Projekt EIDI

Effektive Information nach digitalem Identitätsdiebstahl

Das Projekt „Effektive Information nach digitalem Identitätsdiebstahl (EIDI)“ wurde vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Das vom Unabhängigen Landeszentrum für Datenschutz (ULD) betreute Teilvorhaben „Sammlung digitaler Identitäten – Maßnahmen zur Betroffeneninformation und sowie datenschutzrechtliche und juristische Analyse“ hatte als Gegenstand die Bearbeitung datenschutzrechtlicher Fragestellungen im Kontext der Erhebung und Ermittlung von Gefahren für betroffene Personen durch die Veröffentlichung ihrer Identitätsdaten in Datensammlungen etwa im Darknet. Im Netz sind auf diese Weise Millionen von Daten Betroffener verfügbar, obwohl diese der Veröffentlichung weder zugestimmt haben noch in Kenntnis darüber sind. Dies birgt konkrete Risiken für die Betroffenen, etwa Opfer eines Identitätsmissbrauchs oder Social Engineerings zu werden. Die Unterrichtung der Betroffenen über das Vorliegen solcher öffentlich verfügbaren Informationen über sie dient sowohl der Verwirklichung des Grundrechts auf informationelle Selbstbestimmung als auch dazu, geeignete Schutz- und Vorsichtsmaßnahmen aufseiten der Betroffenen zu treffen.

Strafverfolgungsbehörden und IT-Sicherheitsforscher gelangen bei der Aufklärung von IT-Sicherheitsvorfällen und der Analyse von Schadsoftware oder Botnetz-Kommunikation häufig in den Besitz umfangreicher Sammlungen von Identitätsdaten, die Kriminelle über diese Wege sammeln und austauschen. Es gab bisher keine erprobte oder standardisierte Methode, Opfer zuverlässig und proaktiv über ihre Betroffenheit zu informieren. Um Betroffene frühzeitig über einen Missbrauch ihrer Identität oder den Verlust der Vertraulichkeit ihrer persönlichen Daten zu benachrichtigen und so vor möglichen weiteren Aktionen von Kriminellen zu schützen, müssen verfügbare Identitätsdaten-Sammlungen kontinuierlich analysiert, betroffene Personen identifiziert und angemessen informiert und gewarnt werden. Idealerweise werden den Betroffenen in diesem Zusammenhang auch konkrete und für sie umsetzbare Maßnahmen zur Risikominimierung verständlich vermittelt. In EIDI standen daher diese vier Aspekte im Fokus:

- Qualitätsbewertung verfügbarer Identitätsdatensammlungen,
- effektive und effiziente Information und Warnung betroffener Personen,
- technische Unterstützung des Gesamtprozesses zur Kostenreduktion und
- rechtliche und datenschutzrechtliche Betrachtung relevanter Teile des Gesamtprozesses.

Es wurden verschiedene am Markt vorhandene *Identitätsschutzmodelle* betrachtet. Diese bieten Betroffenen die Möglichkeit zu prüfen, ob ihre personenbezogenen Daten bereits in einer bekannten Identitätsdatensammlung enthalten sind. Betrachtet wurden Lösungen aus dem Angebot einer Versicherung, einer Auskunftei, einer staatlichen Stelle für IT-Sicherheit, eines weiteren Dienstleisters, eines privaten Forschungsinstituts und einer ehrenamtlich gestarteten Initiative. Die Analyse der verschiedenen bestehenden Modelle zeigte, dass der Datenschutz dort bisher sehr unterschiedlich gehandhabt wurde. Hauptkritikpunkt war das Zusammenspiel aus Intransparenz in Bezug auf die Verarbeitung der Nutzerdaten und der umfangreichen Datenerhebung. Daneben überließen die untersuchten Identitätsschutzmodelle die weitere Risikobeurteilung der subjektiven Einschätzung ihrer Nutzenden. Die Analyse führte zu einer Reihe konkreter Hinweise für die weitere Gestaltung im EIDI-Projekt.

Datenerhebung: Für die Phase der Erhebung durch die Forschungspartner im Rahmen des EIDI-Projekts wurden die möglichen Rechtsgrundlagen geprüft für eine Suche nach und Speicherung von Identitätsdatensammlungen sowie mögliche Risiken für die Rechte und Freiheiten der Betroffenen aufgezeigt. Zudem wurden Empfehlungen für technische und organisatorische Maßnahmen unterbreitet, um diese Risiken einzudämmen.

Effektive Benachrichtigung Betroffener: Unter anderem die zuvor genannte Analyse bestehender Identitätsschutzmodelle zeigte, dass die Betroffenen bisher nur sehr generisch über mögliche Folgen informiert werden, die aus einem Leak resultieren können. Empfohlene Schutzmaßnahmen beschränkten sich häufig auf die Änderung von Passwörtern. Im Ergebnis führte dies jedoch dazu, dass Betroffene sich der Situation ausgeliefert fühlen und die Bereitschaft zur Verhaltensänderung, wie beispielsweise die Nutzung verschiedener Passwörter für unterschiedliche Dienste, gleichbleibend gering war. Wünschenswert wäre dagegen z. B. die Trennung digitaler Identitäten oder der verstärkte Einsatz von Mehr-Faktor-Authentifizierung. Im Projekt wurden Hinweise für eine rechtlich hinreichende und in Zusammenarbeit mit den psychologischen Partnern verständliche, nicht abschreckende und zugleich zielführende Gestaltung der Benachrichtigung erarbeitet.

Im Rahmen der Analyse der einzelnen Verarbeitungsschritte wurden zwei verschiedene Methoden der in Art. 35 DSGVO geregelten Datenschutz-Folgenabschätzung (DSFA) bewertend betrachtet. Die Ergebnisse stehen auf der Webseite des EIDI-Projekts und des ULD zur Verfügung.

Zuwendungsempfänger:	Unabhängiges Landeszentrum für Datenschutz (ULD)
Förderkennzeichen:	16KIS0697
Laufzeit des Teilvorhabens:	1. Januar 2017 bis 31. Dezember 2019
Informationen zum Gesamtprojekt:	https://itsec.cs.uni-bonn.de/eidi/
Informationen zum Teilprojekt:	https://www.datenschutzzentrum.de/projekte/eidi/