Für inhaltliche Rückfragen erreichen Sie unser Team unter digikoletter(at)protonmail.com

Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung

Digitale Werkzeuge, wie Apps zur Kontaktnachverfolgung, können einen unterstützenden Beitrag zur Bewältigung einer Pandemie leisten. Um ihr Potential voll entfalten zu können, müssen solche Werkzeuge zielgerichtet in eine Gesamtstrategie eingebettet werden und das Vertrauen der Bevölkerung genießen. Wenn durch ihre Einführung auch neue Risiken für Bürger:innen und Gesellschaftsgruppen entstehen, muss ihr Nutzen gegen diese Risiken abgewogen werden.

Vor einem Jahr haben mehr als 600 internationale Wissenschaftler:innen in einem offenen Brief an ihre Regierungen appelliert, Technologien zur digitalen Kontaktverfolgung verantwortungsbewusst und zielgerichtet zu entwickeln und einzusetzen. Dabei wurde die Einhaltung grundlegender Entwicklungsprinzipien gefordert, die in Deutschland mit der Corona-Warn-App größtenteils vorbildlich umgesetzt wurden:

- **Zweckbindung:** Das einzige Ziel muss die Pandemiebekämpfung sein. Eine Verknüpfung mit anderen Geschäftsmodellen, Anwendungsmöglichkeiten und Profitinteressen muss ausgeschlossen, idealerweise technisch unmöglich sein.
- **Offenheit und Transparenz:** Fachleuten, IT-Sicherheits- und Datenschutzexpert:innen muss frühzeitig die Möglichkeit gegeben werden, sich konstruktiv am Entwicklungsprozess zu beteiligen oder diesen unabhängig zu begutachten.
- **Freiwilligkeit:** Die Nutzung bestimmter Werkzeuge zur digitalen Kontaktverfolgung muss freiwillig sein. Bürger:innen, die das Werkzeug nicht benutzen möchten, dürfen nicht von sozialen Aktivitäten, dem Zutritt zu öffentlichen Gebäuden, Geschäften, usw. ausgeschlossen werden.
- **Risikoabwägung:** Die Beurteilung des Nutzens und der Risiken einer solchen Lösung muss im Vorfeld unabhängig und öffentlich geprüft werden können. Dies gilt ganz besonders dann, wenn der Effekt der technischen Lösung in wesentlichem Umfang auf dem Vertrauen der Bürger:innen basiert.

Der aktuell viel diskutierte Ansatz, digitale Hilfsmittel zur Kontaktnachverfolgung in öffentlichen Räumen und für Veranstaltungen einzubeziehen, erscheint sinnvoll. **Richtig** eingesetzt könnten sie Infektionsketten schneller unterbrechen und die Gesundheitsämter entlasten.

Konkrete funktionale Anforderungen für solch eine digitale Kontaktnachverfolgung wurden durch die verantwortlichen Behörden bislang nicht transparent und klar kommuniziert. Doch nur so ist es möglich effektive Lösungen zu entwickeln, welche einen sinnvollen Beitrag zur Eindämmung der Pandemie leisten können und dabei personenbezogene Daten nur in einem Umfang erheben, der auf das dafür notwendige Maß beschränkt ist.

LUCA

Das bereits in vielen Bundesländern eingesetzte LUCA-System erfüllt keine dieser Prinzipien. Es gibt keine technische Zweckbindung, sondern es wurden bereits weitere Geschäftsmodelle basierend auf LUCA diskutiert [1]. Damit entsteht eine Abhängigkeit von einem einzelnen Privatunternehmen mit Gewinnerzielungsabsicht als Betreiber des Systems. Es wurde ein intransparent entwickeltes System in Betrieb genommen und selbst leicht zu findende Sicherheitslücken konnten erst im laufenden Betrieb entdeckt werden. Wird die App Voraussetzung, um am öffentlichen Leben teilnehmen zu können oder gar von Corona-Schutzverordnungen vorgegeben [2], ist die Freiwilligkeit nicht gegeben, da ein *de facto* Nutzungszwang entsteht.

