DNIP-Briefing #87: Datenhunger und langer Atem

Die Redaktion · 1. September 2026

Foto von Ron Lach bei Pexels, PD-ähnlich

Die Redaktion präsentiert jeden Dienstag die Geschichten, die sie bewegt, aufgerüttelt oder zum Nachdenken angeregt hat. Heute u. a. mit Datenhunger, digitalen Abhängigkeiten und anonymen Chatgruppen.

Inhalte

Visa Waiver-Programm nur noch gegen Polizeidaten
Digitaltod per Unterschrift
Kommunikation nach Cyberangriff
Noch weniger Arbeitsplätze durch Rechenzentren
Und schliesslich:

Visa Waiver-Programm nur noch gegen Polizeidaten

Das Visa Waiver-Programm der USA erlaubt es Schweizerinnen und Schweizern (wie auch EU-BürgerInnen), für bis zu 90 Tagen Visa-frei in die USA einzureisen. Voraussetzung dazu ist primär ein biometrischer Pass (was einer der Gründe ist, wieso der Schweizer Pass seit einigen Jahren einen Chip enthält). Wie Adrienne Fichter schreibt, will die USA die Voraussetzungen für das Visa Waiver-Programm ab 2027 deutlich erhöhen: Neu wird der Zugriff auf die jeweiligen nationalen Polizeidatenbanken gefordert, um Einreisende detaillierter zu überprüfen. Ausgelöst werden können Abfragen von Seiten der USA schon bei vagen Verdachtsmomenten wie einer schlechten «Risikobewertung», angeblichen «kriminalpolizeilichen Erkenntnissen» oder unklaren Angaben bei der Einreise – auch Social-Media-Postings könnten künftig eine Rolle spielen. Basierend auf ersten Treffern soll dann auch der Zugriff auf weitere Daten (darunter Informationen zu Vorstrafen wie auch besonders schützenswerte Daten) möglich sein.

Eine datenschützerische Kontrolle fehlt dabei auf USA-Seite weitgehend. Zwar soll es auch dort Inspektionen oder Datenschutzbeauftragte geben, diese haben aber als Mitarbeitende der zu kontrollieren Behörde eine schwache Position. Wie Adrienne Fichter weiter schreibt, sind genau an solchen Konstruktionen frühere Datentransferabkommen zwischen der EU und der USA gescheitert.

Auch wenn die Verhandlungen über ein neues Visa Waiver-Programm primär zwischen den USA und der EU erfolgen: Auch die Schweiz wurde von den USA schon angefragt. Und da sie Teil des Schengen-Raums ist, wird ein koordiniertes Vorgehen zusammen mit der EU-Kommission und den Schengen-Mitgliedstaaten unerlässlich sein.

Digitaltod per Unterschrift

„Eine einzige Unterschrift von Trump und du bist weg vom Internet„. So titelte, frei übersetzt, *Il Fatto Quotidiano*. Es geht um den jüngsten Streich aus dem Weissen Haus, welches nichts unversucht lässt, Europa zu mehr digitaler Souveränität zu drängen.

Doch worum geht es? Ein kleines italienisches Kollektiv namens Autistici/Inventati hatte vor 25 Jahren begonnen, spendenfinanziert Onlinedienste für Nutzer anzubieten, welche sich gegen Faschismus, Rassismus, Sexismus etc. engagierten. 25 Jahre hatten sie eine Onlinepräsenz, blieben aber ausserhalb ihrer Kreise praktisch unbekannt. Ihr *Claim to Fame* begann vor wenigen Tagen mit einer Unterschrift des US-Präsidenten. Dieser setzte letzte Woche nicht nur seine „persönliche Obsession" einseitiger Umbenennung von Gewässern fort, er deklarierte Autistici/Inventati auch als ein terroristische Organisation.

Der Eintrag auf dieser Liste für „speziell ausgewiesene globale Terroristen" beruht nicht auf irgendwelchen terroristischen Aktivitäten der Gruppe, sondern rein darauf, dass das Kollektiv anonyme Mailkonten anbietet, welche auch von linksextremen Gruppierungen genutzt werden. Wer als US-Amerikaner trotzdem „Geschäfte" mit der sanktionierten Autistici/Inventati tätigt, riskiert bis zu 20 Jahr Gefängnis.

