Die Big Brother Awards sind die «Oscars für Datenkraken» und prämieren Datensünder in Wirtschaft und Politik. Es gibt sie seit 1998 in bisher 19 Ländern. In der Schweiz lancieren wir nach 10 Jahren Pause die Verleihung der Preise neu. Unten finden Sie die Begründung für die Preisvergabe. Der Big Brother Award ist als ein Angebot zum Gespräch zu verstehen.

Jury der Big Brother Awards Schweiz

https://bigbrotherawards.ch

Big Brother Award in der Kategorie Private-Public-Partnership: Elektronisches Patientendossier (Bundesamt für Gesundheit)

Hintergrund

- Beim Elektronischen Patientendossier (EPD) handelt es sich um ein Thema, das Medien und Bevölkerung umtreibt (Beispiele: Tages-Anzeiger mit fragwürdiger Sitzung vom Bundesrat mit Konzernen zum Thema, anderer Tages-Anzeiger-Artikel zur Komplexität des Projekts und Artikel saldo (Paywall).
- Der CCC-CH warnt seit vielen Jahren vor dem Elektronischen Patientendossier – die zentralisierte Architektur ohne Ende-zu-Ende-Verschlüsselung droht eine grössere Datenschutzkatastrophe herbeizuführen; vgl. z. B. Video (2014) mit Volker Birk.

Fakten und Gründe zum Negativpreis

- Bei Gesundheitsdaten handelt es sich gem. Art. 3 Bst. c Zif. 2 DSG um besonders schützenswerte Personendaten.
- Gesundheitsdaten sind potenziell hochdiskrimierend – sie sind zudem kaum oder nicht veränderlich und haften einer Person lange oder lebenslänglich an.
- Patient*innendaten werden aktuell sehr dezentral in den Systemen der Ärzt*innen und Spitäler gehalten, allerdings im Einzelfall unter z.T. katastrophalen Sicherheitsstandards.

Allerdings sind die Systeme jeweils unterschiedlich gestrickt und angebunden, so dass ein/e Angreifer*in unterschiedliche Angriffe ausführen muss, um viele Patient*innendaten einzusammeln.

- Mit einem dezentralisierten und sicher geführten EPD könnte dieser Missstand behoben werden. Stattdessen wird praktisch an einem EPD gearbeitet, das technisch zentralistisch und von nur zwei Systemanbieterinnen - Swisscom und Post - betrieben wird; damit entstehen zentralisierte Angriffspunkte. Mangels Ende-zu-Ende-Verschlüsselung können massenweise Datenabflüsse nicht wirksam bekämpft werden.
- Das Gesetz gebietet, dass man den Datenschutz und die Datensicherheit zwar einhalten muss, fordert allerdings weder dezentrale Systeme zur Datenhaltung noch Ende-zu-Ende-Verschlüsselung.
- Durch die Systemarchitektur entstehen im Wesentlichen zwei zentrale Angriffspunkte, so dass es professionell agierenden oder staatlichen Angreifer*innen möglich wird, auf einheitliche Weise an sehr viele - wenn nicht alle - Patient*innendaten heranzukommen. Die ähnliche Systemarchitektur und die vereinheitlichten Systemschnittstellen, die Swisscom und Post anbieten, verringern für potente Angreifer*innen den Aufwand.
- Ursprünglich sollten 20-40 Stammgemeinschaften existieren; tatsächlich ist diese Zahl schon jetzt auf unter 10 gefallen, vgl. Botschaft https://www.admin.ch/opc/de/federal-gazette/2013/5321.pdf (PDF) und E-Health-Webseite https://www.e-health-suisse.ch/gemeinschaften-umsetzung/epd-gemeinschaften/gemeinschaften-im-aufbau.html.
- Als Beispiel sei die XAD-/Axsana-Stammgemeinschaft betrachtet, welche 13 (!) Kantone der Deutschschweiz umfasst: technisch wird das EPD von der Swisscom („Swisscom Health“) umgesetzt und betrieben.
- In Norwegen kam es 2018 bereits zu einer grösseren Datenschutzkatastrophe im Zusammenhang mit E-Patient*innendossiers – ein staatlicher Angreifer soll am Werk gewesen sein; vgl. https://www.medinside.ch/de/post/norwegen-melden-schweren-angriff-auf-gesundheitsdaten
- Das Bundesamt für Gesundheit gibt sogar selbst „Restrisiken“ zu, die für Gesundheitsdaten untragbar sind (als Single-Point-of-Failures): https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-

ehealth/anhoerung-ausfuehrungsrecht/hintergrundinformationen/risiko.pdf.download.pdf/bag_risikoanalyse_epd_v1_0.pdf (PDF): „Systemadministratoren oder unberechtigte Dritte, die sich Systemadministrationsrechte verschaffen, können deshalb unter Umgehung der applikatorischen Rechteverwaltung auf Daten in potentiell grosser Menge zugreifen und diese an interessierte Dritte weitergeben." (S.45)

Forderungen

- Gesetz und Verordnungen sind so anzupassen, dass Dezentralisierung und Ende-zu-Ende-Verschlüsselung Pflicht sind.
- Da es sich beim Elektronischen Patientendossier um sehr kritische Infrastruktur handelt, ist eine Forderung nach öffentlicher Finanzierung als Open-Source-Software diskutabel (um den Einbau von Hintertüren, wo Daten abfliessen, zu erschweren).
- Das Datenschutzgesetz (DSG) muss so angepasst werden, dass hohe Bussen anfallen, für den Fall, dass Daten abhanden kommen (zum Vergleich: mit der DSGVO können Bussen bis zu EUR 20 Millionen oder 4% des weltweiten Jahresumsatzes auferlegt werden). Ein solches „Damoklesschwert" schafft Anreize, in Dezentralisierung und IT-Sicherheit zu investieren um Datenschutz technisch zu gewährleisten.
- Ein Patientendossier muss freiwillig bleiben (Beibehaltung des gesetzlichen Opt-In-Ansatzes) – das ist gefährdet (vgl. Tages-Anzeiger).
- Mit sogenannt „anonymisierten" Big-Data-Übungen muss aufgepasst werden: je nach Krankheitsmerkmalen bzw. -verlaufen ist eine Deanonymisierung (ein Schliessen auf konkrete Personen) einfach möglich, z.B. bei seltenen Krankheiten oder Krankheitskombinationen.