Der Nutzen des LUCA-Systems bleibt zweifelhaft, da sich die aktuelle Umsetzung im Wesentlichen auf die Automatisierung der manuellen Erfassung von Papierlisten beschränkt, die Auswertung jedoch weiter manuell durch die Gesundheitsämter erfolgt. Da mit LUCA falsche oder gar manipulierte Anmeldungen und Check-Ins leicht und in großer Zahl erzeugt werden können, entsteht zudem die Gefahr, dass die Belastung der Gesundheitsämter bei abnehmender Datenqualität zunimmt [3].

Gleichzeitig erfasst das LUCA-System in großem Umfang Bewegungs- und Kontaktdaten: wer war wo, mit welchen Personen am selben Ort, und wie lange. Die Daten werden zentralisiert und auf Vorrat bei einem Privatunternehmen gesammelt und gespeichert. Die viel beworbene doppelte Verschlüsselung der Kontaktdaten liefert schon deshalb nicht die versprochene Sicherheit, da sich Bewegungsprofile der Nutzer:innen allein aufgrund der anfallenden Metadaten erstellen lassen. Eine solche umfassende Datensammlung an einer zentralen Stelle birgt massives Missbrauchspotential und das Risiko von gravierenden Datenleaks [4].

Einzelne Systeme, die als zentrale Datenspeicher fungieren, sind attraktive und kaum vor Angriffen zu schützende Ziele. Selbst große Unternehmen sind nicht in der Lage, solche Systeme vollständig zu sichern. Es ist nicht zu erwarten, dass dies einem Start-Up, das bereits durch zahlreiche konzeptionelle Sicherheitslücken, Datenleaks und fehlendem Verständnis von fundamentalen Sicherheitsprinzipien [5] aufgefallen ist, besser gelingen sollte.

Fazit

Für den Erfolg von digitalen Hilfsmitteln zur Kontaktverfolgung ist eine breite Unterstützung der Bevölkerung essentiell. Das gilt insbesondere, wenn diese tief in die Privatsphäre der Bürger:innen eingreifen und in umfassender Weise vertrauliche Daten erheben. Das hierfür notwendige Vertrauen kann nur durch Transparenz und Privacy-by-Design, zum Beispiel durch echte Dezentralisierung, geschaffen werden. Sicherheit und Datenschutz sind elementare Voraussetzungen für die Akzeptanz und damit den erhofften Nutzen eines solchen Systems.

Es gibt bereits Systeme, die in diesem Sinne die Risiken für Bürger:innen auf ein Minimum reduzieren und dabei eine schnellere Benachrichtigung garantieren. Dies sind dezentrale Lösungen, wie sie in der Corona-Warn-App, NotifyMe (Schweiz), NHS COVID-19 (Großbritannien) und NZ COVID Tracer (Neuseeland) umgesetzt und bereits genutzt werden. Die mit dem LUCA System verbundenen Risiken erscheinen völlig unverhältnismäßig, da sie den erwarteten Nutzen deutlich überwiegen.

Wir empfehlen eindringlich die Rückbesinnung auf die oben genannten Prinzipien und deren Anwendung bei der Entwicklung digitaler Werkzeuge zur Kontaktnachverfolgung. Insbesondere sollte es aus unserer Sicht keinen *de facto* Zwang zur Nutzung einer Lösung geben, die diese Prinzipien eklatant verletzt.

Falls es konkrete Anforderungen gibt, die von bestehenden dezentralen Systemen noch nicht erreicht werden, dann müssen diese klar formuliert werden, so dass zielgerichtet entsprechende Erweiterungen entwickelt werden können. Auch in einem dezentralen und datensparsamen System können notwendige Informationen zur Pandemiebekämpfung erhoben und den Gesundheitsämtern zur Verfügung gestellt werden.

Referenzen

[1] Bereits am 25. März 2021 gaben Ticket i/O und die Entwickler des LUCA-Systems ihre Zusammenarbeit bekannt. Bisher geht es dabei um die Verifizierung von Schnelltests. Interne Dokumente weisen jedoch auf eine Ausweitung der Kooperation hin.
[2] Aus der Coronaverordnung des Landes Mecklenburg-Vorpommern: "Die verpflichtende Dokumentation zur Kontaktnachverfolgung soll in elektronischer Form landeseinheitlich mittels LUCA-App erfolgen".
[3] Dass ein Check-In von beliebigen Orten aus möglich ist, wurde bereits in der Praxis demonstriert.
[4] Eine ausführliche Analyse der Risiken des LUCA-Systems wurde bereits am 23. März 2021 als Preprint veröffentlicht. Darauf wurde auch in einer Stellungnahme des BfDI hingewiesen.
[5] Eine umfassende Übersicht über die festgestellten Mängel im grundsätzlichen Systementwurf sowie bei der Umsetzung gibt eine Stellungnahme des CCC.