So wurde auch ihre Internet-Domain `autistici.org` gesperrt, die unter der US-kontrollierten .org-Domain läuft. Ebenfalls sei ihr Bankkonto in Gefahr, über das sich das Kollektiv – welches Kryptowährungen aus Prinzip ablehnt – mit Spenden finanziert.

So schreibt die New York Times, dass viele westliche Regierungen und Analysten vor der Gefahr von erstarkenden rechtsextremen, gewalttätigen Organisationen warnen würden, die Administration Trump aber vor allem linke Bewegungen ins Visier nähme und die Gefahren übertrieben darstellen würde.

Verschiedene Zeitungen berichten darüber, dass diese „Terrorismus"-Sanktionen der US-Regierung vor allem den Chilling Effect auf freie Meinungsäusserung haben soll, insbesondere auf Trump-kritische Äusserungen.

Dies reiht sich ein in die US-Sanktionen gegen andere Organisationen in Europa wie den Internationalen Strafgerichtshof (ICC), wo zusätzlich zu den bestehenden Sanktionen vom vergangenen Jahr diesen Monat zusätzliche Sanktionen verhängt wurden oder die Sanktionen gegen HateAid. Und gut möglich, dass die nächsten Sanktionen Domains und Bankkonten grösserer Organisationen treffen werden, die sich für sichere oder verschlüsselte Kommunikation einsetzen. Wie beispielsweise Proton.

> Mehr zu digitaler Souveränität bei Internet-Domains folgt in den nächsten Tagen bei DNIP; bereits früher haben wir über verschiedene Aspekte von digitaler Souveränität geschrieben: Eine Studie über die Sichtweise von KMU, Microsofts Versuch, die Bemühungen zu zersplittern, das Gaia-X-Projekt für europäische digitale Souveränität, die Schwierigkeit von Statistiken dazu, der Lock-In-Effect von Clouds, Handelskammer und Zolldeal als Druckmittel sowie dass Souveränität Selbstbewusstsein bedingt.

Kommunikation nach Cyberangriff

Bei einem „modernen" Cyberangriff wird meist ein volles Programm gefahren: Systeme lahmlegen, Daten kopieren, Daten beim Opfer löschen/verschlüsseln, Opfer erpressen und/oder Daten verkaufen. Alles häufig unter dem Sammelbegriff „Ransomware".

Cyberangriffe können jedem passieren. Deshalb ist es wichtig, zu wissen, was mit den Daten passiert. Im Interview mit dem deutschen Chaos Computer Club (CCC) wird das am aktuellen Fall Berlin erläutert. Vieles davon trifft aber auch auf Schweizer Unternehmen und Behörden zu, die einem Cyberangriff zum Opfer fallen.

Wenn man merkt, dass man gehackt wurde, ist meist die Hölle los. Damit man einen kühlen Kopf behält, hat das Bundesamt für Cybersicherheit (BACS) Informationen für einen Cybervorfall gebündelt. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zusammen mit weiteren Experten ein Handbuch „In Krisen schnell reagieren" (PDF) erstellt. Der Fokus des Krisenhandbuchs liegt zwar auf deutschen Gemeinden, vieles davon lässt sich aber auf die Schweiz im Allgemeinen und auch auf die Privatwirtschaft übertragen. Zusätzlich zu den vom BACS behandelten Punkten finden sich auch Ablaufskizzen und Prozessdiagramme für Angriffserkennung und Reaktion sowie hilfreiche Checklisten, um den Überblick auch in dieser schwierigen Situation zu behalten. Am allerbesten reagiert man allerdings, wenn man einen Cybervorfall im Vorfeld schon einmal in der Theorie oder als Rollenspiel durchexerziert hat.

Die Kommunikation ist dabei das A und O, sowohl nach innen wie nach aussen. Sowohl das BACS wie auch das BSI haben dazu Tipps, die auf einheitlicher, ehrlicher, regelmässiger und verständlicher Kommunikation basieren, die auch die Sorgen der Kundinnen oder Bürger ernst nehmen.

