Secorvo Security News

August 2026

Time Warp

Die Geschichte der Cybersicherheit begann vor ziemlich genau 40 Jahren: Im August 1986 deckte *Clifford Stoll*, Astronom am Lawrence Berkeley National Laboratory, den ersten bekannten Cyberangriff der Geschichte auf, der später als „KGB-Hack" bekannt wurde.

Eine 75-Cent-Abweichung in der Telefonrechnung seines Forschungsinstituts machte ihn stutzig. Nach akribischer Recherche entdeckte er, dass ein Hacker (wie sich später herausstellte der Deutsche *Markus Hess*) die Systeme des Instituts als „Sprungbrett" ins Arpanet nutzte (das Netz, aus dem später das Internet hervorging). Er erriet einzelne Passwörter von nicht mehr genutzten Accounts und konnte unter Ausnutzung eines Konfigurationsfehlers Superuserrechte erlangen. Von dort drang er in Militärcomputer ein.

Da weder das FBI noch die CIA sich für seine Hinweise interessierten, erfand Stoll „Honeypots", um den Angreifer zu ködern: Verzeichnisse, in denen er vermeintlich geheime Dateien über ein fiktives Militärprojekt im Kontext der Strategic Defense Initiative (SDI) ablegte. Nach Monaten kräftezehrender Beobachtung konnte er mit Unterstützung der Deutschen Bundespost über eine Fangschaltung die Verbindung nach Hannover zurückverfolgen. Eine deutsche Hackergruppe hatte dem sowjetischen KGB von Pentagon-Rechnern erbeuteten Quellcode und Daten verkauft. Sieben Mitglieder der Gruppe und der KGB-Mittelsmann wurden schließlich am 01.03.1989 verhaftet.

Seine Hackerjagd publizierte Stoll im August 1988 zunächst in Communications of the ACM (Vol. 31, No. 5: „Stalking the Wiley Hacker"). Im Jahr 1989 erschien die Geschichte als Buch – „Das Kuckucksei", ein von der ersten bis zur letzten der 450 Seiten spannender Bericht über die erste forensische Analyse eines Cyberangriffs, Pflichtlektüre für jeden IT-Sicherheitsexperten. Auf der diesjährigen DefCon 34 blickte der inzwischen 76jährige Forensiker wider Willen auf diese Anfänge zurück – seinen Vortrag sollte man sich nicht entgehen lassen.

Security News

Fast Klartext

Viele Dell-Rechner „verschlüsseln" ihr BIOS-Passwort nur dürftig, anstatt es zu hashen – das zeigt eine am 10.07.2026 publizierte Untersuchung von MDSec und AmberWolf. Dabei bleibt das erste Zeichen unverschlüsselt; die nächsten bis zu 31 Zeichen werden mit einem 20 Zeichen langen, sich wiederholenden festen Schlüssel XOR-verknüpft. Bei Passwörtern mit höchstens 12 Zeichen lässt sich der Schlüssel so direkt auslesen. Längere Passwörter lassen sich leicht

„entschlüsseln“, wenn ein früheres Passwort mit dem gleichen Zeichen begann, da alle alten Passwörter auf diese Weise „verschlüsselt“ gespeichert werden. Wegen eines Fehlers bei der Schlüsselableitung gibt es (pro Gerät) zudem nur 256 mögliche Schlüssel.

Betroffen sind vor allem ältere Plattformen, aber auch aktuelle Geräte wie der Wyse 5070. Dell stellt unter CVE-2026-40639 bislang nur für einen Teil der Geräte neue Firmware bereit.

Wie man Passwörter sicher vorhält – Hashen und Salting – ist seit 1979 bekannt. Warum Dell ohne Not darauf verzichtet, ist unerklärlich. Wer sich Passwörter „merken“ muss, sollte bewährte Verfahren wie Argon2 über Standardbibliotheken nutzen.

Kekspolicies

Am 12.08.2026 hat die Bundesbeauftragte für den Datenschutz (BfDI) mitgeteilt, dass Cookie-Banner abgeschafft und durch Einwilligungsverwaltungsdienste ersetzt werden sollten, da informierte Einwilligungen mit Bannern nicht umsetzbar seien.

Nach der BfDI-Befragung Datenbarometer verstehen viele Internetnutzer Cookies nicht, und 60% lehnen sie pauschal ab, wenn es der Cookie- Banner zulässt.