Erstunterzeichnende

1. Prof. Dr. Florian Alt, Forschungsinstitut CODE, Universität der Bundeswehr München
2. Prof. Dr. Frederik Armknecht, Universität Mannheim
3. Prof. Dr. Michael Backes, CISPA Helmholtz Center for Information Security
4. Prof. Dr. Markus Bläser, Universität des Saarlandes
5. Prof. Dr. Eric Bodden, Heinz Nixdorf Institut der Universität Paderborn und Fraunhofer IEM
6. Prof. Dr. Franziska Boehm, Karlsruher Institut für Technologie (KIT)/FIZ Karlsruhe
7. Prof. Dr. Kevin Borgolte, Ruhr-Universität Bochum
8. Prof. Dr. Stefan Brunthaler, Forschungsinstitut CODE, Universität der Bundeswehr München
9. Dr.-Ing. Sven Bugiel, CISPA Helmholtz Center for Information Security
10. Prof. Dr. Cas Cremers, CISPA Helmholtz Center for Information Security
11. Dr. Jean Paul Degabriele, Technische Universität Darmstadt
12. Prof. Dr. Christian Dietrich, Westfälische Hochschule
13. Prof. Dr. Gabi Dreo Rodosek, Forschungsinstitut CODE, Universität der Bundeswehr München
14. Prof. Dr. Hannes Federrath, Universität Hamburg, Arbeitsbereich Sicherheit in verteilten Systemen
15. Dr.-Ing. Tobias Fiebig, TU Delft
16. Prof. Dr. Nils Fleischhacker, Ruhr-Universität Bochum
17. Prof. Dr.-Ing. Felix Freiling, Friedrich-Alexander-Universität Erlangen-Nürnberg
18. Dr. Michael Friedewald, Fraunhofer ISI
19. Prof. Dr.-Ing. Mario Fritz, CISPA Helmholtz Center for Information Security
20. Dr.-Ing. Kai Gellert, Bergische Universität Wuppertal
21. Prof. Dr.-Ing. Ulrich Greveler, Hochschule Rhein-Waal
22. Asst.-Prof. Priv.-Doz. Dr. Daniel Gruss, TU Graz
23. Dr. Seda Gurses, TU Delft
24. Dr. Felix Günther, ETH Zürich
25. Prof. Dr. Sabine Hark, TU Berlin
26. Prof. Dr. Andreas Heinemann, Hochschule Darmstadt
27. Prof. Dr. Dominik Herrmann, Otto-Friedrich-Universität Bamberg
28. Prof. Dr. Thorsten Holz, Ruhr-Universität Bochum
29. Prof. Dr. Wolfgang Hommel, Forschungsinstitut CODE, Universität der Bundeswehr München
30. Prof. Dr.-Ing. Thomas Hupperich, Universität Münster, European Research Center for Information Systems
31. Dr.-Ing. Swen Jacobs, CISPA Helmholtz Center for Information Security
32. Prof. Dr.-Ing. Tibor Jager, Bergische Universität Wuppertal
33. Prof. Dr. Martin Johns, Technische Universität Braunschweig
34. Dr. Ghassan Karame, NEC Laboratories Europe
35. Prof. Dr. Stefan Katzenbeisser, Universität Passau, PIDS
36. Prof. Dr. Elif Bilge Kavun, University of Passau
37. Prof. Dr. Doğan Kesdoğan, Universität Regensburg
38. Prof. Dr. Eike Kiltz, Ruhr-Universität Bochum
