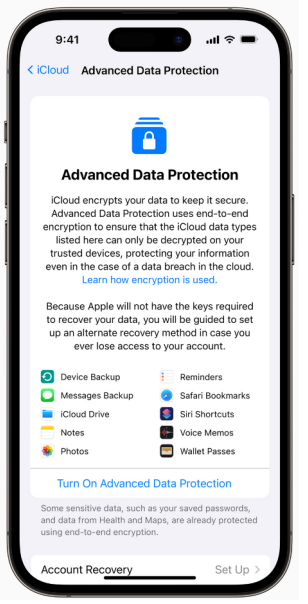
12 Monate Digitalchaos

Die grössten Cyberangriffe, Datenlecks und Lektionen

20. Februar 2026 | Roman Stocker | Winterkongress der Digitalen Gesellschaft


Digitalchaos
Cyberangriffe
Phishing
Social Engineering
Malware
Schwachstellen
Sicherheitslücken
Menschliche Fehler
Faulheit
Auswirkungen
Identitätsdiebstahl
Erpressung
Vertrauensverlust
Kontrollverlust
Datenlecks
Persönliche Informationen
Passwörter
Kreditkarten-daten
Lektionen
Datensparsamkeit
Sicherheit erhöhen
Kognitive Belastung reduzieren

Apple iCloud

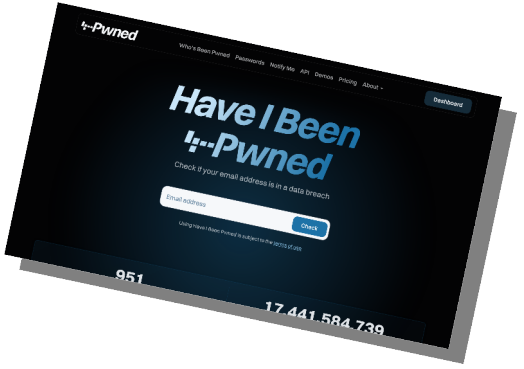


- Advanced Data Protection (ADP)
  - Ende-zu-Ende-Verschlüsselung
- UK - Investigatory Powers Act aus 2016
- Geheimbefehl verlangt Zugriff auf Ende-zu-Ende-Verschlüsselung weltweiter Benutzer:innen
- Apple weigert sich und deaktiviert ADP für Grossbritannien
- Offenlegung dieser Regierungsforderung ist eine Straftat

Feb | Mär | Apr | Mai | Jun | Jul | Aug | Sept | Okt | Nov | Dez | Jan | Feb

Have I Been Pwned

- Datenleck-Prüfdienst von Sicherheitsexperte Troy Hunt
- Phishing Angriff auf seine Mailchimp Mailingliste
- 16'627 E-Mail Adressen, IP-Adressen und geografische Orte der Mailingliste betroffen
- Trotz sofortiger Reaktion bereits zu spät
- Angriff geschah vollautomatisch



Feb | Mär | Apr | Mai | Jun | Jul | Aug | Sept | Okt | Nov | Dez | Jan | Feb

Mixpanel

- Analysefirma digitaler Daten
- Phishing Angriff

Mixpanel - Pornhub

- 94 GB Daten
- 200 Mio Datensätze von Premiumnutzer:innen
  - Such-, Wiedergabe- und Downloadverläufe
  - Details zu angesehenen Videos wie Wiedergabezeitpunkt, URL, Name und Schlüsselwörter
  - E-Mail Adressen und Standortdaten

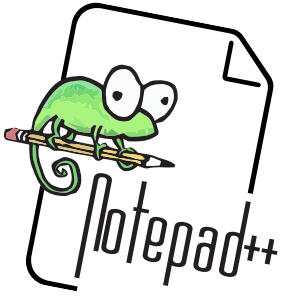
Mixpanel - OpenAI

- Analysedaten einer Entwicklerschnittstelle
  - Name, E-Mail Adresse, grobe Standortdaten, Informationen über Betriebssystem und Webbrowser, sowie mit dem API Konto verknüpfte Organisations- oder Benutzer:innen-IDs

