Secorvo Security News

Dezember 2025

Sicheres Wichteln

Ich mag Kryptografie. Mit jedem beliebigen Menschen sicher kommunizieren zu können, ohne ihn zuvor zu kennen, ist für mich Magie. Magie kann auch weh tun – wer je ein Zertifikat erneuert hat, weiß was ich meine. Doch in der Weihnachtszeit kann man Kryptografie schmerzfrei verwenden: beim Wichteln.

Was hat Wichteln mit Kryptografie zu tun? Beim Wichteln muss jeder Teilnehmer wissen, wen er beschenken soll – aber darf sich weder jemanden aussuchen noch selbst beschenken (müssen). Dazu braucht man eine zufällige (geheime) Zuordnung jedes Teilnehmers zu einem anderen – eine fixpunktfreie Permutation also. Sie ahnen es: Hier kommt Kryptografie ins Spiel.

Dafür genügen gewöhnliche Spielkarten. Jeder der n Wichtel erhält eine Herzkarte und n-1 Kreuzkarten sowie eine Nummer (von 1 bis n). Dann stapelt jeder seine Kreuzkarten und schiebt die Herzkarte an die seiner Nummer entsprechenden Stelle. Die Stapel werden gemischt und neu verteilt. Nun deckt jeder aus seinem Stapel die Karte an der Position seiner Nummer auf: Ist eine Herzkarte dabei, hat sich jemand selbst gezogen – und die Stapel müssen erneut gemischt und verteilt werden. Anderenfalls kennt jeder die Nummer desjenigen, den er beschenken muss – sie entspricht der Position der Herzkarte in seinem Stapel. Gegenüber dem klassischen Lose-aus-dem-Hut-Ziehen kann bei diesem Verfahren die Prüfung, dass niemand sich selbst beschenken muss, öffentlich erfolgen, ohne die Zuordnung der Wichtel offenzulegen.

Wer nun befürchtet, bei sehr vielen Wichteln hohe Kartenstapel tagelang mischen und tauschen zu müssen, wird erfreut sein zu hören, dass dreimaliges Mischen in der Regel ausreicht. Warum das so ist, passt nicht in ein Editorial - aber vielleicht in einen kalten Winterabend mit Papier, Stift und einer Tasse warmem Tee.

Tipp: Für große n nähert sich die Wahrscheinlichkeit, dass eine zufällige Permutation fixpunktfrei ist, dem Wert $1/e$ an. Magisch.

Security News

Frankreich handelt

Die französische Datenschutzbehörde CNIL verhängte am 03.12.2025 ein Bußgeld von 1,5 Mio. € gegen American Express: Das Unternehmen setzte nicht nur gleich beim Aufruf der Webseite Cookies, sondern auch bei Nichterteilung einer Einwilligung durch den Seitenbesucher – eine Praxis, die einige Firmen pflegen (SSN 7/2022).

In Deutschland bleiben solche Rechtsverstöße bisher ungeahndet. Zwar kündigte die Datenschutzkonferenz (DSK) am 12.12.2025 an, sich 2026 (erneut) zu Cookies und Tracking-Pixeln zu äußern – kaum zu erwarten, dass die Stellungnahme signifikant von der Position vom 14.11.2019 abweicht (SSN 11/2019).

Dabei sind Datenschutzverstöße auf Webseiten sowohl für Seitenbesucher (SSN 11/2020) als auch für Aufsichtsbehörden leicht (sogar automatisiert) feststellbar. Es ist schwer verständlich, warum Unternehmen an dieser Stelle hohe Bußgelder riskieren – zumal Nutzen und Aussagekraft von Website-Tracking-Daten äußerst fraglich sind (auch wenn Marketing-Abteilungen gerne anderes behaupten).

Entsorgung

Zertifikate sind nur so sicher wie die Verlässlichkeit der Validierung des Antragstellers – aber die ist dem Zertifikat selbst nicht anzusehen. Öffentliche Trustcenter bieten ihren Kunden meist verschiedene Methoden zur „Domain Validation" an, also zum Nachweis des Besitzes einer Domäne. Einige dieser Methoden sind nur eingeschränkt verlässlich und werden heute kaum noch verwendet.

Deswegen hat das CA/Browser-Forum beschlossen, diese schrittweise abzuschaffen: 2024 traf es WHOIS, am 12.11.2025 folgten die DNS-PTR-Records und am 19.11.2025 kamen E-Mail, Fax und Telefon an die Reihe. Bei den beiden zuletzt genannten Methoden wurde den Trustcentern und ihren Kunden eine Übergangsfrist bis 2028 respektive 2027 eingeräumt.