39. Prof. Dr. Teresa Koloma Beck, Helmut-Schmidt-Universität
40. Prof. Dr.-Ing. Dorothea Kolossa, Ruhr-Universität Bochum
41. Prof. Dr. Martin Kreuzer, Universität Passau, PIDS
42. Dr. Katharina Krombholz, CISPA Helmholtz Center for Information Security
43. Prof. Dr. Nicole Krämer, Universität Duisburg-Essen
44. Dr. Robert Künnemann, CISPA Helmholtz Center for Information Security
45. Prof. Dr. Gregor Leander, Ruhr-Universität Bochum
46. Prof. Dr. Anja Lehmann, Hasso-Plattner-Institut, Universität Potsdam
47. Prof. Dr. Klaus-Peter Löhr, FU Berlin
48. Prof. Dr. Michael Meier, Universität Bonn
49. Prof. Dr.-Ing. Mira Mezini, Technische Universität Darmstadt
50. Prof. Dr. Esfandiar Mohammadi, Universität zu Lübeck
51. Dr. Sebastian Pape, Goethe-Universität Frankfurt
52. Dr. Giancarlo Pellegrino, CISPA Helmholtz Center for Information Security
53. Prof. Dr. Günther Pernul, Universität Regensburg
54. Prof. Dr. Joachim Posegga, Universität Passau, PIDS
55. Prof. Dr. Kai Rannenberg, Goethe-Universität Frankfurt
56. Prof. Dr. Steffen Reith, Hochschule RheinMain
57. Prof. Dr. Anne Remke, WWU Münster
58. Prof. Dr. Konrad Rieck, Technische Universität Braunschweig
59. Prof. Dr. Oliver Rose, Dekan Informatik, Universität der Bundeswehr München
60. Prof. Dr. Christian Rossow, CISPA Helmholtz Center for Information Security
61. Prof. Dr. Martina Angela Sasse, Ruhr-Universität Bochum
62. Dr. Ralf Sasse, ETH Zürich
63. Prof. Dr. Sebastian Schinzel, FH Münster
64. Prof. Dr.-Ing. Thomas Schneider, Technische Universität Darmstadt
65. Prof. Dr.-Ing. Thomas Schreck, Hochschule München
66. Prof. Dr. Dominique Schröder, Friedrich-Alexander-Universität Erlangen-Nürnberg
67. Prof. Dr. Peter Schwabe, Max Planck Institute for Security and Privacy
68. Prof. Dr. Matthew Smith, Rheinische Friedrich-Wilhelms-Universität Bonn, Fraunhofer FKIE
69. Prof. Dr.-Ing. Juraj Somorovsky, Universität Paderborn
70. Prof. Dr.-Ing. Christoph Sorge, Universität des Saarlandes
71. Prof. Dr. LL.M. Indra Spiecker genannt Döhmann, Goethe-Universität Frankfurt
72. Dr.-Ing. Cristian-Alexandru Staicu, CISPA Helmholtz Center for Information Security
73. Dr.-Ing. Ben Stock, CISPA Helmholtz Center for Information Security
74. Prof. Dr. Gunnar Teege, Forschungsinstitut CODE, Universität der Bundeswehr München
75. Prof. Dr. Florian Tschorsch, TU Berlin
76. Prof. Dr. Arno Wacker, Forschungsinstitut CODE, Universität der Bundeswehr München
77. Prof. Dr. Andreas Zeller, CISPA Helmholtz Center for Information Security