Meta WhatsApp

- Forscher:innen fanden gesamtes Mitglieder:innenverzeichnis ungeschützt vor
- 3,5 Mia. Konten: Profilfotos, Statusfeld, öffentliche Schlüssel, Anzahl registrierter Geräte
  - 2,3 Mio. China, 60 Mio. Iran, 1,6 Mio. Myanmar und 5 Nordkorea
- Geringes Interesse von Meta
- Schwachstelle Stand 1 Jahr offen

Notepad++

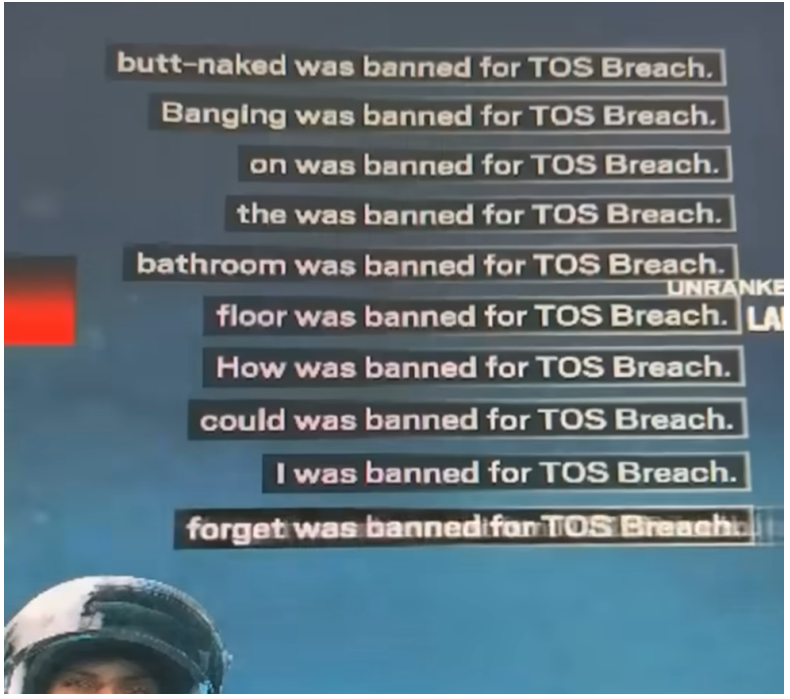


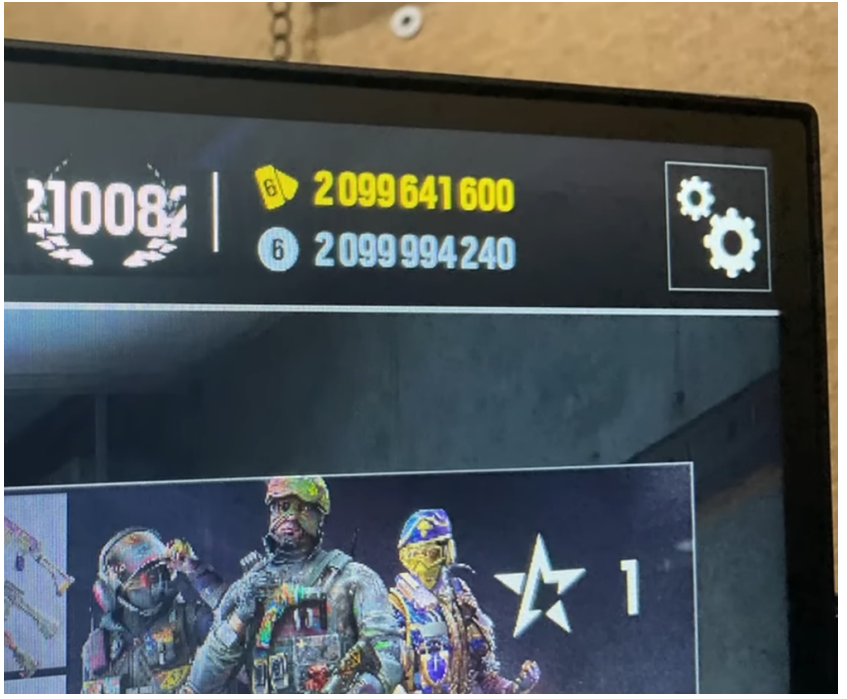
- Sicherheitslücke im integrierten Updater
- Ermöglichte Installation von Malware
- Kompromittierung der Infrastruktur
- Möglicherweise staatlicher Akteure aus China

