gründen Kommissare der Federal Trade Commission (der US-Datenschutzaufsichtsbehörde) entlassen. Das Gericht hält dieses Vorgehen für rechtmäßig. Damit wird die Unabhängigkeit der Aufsichtsbehörde untergraben – ein Kernpunkt des EU-US Data Privacy Framework. Fehlt sie, so genügt das für eine Aufhebung des Angemessenheitsbeschlusses nach Art. 45 DSGVO.

Ende Juli informierte die EU-Datenschutzbeauftragte Anu Talus die EU-Kommission über den Sachverhalt und bat um Prüfung des Angemessenheitsbeschlusses. Sollte die EU-Kommission den Beschluss aufheben, müssten Unternehmen wieder auf Standardvertragsklauseln und andere geeignete Garantien ausweichen (Art. 46 ff. DSGVO). Daher sollte umgehend geprüft werden, ob die abgeschlossenen Verträge mit US-Diensten diese bereits beinhalten, damit im Falle der Aufhebung personenbezogene Daten weiter in die USA übermittelt werden dürfen.

Verdampft

Im März 2026 hatten Drohnen im Iran-Krieg Rechenzentren und Stromversorgung von Amazon Web Services (AWS) in der Region Middle East (Bahrain) angegriffen, Löschwasser richtete weitere Schäden an. Nach dem Ausfall der Zone riet AWS zum Umzug in andere Regionen. Im April war die Availability Zone mec1-az2 in den Vereinigten Arabischen Emiraten von Angriffen betroffen und fiel ebenfalls aus.

Am 15.09.2026 räumte AWS nun auf seiner Statusseite ein: Ressourcen und Daten, die ausschließlich in diesen Regionen lagen, lassen sich nicht wiederherstellen. Für Schäden in mehreren Zonen zugleich seien weder die regionalen noch die zonenübergreifenden Dienste ausgelegt.

Neu ist diese Erfahrung nicht: 2023 verschlüsselte Ransomware beim dänischen Hoster CloudNordic auch die Backups; die meisten Kunden verloren alle Daten (SSN 08/2023). 2025 vernichtete ein Brand im

zentralen Regierungsrechenzentrum Südkoreas 858 TB Daten, für die es kein Backup gab (SSN 10/2025). Diesmal traf es einen Hyperscaler – und eine ganze Region.

Wer Daten in der Cloud speichert, sollte sie auch außerhalb der Region und unabhängig vom Cloud-Anbieter sichern: im eigenen Rechenzentrum oder bei einem zweiten Anbieter. Finanzunternehmen schreibt Art. 12 DORA seit dem 17.01.2025 vor, Daten auf „mindestens einem sekundären Verarbeitungsstandort (...) in geografischer Entfernung vom primären Verarbeitungsstandort" mit eigenem Risikoprofil abzulegen – und das Zurückspielen regelmäßig zu testen. Das BSI verlangt im IT-Grundschutz-Baustein CON.3 Datensicherungskonzept sogar in den Basis-Anforderungen, Sicherungen räumlich getrennt aufzubewahren – möglichst in einem anderen Brandabschnitt. In der Cloud heißen Brandabschnitte „Regionen".

Unsicheres Recycling

Entdeckt ein Angreifer ein mehrfach genutztes Passwort, eröffnet ihm das oft einen einfachen Eskalationspfad. Das gilt besonders für Dienstkonten, deren Passwörter sich häufig aus Konfigurationen, Skripten oder per Kerberoasting gewinnen lassen. Einen solchen Angriff beschrieb der Pentester Spencer Alessi am 02.09.2026.

Nutzt ein Administrator für ein privilegiertes Konto das gleiche Passwort wie für sein Benutzerkonto, untergräbt er damit die Kontentrennung, wie sie etwa ein Tiering-Modell vorsieht. Zwar ist es im Allgemeinen nicht einfach für einen Angreifer, identische Passwörter zu erkennen, denn meist sorgt Salting dafür, dass gleiche Passwörter als unterschiedliche Hashwerte gespeichert werden.