Weitere Unterzeichnende (Auch unterzeichnen)

1. M.A. sanddrn @sand2drn
2. Dipl. Inf. (FH) Tobias Abstreiter
3. Dr.-Ing. Michael Adams
4. Dipl.-Ing. Patrick Ahlbrecht
5. Leonie Ain, koyu.space
6. M.Sc. Lars Almon, Technische Universität Darmstadt
7. Sebastian Alscher, Piratenpartei Deutschland
8. Christian Aretz, VP Data Protection GmbH
9. Manuel Atug, CCC & AG KRITIS
10. Dr. rer. nat. Arne Babenhauserheide
11. M. Sc. Andreas Baldeau
12. Steffen Becker, Ruhr-Universität Bochum
13. Michael Bemmerl
14. Dipl. Inf. Jan Bensch, Hochschule Zittau/Görlitz
15. Frank Berger, Berger, IT-Dienstleistungen
16. Dipl.-Inform. Birko Bergt
17. Dr. rer. nat. Sebastian Berndt, Universität zu Lübeck
18. Stefan Bertels
19. B.Sc. André Beuker
20. Hans-Georg Bickel, Rechtsanwalt, Vorsitzender Kulturkeller e.V.
21. Thomas Bierlein, Fachanwalt für IT-Recht
22. Matthias Bitterlich, Stadt Waren (Müritz) - IT/EDV
23. Leonie Philine Bitto, Full Stack Developer
24. Eugen Blattner, Mayflower GmbH
25. Quality Engineer agile Softwareentwicklung Mirja Blömer, QA
26. Ass jur Kirsten Bock, Datenschutzexpertin
27. B. Sc. Martin Bock, Hochschule der Medien Stuttgart
28. Dr. med. Simon Bock
29. Felix Bohnacker
30. Dipl.-Inf. Christoph Borowski
31. Dr.-Ing. Christian Borß
32. Tim Bossenmaier
33. M.Sc. Davide Bove
34. Dipl. Phys. Gregor Bransky, Layer 9 Solutions
35. Konferenzdolmetscher MA Marius Braun
36. Dr. Jacqueline Brendel, CISPA Helmholtz Center for Information Security
37. Jonas Bushart, CISPA Helmholtz Center for Information Security
38. Renée Bäcker
39. Christoph Bölck
40. Dipl.-Informatiker Josef Börding, Fraunhofer IAIS
41. Felix Büdenhölzer, Senior IT Security Consultant & CCCFr
42. Eike Bühring
43. Jens Büttner
44. Ing. Peter Chvojka, Bergische Universität Wuppertal
45. Dominique Clijsters
46. Aaron Czichon
47. Dr. Gareth T. Davies, Bergische Universität Wuppertal
48. M.Sc. Dennis Dayanikli, Hasso-Plattner-Institut, Universität Potsdam
49. Prof. Dr. Christian Decker, Informatik, Hochschule Reutlingen
50. Cemil Degirmenci, Wavecon GmbH
51. Dr.-Ing. Daniel Demmler, Uni Hamburg
52. Christian Dersch, Piratenpartei Deutschland, Kreisverband Marburg-Biedenkopf
53. Janis Detert
54. Dr. rer. nat. Andreas Dewes, KIProtect GmbH
55. Steffen Diering
56. Torsten Dillenburg
57. Karl Dissen
58. MA Anke Domscheit-Berg, MdB, Deutscher Bundestag
59. Prof. Dr. Christian Drumm, FH Aachen, Fachbereich Wirtschaftswissenschaften
60. M.Sc. Arno Däuper
61. Peter Eckel
62. Dipl. Inf. Andreas Ecker
63. Jens Edler
64. Markus Eisele
65. Prof. Dr.-Ing. Thomas Eisenbarth, Universität zu Lübeck
66. Frank Elsner
67. Prof. Dr. Malte Elson, Ruhr-Universität Bochum
68. Assoc. Prof. Dr. Michael Engel, NTNU Trondheim
69. Dr. Jur. Malte Engeler
70. Philip Engelmartin
71. Peter Falter
72. Julian Feder
73. Journalist Markus Feilner, Feilner IT
74. Diplom-Informatiker (FH) Wolfgang Fey
75. Thomas Fischer
76. M.Sc. Thorsten Fischer
77. M. Sc. Dominik Flagner
78. Dr. David Foerster
79. Uli Fouquet, Digitalcourage OG Braunschweig
80. Dipl.-Inf. Achim Friedland, GraphDefined GmbH
81. Dipl. Inf. (FH) Andreas Frieser
82. Dr.-Ing. Tilman Frosch
83. Dr. rer. nat. Matthias H. Fröhlich
