secorvo
security consulting

Secorvo Security News

Mai 2020

Unterirdisch

Die Londoner „Tube“, benannt nach den Röhren, durch die die Untergrundbahnen fahren, ist die älteste U-Bahn und mit mehr als 270 Stationen an über 400 km Schienenstrecke noch heute das drittgrößte U-Bahn-Netz der Welt.

Der Eröffnung am 09.01.1863 ging jedoch ein erbittertes Ringen voraus. 17 Jahre hatte der Jurist *Charles Pearson* für den Bau gekämpft. Zwar erstickte London damals im Pferdedroschkenverkehr, aber Eisenbahnen waren noch eine junge Technik – erst 1838 hatte *Isambard Kingdom Brunel* die erste Eisenbahnstrecke erbaut. Doch der nur 6,5 km lange erste U-Bahn-Abschnitt wurde allen Widrigkeiten zum Trotz ein riesiger Erfolg: Im ersten Betriebsjahr beförderte die Tube bereits 9,5 Mio. Fahrgäste. Daher folgten bald weitere Linien; heute nutzen über 3 Mio. Menschen die Tube am Tag – fast 1,2 Milliarden im Jahr.

Drei Jahre Bauzeit und 1,3 Mio. Pfund kostete der Bau; für die damalige Zeit ein gigantisches Projekt. Aber es wurde rechtzeitig begonnen, bevor Bebauungsdichte und Kanalisation ein solches Querschnittsprojekt unmöglich gemacht hätten. Der erste Abschnitt konnte fast komplett in offener Bauweise errichtet werden. Wer heute eine U-Bahn plant, muss trotz aller technischen Errungenschaften wie Tunnelbohrmaschinen mit ganz anderen Hindernissen und Kosten kalkulieren. 320 Mio. Euro kostete das nach 14 Jahren Bauzeit am 08.08.2009 eröffnete, 1,8 km lange U-Bahn-Sackgässchen (U55) ins Berliner Regierungsviertel (177 Mio. €/km), und mehr als eine Milliarde Euro wird der knapp 3,4 km lange Stadtbahn-Tunnel in Karlsruhe bei der Fertigstellung 2021 nach 11jähriger Bauzeit voraussichtlich verschlungen haben (294 Mio. €/km).

Mit U-Bahnen verhält es sich offenbar wie mit dem Datenschutz: Auch der benötigt engagierte, idealistische Vorkämpfer, die nicht so leicht aufgeben – und je später man mit der Umsetzung beginnt, desto aufwändiger und teurer wird es am Ende.

Inhalt

secorvo
security consulting

Security News

Präventive Kontaktdaten

Seit dem 04.05.2020 atmet die Republik auf: Viele Dienstleistungen wie Friseur- oder Restaurantbesuche, die wochenlang verboten waren, sind zumindest eingeschränkt wieder zugelassen. Diese Einschränkungen haben es allerdings aus datenschutzrechtlicher Sicht in sich: Je nach Bundesland muss man nun seine Kontaktdaten (Name, Anschrift und Telefonnummer) hinterlassen bzw. werden diese von den Anbietern erfasst. Es sei denn, man wechselt in das „richtige" Bundesland: Nicht überall ist die Kontaktdatendokumentation vorgeschrieben, da es keine bundeseinheitliche Regelung gibt. Auch die Vorgaben zur Art und Weise der Erfassung und Verarbeitung, der Dauer der Aufbewahrung (vier bis sechs Wochen) und der Löschung der Daten sind uneinheitlich. In einem Bundesland muss der Besucher sogar (zwingend) sein Einverständnis zur Erhebung der Kontaktdaten erteilen – hier hat der Verordnungsgeber offenbar das Prinzip der datenschutzrechtlichen Einwilligung nicht verstanden. Einig ist man sich immerhin darin, dass das Aushängen oder Auslegen von Listen keine probate Form der Datenerfassung ist.

In manchen Bundesländern sind die Regelungen zur Kontaktnachverfolgung in einer einheitlichen Corona-Verordnung niedergelegt, in anderen gibt es für jedes Gewerbe getrennte Verordnungen. So wird beispielsweise in der ab dem 02.06.2020 gültigen Fassung der Verordnung des Baden-Württembergischen Kultus- und des Sozialministeriums über Sportstätten der nun wieder zulässige Betrieb von Schwimm- und Hallenbädern sowie Thermal- und Spaßbädern geregelt. Neben der Bereitstellung einer Aufsichtskraft für das Einhalten der Grundsätze des Infektionsschutzes muss der Betreiber solcher Einrichtungen dem Gesundheitsamt oder der Ortspolizeibehörde über die Besucher Auskunft geben können. Diese Angaben umfassen Namen und Vornamen, Datum und Uhrzeit (Beginn und Ende) des Besuchs, eine Telefonnummer oder Adresse. Die Daten sind vier Wochen nach der Erhebung zu löschen. Betriebe, die sich einen Onlineshop leisten können, werden mit der Erfüllung der Anforderungen an die Datenerhebung weniger Probleme haben; alle anderen haben mit Besucherschlangen und Papierbergen zu rechnen. Mit dem Grundsatz der Datensparsamkeit haben die Anforderungen wenig gemein.