MongoDB

- Beliebte Datenbank Software
- Schwerwiegende Sicherheitslücke names Mongobleed
- Zugriff ohne Berechtigungsnachweis auf Arbeitsspeicherbereiche des Datenbankservers
- Proof of Concept in der Weihnachtszeit veröffentlicht

MongoDB - Rainbow Six Siege





Feb | Mär | Apr | Mai | Jun | Jul | Aug | Sept | Okt | Nov | Dez | Jan | Feb

Radio Energy

- Hackerangriff auf Datenbank
- Personendaten von 85'000 Ticketgewinner:innen von «Energy Stars Night» und «Energy Air» der letzten beiden Jahren
- E-Mail Adressen, Telefonnummern, Namen und/oder Geburtsdaten
- Meldung an EDÖB

Microsoft Bitlocker

- Festplattenverschlüsselung
- Schlüssel dazu wird automatisch im Online-Account gespeichert
- Schlüssel kann manuell aus dem Online-Account entfernt werden
- Microsoft hat Zugriff darauf
- Schlüssel wurde das erste Mal an FBI übergeben

Discord

- Chat und Videokonferenz Software, beliebt bei Gamer:innen
- Ab März Altersprüfung per Ausweis oder Einschätzung über Gesichtserkennung
- Ansonsten Ausschluss von altersbegrenzten Server und Kanälen, sensible Inhalte werden gefiltert
- Angriff auf Drittanbieter: 70'000 **Lichtbildausweisbilder**, IP-Adressen, Nachrichten an Support, letzten 4 Ziffern verknüpfter Kreditkarten wurden abgegriffen

… mehr ...

- 6 Mio. Kund:innendatensätze von Oracle gestohlen. Sammelklage gegen Oracle in Amerika
- Angriff auf Daten und Konten mehrerer Pensionskassen in Australien. Geldanlagen scheinen weg zu sein.
- 37 GB Kund:innendaten und Quellcode von Europcar gestohlen
- Proton findet persönliche Daten von 44 schweizer und 54 deutschen Politiker:innen im Darknet. CH: 78 Passwörter und DE: 153 von 220 Passwörter im Klartext
- Daten von Kund:innen vor Mietwagenfirma Hertz gestohlen
- Microsoft sperrt sicherheitshalber Zugänge, weil sie fälschlicherweise Anmeldedaten geloggt haben

… noch mehr ...

- Südkoreanischer Mobilfunkprovider ersetzt nach Cyberangriff sämtliche Sim-Karten um Sim-Swapping vorzubeugen
- Beim Medienkonzern Pearson wurden Terabyte an Daten erbeutet
- Bei VW waren verschiedene Informationen zu Fahrzeugen und Personen frei über eine Entwicklerschnittstelle aufrufbar
- Von der Versandapotheke Volksversand wurden Kund:innendaten gestohlen
- Bei Adidas wurden über einen Drittanbieter Kund:innendaten gestohlen
- Bei zwei unabhängigen Cyberangriffen wurde Coca Cola unter anderem mit gestohlenen Daten erspresst

… einiges mehr ...