84. Sebastian Fuhrmann, Web-Entwickler u. IT-Security, Rechenzentrum Fuhrmann
85. Informatiker Peter Funk, ArtCom GmbH
86. M.Sc. Alexander Förstel, resist.berlin
87. Gabriel Fürst
88. Christian Gaida
89. M.A. Benjamin Garske
90. Malvin Gattinger, University of Groningen
91. Dipl. Ing. (FH) Florian Geldner, Senior Product Manager
92. Prof. Dr. Peter Gerwinski, Hochschule Bochum
93. Diplom Informatiker Mario Glagow, Energiesektor
94. Florian Glatzner
95. M. Sc. Dustin Glaß
96. M.Sc. Andreas Grapentin, Hasso Plattner Institut, Universität Potsdam
97. Patrick Grihn, nextindex GmbH & Co. KG (DSB Ruhr)
98. Dr. Ilya Grishchenko, CISPA Helmholtz Center for Information Security
99. Dr.-Ing. Martin Grothe
100. M.Sc. Matteo Große-Kampmann, AWARE7 GmbH / Westfälische Hochschule
101. Dipl. Inf. Kai Gärtner
102. Prof. Dr.-Ing. Matthias Güdemann, Hochschule München
103. Peter Güman
104. Manuel Günther, Medienwissenschaftler
105. Kristina Haase
106. M.Sc. Oliver Hader, hofhäckerei Software Engineering
107. B.Sc. Wirtschaftsinformatik Matthias Hahn
108. Dominic Hallau
109. Dipl.-Math. Sven M. Hallberg
110. Lars Hammerschmidt, OX Berlin
111. Kevin Hartmann
112. Eduard Hauck, Ruhr Uni Bochum
113. Manfred Hauffen, ZKM Zentrum für Kunst und Medien
114. Dr.-Ing. Vincent Haupert
115. Jonas Heberer, Hochschule RheinMain
116. Markus Heberling
117. Lukas Heiland, Universität Regensburg
118. Christian Heimes, Python Security Response Team
119. Nils Hempel
120. Dr. Marc Herbstritt, Albert-Ludwigs-Universität Freiburg
121. JProf. Dr.-Ing. Ben Hermann, Technische Universität Dortmund
122. Günther Hermann
123. Rechtsanwalt Stefan Hessel, Algoright e.V.
124. Ba. Sc. Lennart Hessenauer
125. Dipl. Dok. (FH) Anja Hirschel, Piratenpartei
126. Christian Hoffmann
127. Dr. rer. nat. Kurt M. Hofstetter
128. Dipl.-Ing. Daniel Hofstetter
129. b.Sc. Tobias Hoge
130. ass. iur.; Dipl.Forstwirt (univ.) Roland Hoheisel-Gruler, HS Bund
131. David Holin
132. Thorsten Huber, crazyALEX.de GmbH
133. Dr. Anna Jager
134. Tomas Jakobs
135. Dr. Christian Janson, Technische Universität Darmstadt
136. Michael Junker, Google Cloud Architect
137. Dipl.-Ing. Maik Kaemmerer
138. Kristof Kamm
139. Bianca Kastl, Team #LucaTrack
140. Dipl.-Inform. Philipp Kern
141. Dipl. Inf. Sascha Kieferr
142. Software-Engineer Max Kiehnscherf
143. Niklas Kilian
144. Dipl.-Ing. Jürgen Kleer
145. Dr.-Ing. Thomas Kleinbauer, Saarland Informatics Campus, Saarland University
146. Michael Kleinhenz, Software-Entwickler
147. Christian Klemm, Volt Deutschland
148. Dipl.-Inf. Martin Klepper
149. Holger Kloss
150. Dominik Kloé, IAM & Security Consultant
151. Florian Knodt, Network Engineer
152. Dipl.-Ing. Martin Knopp, Technische Universität München
153. M. Sc. IT-Sicherheit Phil Knüfer
154. M.Sc. Sebastian Koch
155. Prof. Dr. Alexander Koller, Universität des Saarlandes
156. Marcel Komowski, IT-Consultant
157. Dipl.-Ing. Simon Kowalewski, Piratenpartei Berlin
158. Alexander Krause
159. J. Maximilian Kroschewski, Hasso-Plattner-Institut, Universität Potsdam
160. Henry Krumb
161. Johannes Krupp, CISPA Helmholtz Center for Information Security
162. Diplom-Informatiker Andreas Kruse
163. Matthias Kuom
164. J. Kupfer