Bleibt die (vage) Hoffnung, dass damit anonyme Schwimmbad- und Restaurantbesuche nicht der Vergangenheit angehören – und die Listen nicht zum Standard werden. Schließlich könnte ja eine zweite Infektionswelle kommen – und da wäre es doch praktisch, auf diese Daten zurückgreifen zu können...

Corona-App und Datenschutz

Nach vielen Warnungen hat die Bundesregierung am 26.04.2020 den Schwenk auf eine freiwillige, dezentrale App-Lösung zur Kontaktverfolgung und Infektionseindämmung vollzogen. SAP und die Deutsche Telekom sollen die App nun bis Mitte Juni fertigstellen. Viele Politiker möchten weitere Lockerungen der Kontaktbeschränkungen mit der Einführung einer solchen App verknüpfen, um bei Neuinfektionen mögliche weitere Betroffene zukünftig schneller und mit weniger Aufwand informieren zu können.

Mit der Hinwendung zu einem datenschutz-freundlicheren, dezentralen Konzept sind die Herausforderungen jedoch noch nicht gelöst. Es bleibt eine pseudonyme Datenverarbeitung durch den Anbieter, zu der Rechtsgrundlage, Verantwortlichkeit und Sicherheit zu bestimmen sind. An der Einwilligung des Nutzers als Rechtsgrundlage hat bereits der EDSA Zweifel geäußert. Kritisch wird diesbezüglich die Freiwilligkeit sein. Diese besteht nur, wenn Eingriffslockerungen wie Restaurantbesuche auch von privater Seite nicht von der App-Nutzung abhängig gemacht werden.

Ungeklärt sind zudem die Folgen von Kontaktwarnungen. Ist der Nutzer dadurch zur Quarantäne verpflichtet, hat er einen sofortigen Testanspruch oder besteht sogar eine Testpflicht? Gilt der Nutzer nach einer Warnung als „in Kontakt mit einem Infizierten" und werden die App-Daten damit zum Beweismittel gegen den Nutzer?

Diese Fragen erfordern ein Begleitgesetz, denn für eine diesbezügliche Verordnung gibt das Infektionsschutzgesetz selbst bei weitester Dehnung keine Ermächtigung her. Einen sehr bedenkenswerten Gesetzentwurf hat eine Privatinitiative bereits vorgelegt. Die Verfügbarkeit der App wird dadurch jedoch weiter verzögert, denn im Unterschied zu einer Verordnung unterliegen Gesetze demokratischen Entscheidungsprozessen.

Zuverlässige Corona-App?

Unabhängig von der datenschutz-konformen Gestaltung der Corona-App stellt sich die grundlegendere Frage, ob eine derartige App die in sie gesetzten Erwartungen auch technisch erfüllen kann. Die vorgeschlagenen Lösungen basieren überwiegend auf der Signalstärkemessung mittels *Bluetooth Low Energy Beacons*, beispielsweise mit den Google und Apple APIs. Leider sind derartige Messungen physikalisch bedingt trotz Kalibrierungen sehr ungenau und werden durch Faktoren wie die Antennenform,

den Gerätetyp und die Umgebung stark beeinflusst. Nicht ohne Grund werden bei der Entfernungsmessung (z. B. mit GPS) nicht die Signalstärken, sondern die sehr viel präziseren Zeitdifferenzen zwischen dem Senden und Empfangen verwendet.

Tatsächlich kann auch die Exposition nicht verlässlich festgestellt werden, da sich Smartphones in der Regel nur beim Telefonieren in Gesichtsnähe befinden und sonst meist in einer Hosen-, Hand- oder Jackentasche stecken oder irgendwo herumliegen. Bluetooth-Signale werden zudem von Vorhängen, Plexiglasscheiben und dünnen Wänden nicht abgeschwächt. Daher sind häufige Fehlerkennungen zu erwarten – sowohl *false positives* (Kontakteinträge, auch wenn die Personen wirksam voreinander geschützt waren) als auch *false negatives* (keine Kontakteinträge, weil z. B. die Smartphones weiter voneinander entfernt waren als die Personen oder das Signal abgeschirmt wurde).

