EINE ÖKONOMISCHE ANALYSE DER ANGEMESSENHEIT TECHNISCHER UND ORGANISATORISCHER MAßNAHMEN GEMÄß ARTIKEL 32 DSGVO

Fraunhofer SIT

Annika Selzer, Fraunhofer SIT | ATHENE

annika.selzer@sit.fraunhofer.de

Art. 32 DSGVO

[…]

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

[…]

Quantifizierung der Kosten der Gefährdung der Rechte und Freiheiten der betroffenen Personen: Schadensersatz

- Speziell für Verstöße gegen Art. 32 DSGVO wurde betroffenen Personen kein Schadensersatz zugesprochen.
- Ein Richtwert für Schadensersatzzahlungen im Allgemeinen kann anhand von Entscheidungen zu anderen Aspekten der DSGVO ermittelt werden.
- Im Durchschnitt mussten Organisationen für Verstöße gegen die DSGVO eine Entschädigung von 1.700€ zahlen. In den meisten Fällen wurde jedoch keine Entschädigung gewährt.
- Addiert man die durchschnittliche Entschädigung (1.700€) zu den durchschnittlichen Verfahrenskosten (1.600€), so ergibt sich eine durchschnittliche Gesamtentschädigung von 3.300€.

Quantifizierung der Kosten der Gefährdung der Rechte und Freiheiten der betroffenen Personen: Bußgelder

- Die durchschnittliche Bußgeldhöhe beträgt
  - 5.600€ (für kleine Unternehmen),
  - 77.000€ (für mittlere Unternehmen), und
  - 9.000.000€ (für große Unternehmen).
- Unter Berücksichtigung der Wahrscheinlichkeit eines Bußgeldes sollten Unternehmen
  - alle 5.000.000 Jahre (für kleine Unternehmen),
  - alle 100.000 Jahre (für mittlere Unternehmen), und
  - alle 1.200 Jahre (für große Unternehmen),

  mit einem Bußgeld rechnen.
- Unter Berücksichtigung der Wahrscheinlichkeit eines Bußgeldes ergibt sich ein zu erwartendes Bußgeld von
  - weniger als einem Cent (für kleine Unternehmen),
  - weniger als einem Euro (für mittlere Unternehmen) und
  - rund 7.500€ (für große Unternehmen).

Fazit

- Die DSGVO fordert angemessene technische und organisatorische Maßnahmen.
- Organisationen fühlen sich mit der hierfür notwendigen Abwägung zwischen dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen (1) und den Risiken für die Rechte und Freiheiten der betroffenen Personen (2) häufig überfordert.
- Unsere ökonomische Untersuchung ergab:
  - Höhe und Wahrscheinlichkeit von Bußgeldern und Schadensersatzzahlung vs. Implementierungskosten:
    - ➢ Übererfüllung der Organisationen.
  - Höhe und Wahrscheinlichkeit von Bußgeldern und Schadensersatzzahlung vs. Wahrscheinlichkeit eines Datenschutz- oder Datensicherheitsvorfalls:
    - ➢ Angemessene Abwägung der Organisationen.

Danke und Hinweise

Dr. Annika Selzer

Fraunhofer SIT/ATHENE

Dr. Daniel Woods

Universität Edinburgh

Prof. Dr. Rainer Böhme

Universität Innsbruck

Dieser Vortrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE sowie vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Projektes Edumida (16KIS1361K & 16KIS1363) unterstützt.