165. Sven Köhler, Hasso-Plattner-Institut, Universität Potsdam
166. Dr. Frank Köhne, viadee IT-Unternehmensberatung AG
167. Sebastian König
168. Lars Kück
169. M.Sc. Georg Land, Ruhr-Universität Bochum
170. Eric Lanfer, Chaostreff Osnabrück e.V.
171. PD Dr. Katja Lapshinova, Universität des Saarlandes
172. Dipl. Wirtschaftsinformatiker Athanasios Lasos
173. Marius Lauer
174. Dipl.-Ing. Peter Leppelt
175. Frank Lerche, Piratenpartei Deutschland, Kreisverband Marburg-Biedenkopf
176. Stefan Lewanskowski
177. Nicolas Louis, Universität des Saarlandes
178. Jens Luef
179. Rudolf Lörcks
180. B. Eng. Matthias Mahler
181. Chris Martin
182. Matthias Marx, Universität Hamburg
183. Tobias Maschek
184. Daniel Maslowski
185. Denis Maurer
186. Thomas Mechenbier, CISPA Helmholtz Center for Information Security
187. MSc Wirtschaftsinformatik Markus Mergle
188. Dipl. Inform. Matthias Meyer, MAMEDO IT-Consulting GmbH
189. Dipl.-Ing. Ulrich Meyer-Ciolek, IT-Beratung
190. Mirko Mollik, TrustCerts
191. Dr.-Ing. Andreas Mull
192. Fridtjof Mund
193. B.Sc. Florian Märkl
194. M.Sc., LL.M. Frederik Möllers, Saarbrücker Zentrum für Recht und Digitalisierung & Defendo IT GmbH
195. M. Sc. Cedric Mössner
196. Dr. Rainer Mühlhoff, Technische Universität Berlin
197. Staatlich geprüfter Techniker für Betriebsinformatik Maik Nauheim, Westwoodlabs e.V.
198. B. Sc. Florian Nehmer
199. Dipl.-Phys. Lothar Neumann
200. Dipl.-Psych. Linus Neumann, Chaos Computer Club
201. Msc. David Niehues, Universität Paderborn
202. Dipl. chem. Sascha Nonn
203. Aaron Nottbeck
204. Maximilian Ochs, Volt Deutschland
205. Carsten Ott
206. Konrad Oziom
207. Manfred Paul, Vulnerability Researcher
208. Dipl.-Ing. Dominik Paulmichl
209. B. Eng. Johannes Pein, Universität Leipzig
210. David Pfaff, CISPA Helmholtz Center for Information Security
211. Jonas Pfalzgraf
212. Felix Pfeiffer
213. Pascal Pflaum
214. Dipl.-Ing. (FH) Nils Philippsen
215. Prof. Dr. Joel Phillips
216. M.Sc. Stephan Plarre, Freifunk
217. B.Sc. Sebastian Preuß, FDP Brandenburg
218. Dr. Daniela Pöhn, Forschungsinstitut CODE, Universität der Bundeswehr München
219. Tobias Ravenstein
220. Youssef Rebahi-Gilbert
221. Rainer Rehak, Weizenbaum-Institut für die vernetzte Gesellschaft
222. Dr. Christoph Reichenbach, Universität Lund
223. Datacenter Architect Timo Reimann
224. Journalist Marcus Richter, richter.fm
225. Martin Richter, Datenschutzbeauftragter
226. Jens Rieger, CCCFr
227. Marko Rogge
228. Kevin Rohland
229. Karsten Rohrbach
230. Anne Roth, Referentin für Netzpolitik, Die Linke im Bundestag
231. Dipl Biol. (Molekularbiologie) Thomas Rother
232. Ralf Rottmann
233. Ilja Rozhko, Software Developer
234. Alexander Ruhland
235. Dr.-Ing. Paul Rösler, TU Darmstadt
236. B.Sc. Computerlinguistik Justus Saul
237. Dipl.-Ing. Tahar Schaa, Neuland@Homeland GmbH
238. Micha Schauer, Büro für angewandtes Chaos GbR
239. Dominik Scheible
240. Dipl. Ingenieur (Datenschutzkoordinator, IT Compliance Manager) Armin Scherer
241. Veit Schiele, Cusy GmbH
242. Prof. Dr. Ina Schiering, Ostfalia HaW
243. Dr. Michael Schilling, CISPA Helmholtz Center for Information Security
244. Dipl.-Phys. Gerhard Schimpf
245. M. Sc. Thomas Schindler, FAU Erlangen-Nürnberg
246. M. Sc. Moritz Schlarb