Besser spät als nie: Die Entsorgung nicht mehr ausreichend sicherer Standards, Protokolle und Verfahren durch das CA/Browser-Forum ist ein wichtiger Beitrag zur IT-Sicherheit, an der sich auch andere Hersteller ein Beispiel nehmen sollten. Manchmal dürfte sie sogar noch ein wenig konsequenter erfolgen.

Löschfrist ist abzuwägen

Am 18.12.2025 hat der Bundesgerichtshof (BGH) klargestellt, dass bei der Bestimmung von Löschfristen für personenbezogene Daten immer eine konkrete Interessensabwägung erforderlich ist. Im Streitfall hatte die SCHUFA Daten des Klägers über ausgeglichene Forderungen teilweise länger als drei Jahre gespeichert – obwohl dafür in den von der Hessischen Beauftragten für den Datenschutz und die Informationsfreiheit genehmigten Verhaltensregeln für Wirtschaftsauskunfteien lediglich 18 Monate vorgesehen sind.

Der BGH entschied nun, dass die Löschfrist sich zwar an Richtlinien und Löschfristen von Einrichtungen anderer Art (z. B. Insolvenzbekanntmachungen) orientieren kann. Letztlich seien aber in einer „konkret vorzunehmenden Interessensabwägung" die Erforderlichkeit zu prüfen und die Besonderheiten des Einzelfalls zu berücksichtigen.

Kleinigkeiten zählen

Trend Micro beobachtet (wie andere EDR-Anbieter auch) täglich Angriffe auf IT-Systeme. 2024 fielen ihnen .LNK-Dateien (Windows-Explorer-Verknüpfungen) auf, die ab dem 261. Zeichen Befehle enthielten.

Diese bleiben verborgen, weil die Benutzerschnittstelle nur die ersten 260 Zeichen zeigt. Trend Micro meldete das am 20.09.2024 dem Microsoft Security Response Center. Dort hielt man das Problem für unbedeutend. Nachdem die Schwachstelle zunehmend in „staatlichen" Angriffen – etwa gegen europäische diplomatische Einrichtungen – verwendet wurde, hat Microsoft sich im November-Update 2025 stillschweigend darum gekümmert. Der Hinweis vom 01.11.2025 stuft den Fehler allerdings nicht als Sicherheitslücke ein.

Genau genommen schließt der Fix die Schwachstelle nicht, sondern erleichtert die Entdeckung ihrer Nutzung: Microsoft begrenzte nämlich nicht die Länge oder den Inhalt der Verknüpfung, sondern änderte die Anzeige – vermutlich aus Kompatibilitätsgründen. Doch braucht man wirklich mehr als 260 Zeichen in einer Verknüpfung? Sollte jemand dort Skripte verstecken dürfen?

Wer verhindern möchte, dass die eigene Software nach und nach löchrig wird wie Schweizer Käse, sollte auch kleine Sicherheitslücken schließen.

500 Seiten Binsenweisheit

Am 09.12.2025 hat das Bundesinnenministerium auf Antrag der Plattform fragdenstaat.de ein Rechtsgutachten der Universität zu Köln veröffentlicht. Darin kommen die Autoren zu dem – kaum überraschenden – Ergebnis, dass Section 702 des FISA, der CLOUD Act und weitere Gesetze es den US-Geheimdiensten erlauben, auf nahezu sämtliche Daten in der Cloud zuzugreifen, egal, wo die Server stehen, und fast egal, wer sie betreibt: Es kommt nicht darauf an, ob es sich um ein deutsches, ein europäisches oder ein amerikanisches Unternehmen handelt. Auch bedarf es keines richterlichen Beschlusses.

Diese Erkenntnis lässt sich auch einem von der DSK vor vier Jahren veröffentlichten Gutachten entnehmen (SSN 2/2022) – die Kosten für das neue Gutachten hätte das BMI sparen können.

Schutz vor (nach US-Recht legalen) Geheimdienstzugriffen bietet allein echte technische Souveränität. Helfen können zusätzliche technische Maßnahmen (wie Verschlüsselung) oder die Bevorzugung deutscher oder zumindest europäischer Plattformen.

Resiliente Kommunikation

Nach dem Brandanschlag auf eine Kabelbrücke über den Teltowkanal am 03.01.2026 waren rund 45.000 Haushalte und 2.200 Gewerbekunden im Berliner Südwesten tagelang ohne Strom. Stromnetz Berlin informierte auf einer Krisenseite über den Verlauf der Störung. Nur: Wie kommuniziert man, wenn mit dem Strom auch die Mobilfunknetze ausfallen?

Der Vorfall zeigt die Verwundbarkeit moderner Gesellschaften. Stromausfälle legen nicht nur Haushalte lahm, sondern auch Komponenten der Kommunikationsinfrastruktur: WhatsApp, Telefon, Internet – nichts funktioniert mehr.