- Beim Rüstungskonzern Rheinmetall wurden vertrauliche Daten gestohlen und Beispieldaten veröffentlicht
- Gesundheitsstiftung Radix wurde gehackt und erpresst. Anschliessend wurden 1,3 TB Daten veröffentlicht
- 500'000 Rechnungen und Ausweise von Gäst:innen der Hotelkette Numa waren einsehbar
- Miserable Reaktion des Sexspielzeugherstellers Lovense nachdem ein Forscher mehrere gravierende Sicherheitslücken feststellt
- 3,5 TB Daten wurden nach Angriff auf IT-Grosshändler Ingram Micro veröffentlicht
- Daten aller Pi-hole-Spender:innen waren durch einen Fehler im Wordpress Plugin GiveWP öffentlich einsehbar

… mehr? ...

- Pro-ukrainische Angreifer bescherten russischer Aeroflot Flugzeugausfälle und veröffentlichen Daten
- Sensible Daten von Swiss Pilot:innen waren öffentlich zugänglich
- 850'000 Kund:innendaten von Telekommunikationsanbieter Orange gestohlen
- Anmeldeinformationen von Streamingplattform Plex gestohlen
- Millionen an Daten von Gäst:innen waren in Hotelsoftware Sihot einsehbar
- Salesforce wurde mit 1 Mia. Datensätzen von Kund:innen aus 39 Unternehmen von Hackergruppe erpresst

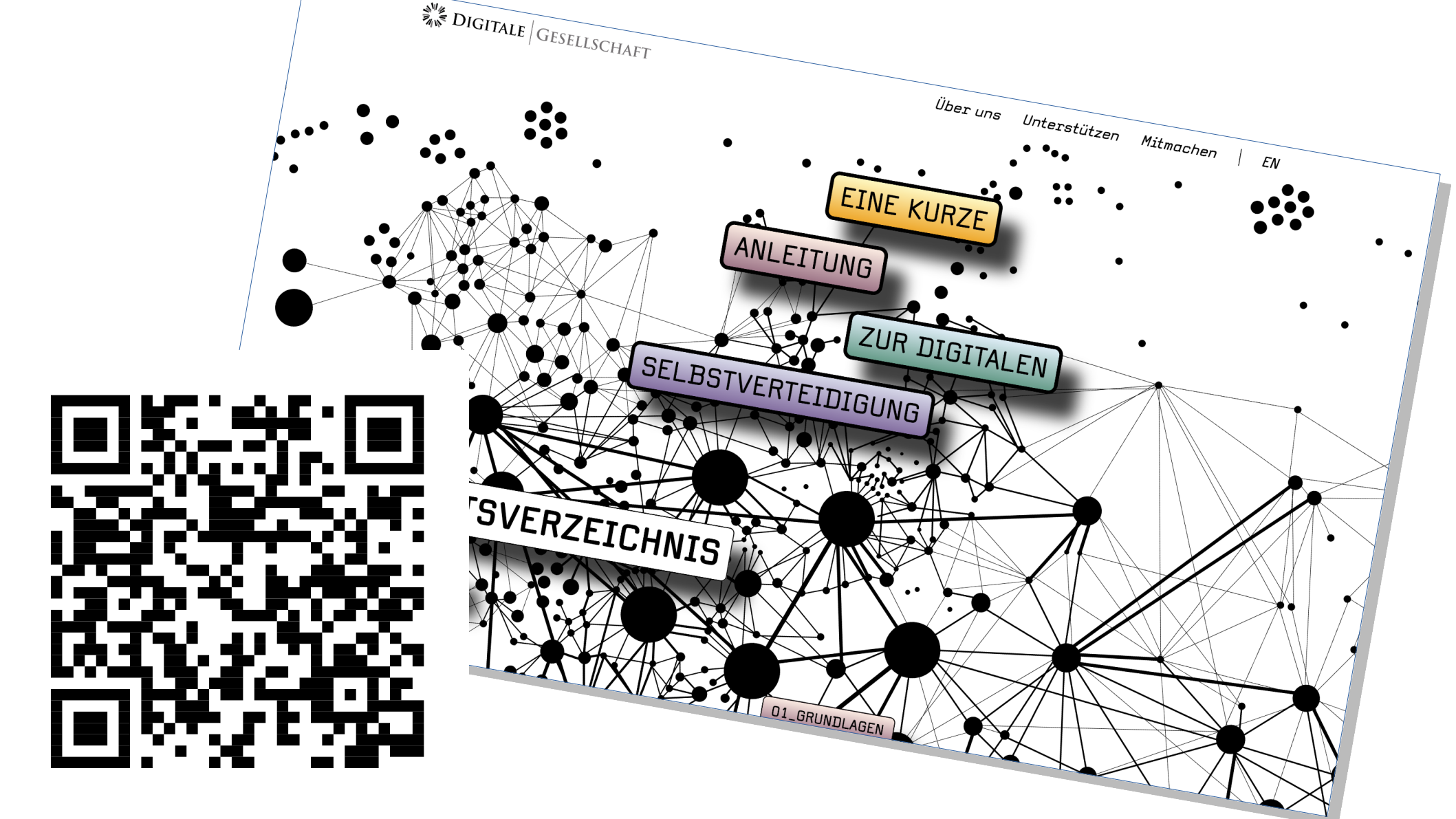
… genug? ...

