ENISA: Keine Patentlösung für die Pseudonymisierung von Daten

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>ENISA: Keine Patentlösung für die Pseudonymisierung von Daten</h1> Stefan Krempl </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: Timofeev Vladimir/Shutterstock.com)</figcaption></figure> Die EU-Cybersicherheitsbehörde ENISA stellt aktuelle Techniken sowie Einsatzszenarien zur Pseudonymisierung vor und fordert vorab eine Risikobewertung. „Pseudonymisierung ist eine etablierte und akzeptierte Datenschutzmaßnahme, die nach der Verabschiedung der Datenschutz-Grundverordnung (DSGVO) zusätzliche Aufmerksamkeit erlangt hat“, schreibt die EU-Cybersicherheitsbehörde ENISA in ihrem vorige Woche veröffentlichten Bericht zu fortgeschrittenen Verfahren und Einsatzmöglichkeiten der Technik. „Jüngste Entwicklungen“ wie das Aus für das Abkommen für den Transfer personenbezogener Daten in die USA machten es nötig, entsprechende geeignete Schutzmaßnahmen weiter voranzutreiben. Auf gut 50 Seiten beleuchtet die ENISA [1] so konventionelle und neuere Pseudonymisierungsmechanismen wie Zufallszahlengeneratoren, kryptographische Hashfunktionen, symmetrische und asymmetrische Verschlüsselung, Ringsignaturen und Gruppenpseudonyme, Pseudonyme auf der Basis von mehreren Identifikatoren oder Attributen, sichere Mehrparteienberechnungen und „Secret Sharing“ Schemata. Zugleich warnt sie, dass es hier keinen „One-size-fits-all“-Ansatz gebe und je für den Einzelfall passende Lösungen gesucht werden müssten. Generell werde der Einsatz und die richtige Anwendung von Techniken, eine Personenbeziehbarkeit von Daten zu erschweren, „heftig diskutiert“, ist der Behörde nicht entgangen. Forscher verweisen darauf, dass mithilfe von Big-Data-Analysen ein individueller Bezug schnell wieder hergestellt werden könnte. Gremien wie die Datenethik-Kommission fordern daher den standardmäßigen Einsatz weitergehender Verfahren zur Anonymisierung und ein Verbot, diese zu umgehen [2]. <h3 class=„subheading“ id=„nav_pseudonymisierun0“>Pseudonymisierung wichtig für Datenschutz</h3> Auf Basis früherer Arbeiten über <a href=„https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices“

rel=„external noopener“ target=„_blank“>bewährte Pseudonymisierungspraktiken [3] und Empfehlungen zur DSGVO-Umsetzung [4] geht es der ENISA aber vor allem darum, dass Anwender den Gesamtkontext einer Datenverarbeitung beachten und die Implementierung verbessern. Der Direktor der Behörde, Juhan Lepassaar, betonte: Security-Techniken wie Pseudonymisierung seien „ein integraler Bestandteil, um die Datenschutzverpflichtungen zu erfüllen und es den Nutzern zu ermöglichen“, und ihr Grundrecht auf Privatsphäre vollumfänglich zu genießen. Generell ist dem Bericht zufolge „ein hohes Maß an Kompetenz erforderlich“, um Bedrohungen zum Aushebeln einschlägiger Techniken zu reduzieren und die Effizienz bei der Verarbeitung pseudonymisierter Daten in verschiedenen Einsatzbereichen zu erhalten. Als konkrete Anwendungsfälle beleuchten die Autoren das Gesundheitswesen und dem Informationsaustausch im Bereich Cybersicherheit. „Ein Arzt benötigt meist Zugriff auf die relevanten medizinischen Daten, aber nicht unbedingt auf die versicherungsrelevanten finanziellen Aspekte“, heißt es in einem Beispiel. Eine Krankenkasse wiederum sollte bestenfalls keinen Zugriff auf viele Details über die genaue Diagnose und die Krankengeschichte haben, solange diese nicht zahlungsrelevant sind. Medizinische Forschungseinrichtungen wiederum bräuchten Informationen darüber, ob ein Patient mit einem bestimmten Medikament behandelt wird oder nicht und obendrein eventuell die Diagnose, aber nicht den echten Namen von Patienten oder die genaue Krankengeschichte oder die finanziellen Daten. Im zweiten Bereich verweisen die Verfasser etwa auf den Streit über Telemetrie-Daten [5] bei Anwendungen wie Microsoft Windows und Office 365. Das Sammeln solcher Nutzungsinformationen aus der realen Welt sei für eine „analytikbasierte“ effiziente Cyberabwehr unerlässlich. Dies könne etwa über eine Honeypot-Infrastruktur weitgehend anonym erfolgen, in den meisten Fällen würden aber Daten per „Crowdsourcing“ von Benutzerendpunkten erhoben, was eine „sensible Aufgabe“ darstelle. Als mögliche organisationale Lösungen jenseits der reinen Technik bringen die Autoren etwa Treuhänder oder „Personal Information Management“-Systeme (PIMS) ins Spiel. <h3 class=„subheading“ id=„nav_risikobewertung_1“>Risikobewertung</h3> Die ENISA plädiert für eine „kontinuierliche Analyse des Stands der Technik im Bereich der Pseudonymisierung“, um neue Forschungsergebnisse und Geschäftsmodelle rasch zu berücksichtigen, sowie die Entwicklung fortgeschrittener Szenarien für Fälle mit hohen Risiken beim Verarbeiten persönlicher Daten. Die EU-Kommission sowie die relevanten Institutionen und Aufsichtsbehörden sollten einen breiteren Einsatz der Technik diskutieren und fördern, „indem sie alle relevanten Akteure in diesem Bereich zusammenbringen“. () <hr /> URL dieses Artikels:
<small>

```
https://www.heise.de/-5042562
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong> https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/
```

</small>
<small>

```
<strong>[2]</strong> https://www.heise.de/meldung/Datenethik-Kommission
```

```
-Verbot-von-De-Anonymisierung-und-Profilbildung-4566788.html
```

</small>
<small>

```
<strong>[3]</strong> https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
```

</small>
<small>

```
<strong>[4]</strong> https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2
```

</small>
<small>

```
<strong>[5]</strong> https://www.heise.de/news/Datenschuetzer-Windows-10-Nutzer-bei-Telemetrie-nicht-aus-dem-Schneider-4976556.html
```

</small>
<small>

```
<strong>[6]</strong> mailto:olb@heise.de
```

</small>
 Copyright © 2021 Heise Medien </html>