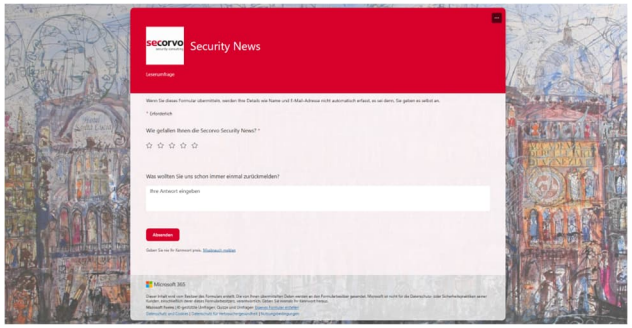
Windows und das Active Directory bilden jedoch eine Ausnahme: Der NT-Hash wird ohne Salt aus dem Passwort berechnet. Haben zwei Konten denselben NT-Hash, haben sie auch dasselbe Passwort. Angreifer müssen aufgrund einer Schwäche des Verfahrens das Passwort selbst nicht einmal kennen – der Hash lässt sich direkt zur Authentifizierung nutzen (Pass-the-Hash).

Daher sollte man die AD-Datenbank regelmäßig nach identischen Hashes durchsuchen. Das geht zum Beispiel mit den kostenlosen Werkzeugen DSInternals oder Specops Password Auditor (mit Replikationsrechten oder einer Kopie der Datenbank). Das löst nicht das Grundproblem, erschwert einem Angreifer aber Privilege Escalation.

Secorvo News

In eigener Sache

Seit knapp 25 Jahren informieren wir monatlich über unserer Ansicht nach wichtige Entwicklungen in IT-Sicherheit und Datenschutz. Da uns nur selten Rückmeldungen von Lesern erreicht, haben wir eine aufwandsarme Möglichkeit für ein anonymes Feedback geschaffen – und freuen uns auf Ihre Bewertung.



Wissensdurst löschen

Beim T.P.S.S.E. – Sichere Softwareentwicklung (**02.–05.11.2026**) zeigen wir Ihnen, wie Sie Security von Anfang an im Softwareentwicklungsprozess berücksichtigen, um Sicherheit systematisch zu integrieren und Schwachstellen zu vermeiden.

Wie Sie Sicherheitsvorfälle professionell bewältigen, üben Sie im Seminar Vorfall-Experte (BSI) (**10.–12.11.2026**) – praxisnah nach dem Curriculum des BSI und vorbereitend auf die BSI-Zertifizierung.

Unser Seminar T.I.S.P. TeleTrusT Information Security Professional (**16.–20.11.2026**) haben schon mehr als 400 Sicherheitsexperten besucht; über 95% der Teilnehmer haben das Seminar mit 4 oder 5 Sternen bewertet. Die Referenten sind Autoren des Fachbuchs „Informationssicherheit und Datenschutz" (4,9 ✶ bei Amazon).

Die Seminartermine für das Jahr 2027, Seminarprogramme und die Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Patch me, if you can!

Warum Linux-Server und Docker-Container regelmäßig und möglichst zügig mit Betriebssystem-Updates versorgt werden sollten und wie das bei dmTECH mit geringstem laufenden Aufwand implementiert wurde, zeigt Thomas Merz beim kommenden KA-IT-Si-Event am **22.10.2026** im dm-dialogicum in Karlsruhe. dmTECH betreibt die IT des gesamten dm-Konzerns in 14 Ländern, darunter geschäftskritische Systeme, über 4000 Filialen und ein Online-Shop für mehrere europäische Länder. Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Wir freuen uns auf Ihre Anmeldung (nur noch wenige Restplätze).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Oktober 2026	
20.10.	Swiss Cyber Storm 2026 (Swiss Cyber Storm Association, Bern/CH)
20.-23.10.	hack.lu (CIRCL, Luxembourg/LU)
22.10.	KA-IT-Si-Event „Patch me, if you can!“ (KA-IT-Si, Karlsruhe)
27.-29.10.	it-sa 2026 (itsa 365, Nürnberg)
27.-29.10.	26. IDACON 2026 (TALENTUS, München/virtuell)
November 2026	
02.-05.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
02.-06.11.	OWASP Global AppSec USA 2026 (OWASP Foundation, San Francisco/US)
03.11.	Cloud Identity Summit (Gregor Reimling, Frankfurt)
10.-11.11.	T.I.S.P./T.P.S.S.E. Community Meeting (TeleTrusT, Berlin)
10.-12.11.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
15.-19.11.	ACM CSS 2026 (ACM SIGSAC, Den Haag/NL)
16.-20.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-26.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Friederike Schellhas-Mende, Jochen Schlichting, Michael Schrempp, Liza Trace.

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Bahnhofplatz 8
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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.