Wer sich allein auf eine zentrale Kommunikationsinfrastruktur verlässt, ist im Krisenfall gegebenenfalls isoliert. Dabei gibt es Alternativen zum Mobilfunknetz wie den von der Bundesnetzagentur erlaubten LoRa-

Funkstandard. Zusammen mit einem dezentralen Mesh-Netzwerk wie Meshtastic kann darüber eine grundlegende Kommunikationsfähigkeit gewahrt werden – mit wenig technischem Know-How und zu geringen Kosten. Eine erste Basis an lokalen Netzen existiert bereits.

Krisenvorsorge meint nicht nur die Anlage von Wasservorräten und Notfallrationen. Sie bedeutet auch die Verfügbarkeit alternativer Kommunikationswege. Darum kümmern sollte man sich vor der Krise.

Secorvo News

Rechnen mit privaten Daten

Die statistische Auswertung großer Bestände sensibler personenbezogener Daten – von Gehältern bis Gesundheitsdaten – scheitert oft an Datenschutzvorbehalten. Mit Hilfe moderner kryptographischer Verfahren können solche Auswertungen vorgenommen werden, ohne dass dabei einzelne personenbezogene Datensätze offengelegt werden.

Die dahinterstehende Technik wird „sichere Mehrparteienberechnung“ (MPC) genannt. Sie ermöglicht es, mit sensiblen Daten zu „rechnen“, ohne dabei einzelne Datensätze zugänglich zu machen. Das Verfahren wird zunehmend in der Praxis eingesetzt, so zum Beispiel in einer Studie zur geschlechtsspezifischen Lohnlücke im Großraum Boston oder in einer Studie zum sicheren Rechnen auf klinischen Daten, die im vergangenen Jahr veröffentlicht wurden.

Dr. Alexander Koch (Secorvo) stellte am 02.12.2025 auf der 23. Konferenz Theory of Cryptography (TCC) in Aarhus ein Forschungsergebnis zur Weiterentwicklung von MPC vor: Um das Verfahren mit minimaler Kommunikation zwischen je zwei Parteien durchzuführen werden neuartige Zufallsgeneratoren eingesetzt, mit denen die Beteiligten ohne weitere Kommunikation korrelierte Zufallswerte erzeugen können – ein weiterer Beitrag zur Praxiseignung von MPC.

NIS-2-Schulungen am Kamin

§ 38 BSIG verpflichtet Geschäftsleitungen wichtiger Einrichtungen nicht nur, Risikomanagementmaßnahmen umzusetzen und zu überwachen, sondern auch, sich regelmäßig zu Kenntnissen und Fähigkeiten zur Erkennung und Bewertung von Risiken und Risikomanagementpraktiken der Informationssicherheit weiterzubilden.

Wir machen aus der Not eine Tugend: Auf unserem NIS-2-Kaminabend führen wir Sie konzentriert in diese Praktiken nach den Anforderungen des BSI ein – und bieten Ihnen zugleich ein C-Level-Forum für den Austausch mit anderen Verantwortlichen. Die nächsten Termine finden Sie auf unserer Webseite – wir informieren Sie auch gerne per E-Mail.

Seminare 2026

Auf unseren Seminaren vermitteln wir auch 2026 aktuelle Einblicke und bieten praxisorientierte Vertiefungen zu Themen der Informationssicherheit. Mit den Seminaren T.I.S.P., T.P.S.S.E. und Vorfallsexperte

bereiten wir Sie auf den Erwerb anerkannter berufsqualifizierender Zertifizierungen vor.

Im kommenden Jahr bieten wir neben dem „Klassiker“ zu Konzeption und Aufbau von Public-Key Infrastrukturen mit dem ISMS-Intensivseminar einen praxisorientierten und pragmatischen Einstieg in den Aufbau eines wirksamen Sicherheitsmanagements.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)
März 2026	
02.-06.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
05.03.	NIS-2-Kaminabend – Schulung nach BSIG (Secorvo, Karlsruhe)
09.-12.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-19.03.	secIT 2026 (Heise Medien, Hannover)
23.-24.03.	ISMS verstehen und planen (Secorvo, Karlsruhe)
23.-26.03.	RSA Conference 2026 (RSA Conference, San Francisco/US)
23.-27.03.	FSE 2026 (IACR, Singapur/ASE)
24.-27.03.	DFRWS EU 2026 (DFRWS, Linköping/SE)
April 2026	
14.-16.04.	Datenschutztage 2026 (WEKA-Akademie, Frankfurt)
14.-16.04.	PQCrypto 2026 (IACR, Saint-Malo/FR))

Impressum

Secorvo Security News – ISSN 1613-4311

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