Der Digital Omnibus soll diese Änderung bringen. Wann dieses Reformpaket tatsächlich kommt, ist jedoch ungewiss. Bis dahin sollten Unternehmen kritisch prüfen, ob ihre eigenen Cookie-Banner eine informierte Einwilligung zulassen. Vor allem muss es möglich sein, alle nicht notwendigen Cookies und Trackingmöglichkeiten abzulehnen. Wird der Cookie-Banner vom Seitenbesucher ignoriert, ist das als Ablehnung zu werten. Die Aufsichtsbehörden können bis zur Reform der DSGVO von ihren Kontrollrechten Gebrauch machen und nicht rechtskonforme Cookie-Banner mit Bußgeldern belegen.

Domänen-Recycling

Täglich werden mehr als 65.000 Domänen sofort nach Ablauf neu registriert. Solche „Second-Hand- Domänen“ können wertvoll sein, denn sie erben die Reputation und Verbindungen ihrer Vorgeschichte. Dieses so genannte Domain Drop Catching ist ein lukratives Geschäft der Drop-Registrars. Dabei ist der Domänenablauf nicht immer beabsichtigt: Wer die Domäne nicht rechtzeitig verlängert, muss sie mitunter teuer von einem neuen Eigentümer zurückkaufen.

In einer am 13.08.2026 veröffentlichten dreiteiligen Artikelserie beschreibt der Softwarehersteller Infoblox, wie Kriminelle solche abgelaufenen Domänen verwerten. Teil 2 schildert das am Beispiel von „Sable Squirrel“, einer Gruppe, die mehr als 10.000 ehemals populäre Domänen besitzt und sie für illegale Spielcasinos, Streaming-Plattformen und die Verbreitung von Schadsoftware nutzt. Für den Ankauf ihrer Domänen hat sie schätzungsweise 7 Mio. € investiert. Teil 3 beschreibt Drittverwerter, die bereits für bösartige Zwecke verwendete, abgelaufene Domänen erwerben, um den verbleibenden Besucherverkehr weiterzunutzen.

Die Hackerin „Lina“ berichtete am 21.08.2026, wie sie die Domäne enum.org.uk übernehmen konnte und so für Telefonie bestimmte e164.arpa-DNS-Anfragen

abfing. Für gerade einmal 10 Euro hätte sie damit Anrufe zu einer Militärbasis abhören können. Und auf dem vergangenen Chaos Computer Congress beleuchtete Tim Philipp Schäfers den Missbrauch ehemaliger Behördendomänen.

Anstatt seinen Internetauftritt mit zahlreichen Domänen zu „schmücken" ist es häufig besser, Subdomänen zu verwenden – die lassen sich nach der Aufgabe nicht von Dritten missbrauchen.

Schlüssel unter der Matte

In seinem Vortrag auf der diesjährigen Konferenz Black Hat beschrieb IT-Sicherheitsforscher Michael Grafnetter (SpecterOps) am 05.08.2026 mehr als 20 Schwachstellen in Passkey-Implementierungen („Pass-the-Passkey").

Besonders kritisch war der fehlende Replay-Schutz in Entra ID, den Microsoft im Mai ergänzt hatte. Der Angriff mit „gebrauchter" Passkey-Signatur wurde dadurch erleichtert, dass Windows die WebAuthn Assertion inklusive Signatur ins Eventlog schrieb – vermutlich zu Debugging-Zwecken. Kein Einzelfall, wie die Schwachstellenkategorie CWE-532 zeigt („Insertion of Sensitive Information into Log File").

Will man sicherheitskritische Daten zum Debugging ausgeben, sollte der Code durch Conditional Compilation geschützt werden (Security by Design) oder – falls man das Feature auch im Produktionscode haben will – durch eine automatische Prüfung vor dem Release sichergestellt werden, dass es standardmäßig ausgeschaltet ist (Security by Default). Microsoft hat die beschriebene Schwachstelle CVE-2026-34348 im Juli-Update behoben; jetzt werden nur noch die ersten sechs Bytes der Signatur protokolliert.

Sicherer ohne App

Das IT-Sicherheitsunternehmen „A Security" veröffentlichte am 11.08.2026 eine Analyse mehrerer Schwachstellen der Videokonferenzlösung Zoom (CVE-2026-53413, -53414, -53415). Sie wurden von KI-Tools innerhalb von 24 Stunden gefunden und ermöglichten es, unbemerkt Schadcode an alle Teilnehmer einer Besprechung zu verteilen. Zoom behob die „Zoomsday" genannten Schwachstellen im Juni und Juli dieses Jahres. Sie betrafen die Zoom-Clients aller Plattformen: Windows, Mac, iPhone, Android und Linux; lediglich die Webanwendung war nicht betroffen. Dort bietet die Sandbox des Browsers zudem einen zusätzlichen Schutz.