- 2 KI Chat-Apps speicherten intime Unterhaltungen und 600'000 Bilder von 400'000 Kund:innen ungeschützt
- Von Modekonzern Mango wurden Daten von Kund:innen gestohlen
- Vollständige Kreditkartendaten vom Miniaturwunderland Hamburg gestohlen
- Von Logitech wurden Informationen über Mitarbeiter:innen, Verbraucher:innen sowie Daten zu Kund:innen und Lieferant:innen gestohlen
- Daten von Kund:innen der spanischen Airline Iberia wurden gestohlen
- Bei Soundcloud wurden von 20% (28 Mio.) der Nutzerschaft Daten gestohlen

… noch viel mehr ...

- Beim Magazin Wired wurden Informationen zu 2,3 Millionen Abonnent:innen gestohlen und stehen zum Verkauf
- Telemedizinanbieter Dr. Ansay hatte zum wiederholten Male eine Datenpanne. 1,7 Mio. Rezepte von Hundertausenden Kund:innen waren abrufbar
- Bei Eurail und Interrail wurden Daten von Kund:innen gestohlen und kursieren im Darknet
- Bei der Bekleidungsmarke Under Armour wurden 72,7 Mio. Datensätze von Kund:innen gestohlen
- Trisa wird mit Daten von Kund:innen und Mitarbeiter:innen erpresst

Lektionen


DIGITALE | GESELLSCHAFT
Über uns
Unterstützen
Mitmachen
EN
EINE KURZE
ANLEITUNG
ZUR DIGITALEN
SELBSTVERTEIDIGUNG
TSVERZEICHNIS
01_GRUNDLAGEN

Datensparsamkeit

- Notwendigkeit eines Accounts überdenken
- Wegwerf E-Mail Adressen verwenden
- Falsche Identitäten und Angaben verwenden
- Handynummer möglichst sparsam verwenden
- Keine Kreditkarteninformationen speichern

→ Auch ohne Account entstehen Spuren!

Accountsicherheit erhöhen

- Verwendet Passkeys wo möglich
  - Resistent gegenüber Phishing-Angriffen
  - Resistent gegenüber Datenlecks
  - Je nachdem Hardwaregebunden
- Verwendet 2FA/MFA wo möglich
- Passwörter mindestens 12 Zeichen bei voller Komplexität
- Passwörter niemals mehrfach verwenden

Kognitive Belastung reduzieren

- E-Mail Aliasse verwendet
- Dedizierte E-Mail Adressen verwenden
  - bankname.xy12@domain.ch

Entrümpeln

- E-Mail Adresse(n) auf HaveIBeenPwned prüfen
- Passwortmanager (lokal) verwenden
- Schwache Passwörter erneuern
- Alte Accounts löschen
- Daten aus der Cloud entfernen
- OpenSource Software unterstützen
- Software regelmässig aktualisieren

→ Cloud alleine ist kein Backup

Sicherheit <> **Einfachheit**

Datenschutz <> **Kosten**

Präsentation

Quellen