Noch besser ist es aber, wenn man gar nicht von Angriffen von Cyberkriminellen betroffen ist. Dazu kann man (als Organisation) selbst beitragen, indem man:

- die IT-Infrastruktur aktuell hält (Sicherheitsupdates regelmässig einspielen, möglichst wenig bzw. einfache Software einsetzen, Software von vertrauenswürdigen Herstellern nutzen, die moderne Softwareentwicklungsprozesse nutzen und auch regelmässig externe Sicherheitsexperten auf ihre Software schauen lassen),
- die verschiedenen Systeme möglichst gut voneinander trennt,
- die Zugangsdaten schützt (möglichst eng gefasste Berechtigungen, gute Passwörter und MFA, keine Weitergabe an Dritte) und
- unabhängige Backups anlegt (Nutzer und Systeme, welche die Originaldaten bearbeiten oder löschen können, dürfen keine Backups löschen können, damit Ransomwaregangs zumindest hier keine Chance haben).

Einen Kürzestüberblick über die Massnahmen und ihren Zweck gab es auch hier und einen längeren hier.

Noch weniger Arbeitsplätze durch Rechenzentren

Die Ansiedlung von Rechenzentren in einer Gemeinde wird häufig mit Arbeitsplätzen, Steuereinnahmen und Standortattraktivität begründet (und deshalb z. T. die Ansiedlung auch direkt oder indirekt finanziell gefördert). Doch die Erwartungen an Stellen oder Steuereinnahmen werden oft nicht erfüllt und generell ist die Anzahl neu geschaffener Stellen meist klein. Doch bald könnte die Anzahl Stellen noch weiter schrumpfen: Meta (der Mutterkonzern von Facebook, Instagram und WhatsApp) will nämlich zukünftig seine KI-Rechenzentren von KI-Robotern warten lassen.

> Mehr zu Rechenzentren bei DNIP: Neben der grossen Reportage zum digitalen Fussabdruck inklusive Innovation, Kühlung und Wasserverbrauch haben wir auch schon zur Zunahme und Wasserverbrauch in der Schweiz, Wassermangel, bald RZ-Kollisionen im Weltraum?, im Wasser und im Weltraum, exponentielles Wachstum, Intransparenz.

Und schliesslich:

- Seit 2019(!) kämpft die Digitale Gesellschaft um Transparenz bei der Kabelaufklärung, Transparenz, welche wichtig ist um allenfalls Löschbegehren stellen zu können oder zu erkennen, inwieweit der NBD das Gesetz (welches „eigentlich“ nur Auslandsüberwachung zulässt) übertritt. Dieser Kampf mündete im Juli 2026 in der klaren Erkenntnis, dass der NDB (bzw. dessen mit dem Abhören beauftragter Dienst CEA) sowohl die Digitale Gesellschaft wie auch deren Geschäftsführer überwachte. Die Irrungen und Wirrungen bis es soweit war, und wie es jetzt weitergeht, kann man bei der Digitalen Gesellschaft nachlesen.
- Eine IMEI ist eine weltweit eindeutige Identifikationsnummer von Mobiltelefonen. Man kann diese zwar nicht nutzen, um einem anderen Mobiltelefon anzurufen, aber als Identifikationsmerkmal eignet sie sich hervorragend. Es liegt daher nahe, dass sie nicht mit anderen geteilt werden sollte. Wie Recherchen des Bayrischen Rundfunks jetzt gezeigt haben, wurde die IMEI unter gewissen Umständen jedoch beim Verbindungsaufbau sehr wohl an die Gegenseite übermittelt. Und auch wenn die telefonierende Benutzerin davon nichts merkt: Mit geeigneten technischen Mitteln kann man diese Information sehr wohl abfangen und zum Beispiel zum Anreichern von Persönlichkeitsprofilen oder zur Überwachung nutzen. Gefordert sind nun die Mobiltelefonanbieter und die Telecom-Unternehmen, welche sicherstellen müssen, dass IMEI und ähnliche Informationen konsequent ausgefiltert werden.
- Wie SRF berichtet, wurden in mehreren Mehrfamilienhäusern in Winterthur und Zürich Zettel mit einem QR-Code in die Briefkästen gesteckt. Es ist ein Aufruf dazu, einer Whatsapp-Gruppe für die Nachbarschaft beizutreten. Die Gruppe soll dem Austausch unter Nachbarinnen und Nachbarn dienen: für Anlässe, gegenseitige Hilfe und anderes. Klingt nach einer sympathischen Idee, aber leider sind die Hintergründe und Urheber dieser Chats völlig unbekannt. Kurz gesagt sollte man die Finger von Chatgruppen lassen, deren Urheber man nicht kennt, vor allem wenn sie unter dem Deckmantel der Nachbarschaftshilfe dazu verleiten können, zu viel preiszugeben („ich bin nächste Woche in den Ferien, wer kann meine Blumen giessen“).