Fast alle Videokonferenzlösungen gibt es als Webanwendung. Die „Native Clients" von Zoom, Microsoft Teams und Cisco Webex bieten zusätzliche Funktionen, u. a. verhindern sie über eine Ende-zu-Ende-Verschlüsselung (E2EE) ein Mithören durch den Anbieter. Wer eine Plattform nur gelegentlich nutzt und auf E2EE verzichten kann, sollte jedoch den Webclient vorziehen.

Wem gehören Ihre Daten?

Das amerikanische Medienportal Current berichtete am 11.08.2026 von einem Vorfall beim Fernsehsender Nine PBS, der sein Archiv an den Clouddienstleister

Open Source Storage (OSS) ausgelagert hatte. Dieser nutzte ein Rechenzentrum des Großanbieters Iron Mountain. Als OSS unangekündigt seine Dienste einstellte, verlor Nine PBS den Zugang zu ihrem gesamten Archiv, da Iron Mountain die Herausgabe der Daten verweigerte. Nine PBS musste den Zugriff vor Gericht einklagen; am 28.07.2026 wurde die Eigentümerschaft von Nine PBS an den Daten bestätigt. Ein ehemaliger OSS-Mitarbeiter fand sich bereit, bei der Wiederherstellung zu helfen.

Wer Daten bei einem (Cloud-) Dienstleister ablegt, sollte klären, wie sie im Notfall zugänglich sind – oder, besser noch, eine Kopie an einem anderen Ort speichern. Auch sollten die gesamte Kette der Unterauftragnehmer bekannt und der Zugriff auf die Daten vertraglich geregelt sein.

Secorvo News

KI-Transkriptionen

In Ausgabe 8/2026 der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) diskutiert Dirk Fox die datenschutzrechtlichen Anforderungen an eine KI-gestützte Transkription von (Online-) Meetings und gibt konkrete Umsetzungsempfehlungen für die Praxis.

Für Experten

Auf unseren Seminaren vertiefen Sie Ihr IT-Security-Know-how praxisnah und erhalten neue Impulse für Ihre tägliche Arbeit:

Die nach § 38 BSIG verpflichtenden, für die Erkennung und Bewertung von Informationssicherheitsrisiken erforderlichen Kenntnisse vermitteln wir Geschäftsleitungen in unserer vierstündigen NIS-2-Schulung am **15.10.2026**.

Das Seminar T.P.S.S.E. – Sichere Softwareentwicklung (**02.–05.11.2026**) stellt vor, wie Sicherheit in den Software Development Lifecycle integriert wird – SDLC in der Praxis.

Die nächste Vorbereitung auf die T.I.S.P.-Zertifizierung (TeleTrusT Information Security Professional) bietet unser T.I.S.P.-Seminar am **16.–20.11.2026**.

Die dreitätige Ausbildung zum Vorfall-Experten (**10.–12.11.2026**) befähigt Sie, Sicherheitsvorfälle professionell zu bewältigen – eine praxisnahe Schulung nach dem Curriculum des BSI mit der Möglichkeit zur anschließenden Zertifizierung.

Alle Termine, Programme und die Möglichkeit zur Anmeldung unter www.secorvo.de/seminare.

Patch me, if you can!

Thomas Merz (dmTECH GmbH) wird auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **22.10.2026** im wunderschönen dm-dialogicum vorstellen, 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 im großen Maßstab automatisiert wurde.

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 erwartet Sie der Erfahrungsaustausch am Buffet. Wie immer empfehlen wir eine baldige Anmeldung. Wir freuen uns auf Sie!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

September 2026	
28.09.-02.10.	TeleTrusT Information Security Professional (T.I.S.P.) (Secorvo, Karlsruhe)
29.-30.09.	secIT digital (Heise Medien, virtuell)
29.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt, hybrid)
Oktober 2026	
06.-09.10.	10th International Joint Conference on Electronic Voting (KIT, Universitaet Rovira i Virgili, Kozminski University, Université du Luxembourg, Tallinn/EE)
11.-15.10.	CHES 2026 (IACR, Antalya/TR)
12.-13.10.	ISMS verstehen und planen - Systematischer Einstieg (Secorvo, Karlsruhe)
20.10.	Swiss Cyber Storm 2026 (Swiss Cyber Storm, Bern/CH)
22.10.	Patch me, if you can! (KA-IT-Si, dm-dialogicum, Karlsruhe)
27.-29.10.	it-sa 2026 (itsa 365, Hannover)
27.-29.10.	26. IDACON 2026 (TALENTUS, München)

Fundsache

Mit Open Source Software: Security Principles and Practices hat die CISA auf 31 Seiten Empfehlungen zum sicheren Umgang mit Open-Source-Software vorgelegt – von der Auswahl und Pflege eingesetzter Komponenten über eigene Beiträge und Projekte bis zur Frage, wann ein KI-Modell wirklich Open Source ist.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, 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.