Die Messungen sind daher prinzipiell unzuverlässig und können nur Hinweise geben. Zudem könnten Angreifer mittels starker Signale die App täuschen und einer großen Zahl von Personen einen Kontakt mit einem Corona-Infizierten vorspielen. So ließe sich beispielsweise ein ganzes Unternehmen vorsätzlich in Quarantäne schicken. Weitere Angriffsmöglichkeiten sind das Kopieren fremder Identitäten oder Falschmeldungen zu positiven Tests.

Zwar ist die Forderung nach staatlichem Schutz vor der Corona-App zu begrüßen, aber auch darüber lassen sich die technisch bedingten Unzulänglichkeiten und die genannten Angriffsvektoren nicht ausräumen. So deutet alles darauf hin, dass der praktische Nutzen der App im besten Fall eher gering sein dürfte – und im schlimmsten sogar die negativen Folgen überwiegen.

Corona-Patientendatenschutz

Einige Gesundheitsämter haben sich in den vergangenen Wochen offenbar „vorsorglich“ mit Schreiben an die Kliniken ihrer Region gewandt und diese zur unverzüglichen Fax-Übermittlung aller Entlassungsberichte von mit Corona-Viren infizierten Patienten aufgefordert. Tatsächlich lässt sich aus dem Infektionsschutzgesetz jedoch keine solche Ermächtigung ableiten. Die Gesundheitsämter müssen sich, wenn sie diagnostische Daten benötigen, direkt an die betroffenen Patienten wenden. Denn auch eine Pandemie entbindet Kliniken nicht von der ärztlichen Schweigepflicht, und sie entzieht den Betroffenen auch nicht ihre Persönlichkeitsrechte.

Eine Übermittlung von Patientendaten an die Gesundheitsämter ist damit regelmäßig nicht nur ein Verstoß gegen geltendes Datenschutzrecht, sondern nach § 203 Strafgesetzbuch eine Verletzung von Privatgeheimnissen – und damit eine Straftat. Werden die Patientendaten dann auch noch per Fax übermittelt, kann dies zudem als ein mindestens fahrlässiger Verstoß gegen Sicherungspflichten gewertet werden.

Videokonferenzen & Datenschutz

Die Berliner Beauftragte für Datenschutz hatte am 08.04.2020 auf der Webseite ihrer Behörde eine „Checkliste zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen“ bereitgestellt. Darin wies sie darauf hin, dass die Dienste Microsoft Teams, Skype Communications und Zoom Video Communications „die aufgeführten Bedingungen nicht erfüllen.“

Microsoft veröffentlichte daraufhin am 06.05.2020 eine Stellungnahme, in der sich das Unternehmen gegen diese Einschätzung von Teams und Skype wehrt. Unterschiedliche Medien berichten in diesem Zusammenhang von einer Abmahnung von Microsoft gegenüber der Berliner Beauftragten für Datenschutz. Kurz darauf war das Dokument der Datenschutzaufsicht nicht mehr abrufbar.

Dabei ist nicht etwa der Inhalt des Dokuments unzutreffend. Vielmehr wurde von der Aufsichtsbehörde nicht begründet, warum genau die genannten Produkte die Anforderungen nicht erfüllen. Seit dem 22.05.2020 ist eine überarbeitete Version 1.3 der Checkliste verfügbar, in der die Behörde weiterhin fordert, kurzfristig eingesetzte „nicht datenschutzgerechte Lösungen“ so bald wie möglich abzulösen, aber auch ankündigt, „in Kürze eine ausführlichere Übersicht mit detaillierteren Angaben zu verschiedenen gängigen Anbietern von Videokonferenz-Diensten zu erstellen.“

Doch wie findet man bis dahin geeignete datenschutzrechtlich zulässige Produkte? Auf die Tests von Institutionen wie der Stiftung Warentest kann man sich dabei wohl eher nicht stützen – Testsieger waren am 13.05.2020 Microsoft Teams und Skype, trotz eines „befriedigend“ beim „Basisschutz persönlicher Daten“.

Secorvo News

Herbstseminare

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg eingestellten Seminarbetrieb werden wir wie geplant nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen Ihnen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
09.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
16.-20.08.	Crypto 2020 (IACR, Santa Barbara/US)

Fundsache

Im April 2020 veröffentlichte das CrypTool-Entwicklerteam Release 2020.1 der Version 2 des bewährten Kryptographie-Lerntools. Es enthält zahlreiche Verbesserungen, Ergänzungen und Korrekturen – darunter auch ein Tutorial für die Differentielle Kryptoanalyse. Die neue Version wird im Dezember bei unserem Adventsrätsel „Krypto im Advent“ zum Einsatz kommen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
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