247. T. Schlenkhoff, CCCFR / Gardion
248. Dipl. biochem. / Software Engineer Martin Schmidt
249. Dipl.-Inf. Marcus Schmidt
250. Ole Schmidt
251. Max Schmitt
252. M. Sc. Carl Richard Theodor Schneider, Ruhr-Universität Bochum
253. Peter Schneider
254. Jonas Schneider-Bensch, CISPA Helmholtz Center for Information Security
255. Dirk Schneidereit
256. Dipl.-Inform. Peter Schoo
257. Rolf Schorn, Informatiker
258. Dipl.-Ing. Tim Schröder
259. Thomas Schröer
260. MSc Marco Schultewolter, Scutisec Security & Datenschutz
261. Oliver Schuster
262. Philipp Schwab
263. Jens Schwehn
264. Tim Philipp Schäfers, Internetwache.org
265. Prof. Dr.-Ing. Johannes Schöning, Universität Bremen
266. Philipp Schürmann
267. Prof. PhD Hartmut Seichter, Hochschule Schmalkalden
268. Oliver Seifert
269. Leander Seige
270. Dr. Markus Seiler, Thyssenkrupp AG
271. Benjamin Sertl
272. Dipl. Inf. Eric Sesterhenn, X41 D-Sec GmbH
273. Florian Sieck, Universität zu Lübeck
274. Jörg Sievers
275. Hannes Spicker, filmreflex medienpädagogik
276. Theresa Stadler, EPFL
277. Prof. Ralf C. Staudemeyer, Ph.D., Hochschule Schmalkalden
278. Marius Steffens, CISPA Helmholtz Center for Information Security
279. Dr. Dominic Steinhöfel, CISPA Helmholtz Center for Information Security
280. Sebastian Stelter, Universität Hamburg
281. Dipl.-Phys. Manuel Strehl
282. Paul Strobach
283. Dennis Sädtler, Hochschule Trier
284. Datenschutzbeauftragter Jörg Thomi
285. Thore Tiemann, Universität zu Lübeck
286. Ioannis Tourountzis
287. Christian Tramnitz, TraSec GmbH
288. Prof. Dr. Peter Trapp, Hochschule München
289. Prof. Dr. Carmela Troncoso, EPFL, Switzerland
290. Dipl.-Inform. Florian Unger
291. Dajana Unverzagt, Piratenpartei Deutschland, Kreisverband Marburg-Biedenkopf
292. Guido Valentini
293. Markus Vervier, X41 D-Sec GmbH
294. Markus Viel, Senior Developer
295. Friedrich Vierkorn
296. Maximilian Volmari
297. Moritz Vondano, Softwareentwickler
298. Prof. Dr Marcel Waldvogel
299. Marie-Therese Walter
300. Andreas K. Weber, Software-Architekt & Berater
301. Dipl.-Inf. Lorenz Weber
302. Dr. Michael Weber, Stadtverordneter, Piratenpartei, Kreisverband Marburg-Biedenkopf
303. Dr. Christoph Wegener, wecon.it-consulting
304. Felix Wegener
305. B.Eng. Christian Weichselfelder
306. Vanessa Weidler, Uni Stuttgart
307. Marc Simon Timotheus Weidner-Zimnol, Centurion Consulting Weidner-Zimnol
308. Olaf Weitner, SequiSoft GmbH
309. M.A. Andreas Werner
310. MA. Marie Wetzle, CS Uni Saarland
311. Enrico Wexel
312. Daniel Weßling
313. Jan Wichelmann, Universität zu Lübeck
314. M. Sc. Benedikt Wildenhain, Hochschule Bochum
315. M.Sc Kevin Wittek, Institut für Internet-Sicherheit - Westfälische Hochschule
316. M.Sc. Marvin Wißfeld
317. Stefan Wolf, CryptoSoft GmbH
318. Matheo Zech, abat+ Gmbh
319. Klaus Zell, Datenschutzbeauftragter
320. Christoph Ziegenberg, Softwareentwickler
321. Solveigh Zieger
322. Stefan Zitz, Friedrich Alexander Universität Erlangen Nürnberg
323. Prof. Dr. Alf Zugenmaier, Hochschule München
324. Till von Ahnen
325. Prof. Dr. Jörn von Lucke, Zeppelin Universität
326. Nicolai von Neudeck, Cloud Engineer
327. Dipl. phys. Holger Öhm

Zuletzt aktualisiert: 30.04.2021, 08:10:08