dnip.ch mit Deiner Spende unterstützen

Wir wollen, dass unsere Inhalte frei verfügbar sind, weil wir es wichtig finden, dass möglichst viele Menschen in unserem Land die politischen Dimensionen der Digitalisierung erkennen und verstehen können.

Damit das möglich ist, sind wir auf deine Unterstützung angewiesen. Jeder Beitrag und sei er noch so klein, hilft uns, unsere Aufgabe wahrzunehmen.

CHF 5
CHF 10
CHF 20
CHF 25
CHF 50
CHF 75
CHF 100
CHF 150
CHF 200
CHF 250
CHF 500
CHF 1'000
Anderer

SPENDEN »

3 Kommentare

Theo Schmidt sagt:

1. September 2026 um 08:45 Uhr

.org Domains waren schon vor Trump ein Risiko. Ihpva.org war die Domain für die Website eines international ausgerichteten US-Vereins, der dann in einen Weltverband umgewandelt wurde, der den Namen erbte, mit dem ursprünglichen US-Verein als einer der Verbandsmitglieder. Dieser nannte sich um zu Hpva.org. Wegen Differenzen wollte der US-Klub nach einem Jahr oder so seinen alten Namen zurück, gegen die Stimmen der anderen amerikanischen, europäischen und pazifischen Mitgliedern. Es gelang ihm die ICANN zu überzeugen, welche die US-Position übernahm.

Antworten

↪

Marcel Waldvogel sagt:

1. September 2026 um 16:58 Uhr

Ist das `.org`-spezifisch? Die UDRP (Domain-Streitbeilegungsverfahren) gilt für dutzende Domains, inklusive `.org` oder auch `.ch` und andere europäische ccTLDs.

PS: Weisst du, ob es irgendwo eine Liste von Domain-Disputen gibt, pendenten und abgeschlossenen?

Antworten

Theo Schmidt sagt:

4. September 2026 um 08:35 Uhr

Du hast recht, .org ist nicht spezifisch. Ich hätte obigen Kommentar nicht schreiben sollen und finde nicht einmal heraus, ob man mit einer .ch Domain unabhängiger von ICANN und den USA wäre. Eine Liste finde ich auch nicht.

Antworten

Schreibe einen Kommentar

Deine E-Mail-Adresse wird nicht veröffentlicht. Erforderliche Felder sind mit * markiert

Kommentar *

Name *

E-Mail-Adresse *

Website

☐ Name, E-Mail-Adresse und Website in diesem Browser für meinen nächsten Kommentar speichern.

☐ Ja, ich möchte die neuen Blogbeiträge via E-Mail abonnieren. Ich kann mich jederzeit wieder aus der Liste austragen.

KOMMENTAR ABSCHICKEN

‹ Vogt am Freitag: Scheinriese
Vogt am Freitag: Werbeunterbrech… ›

Weitere Beiträge

Vogt am Freitag: Vollkostenrechnung

Reto Vogt · 30. Oktober 2026

127 Millionen Franken wird ein IT-Projekt der Migrationsbehörden teurer als geplant. Kolumnist Reto Vogt sagt: Das ist kein Einzelfall. Und

Weiterlesen »

DNIP-Briefing #95: Mit Sicherheit für die Katz?

Die Redaktion · 27. Oktober 2026

Die Redaktion präsentiert jeden Dienstag die Geschichten, die sie bewegt, aufgerüttelt oder zum Nachdenken angeregt hat. Heute mit allem ausser

Weiterlesen »

Newsletter abonnieren

… und auf dem neusten Stand bleiben

E-Mail

SENDEN

Wenn nicht anders gekennzeichnet, stehen alle durch Mitglieder der dnip-Redaktion erstellten Inhalte dieser Website unter der Lizenz Creative Commons Namensnennung 4.0 International (CC BY 4.0).