Datenpannen und der Datenschutz

Night of Openknowledge 2025

w1ntermute

Was bedeutet Databreach Juristisch?

Datenpanne bei Behörde durch versehentlich entsorgten Rollcontainer

Stand: 22.03.2024 21:27 Uhr

Bei der Ausländerbehörde in Hamburg gab es eine Datenschutzpanne. Sie entsorgte offenbar einen Rollcontainer, der noch zahlreiche behördliche Unterlagen enthielt. Neben Stempeln und CDs mit Daten befanden sich darin auch rund 150 Aufenthaltstitel - also Ausweise für Ausländer, die in Hamburg leben.

Was bedeutet Databreach Juristisch?

- Art. 33 DSGVO
- Bei jeglicher verletzung des schutzes Personenbezoger Daten
- Das müssen keine technischen Fehler sein. Z.b. falsch versand von Briefen
- Jede verletzung muss innerhalb 72h an die zuständige Datenschutzbehörde gemeldet werden

Was muss gemeldet werden?

- Im Gesetz sind unter Art.33 Abs. 3 aufgelistet, welche Daten mindestens gefordert werden
- Jede Behörde kann darüber hinaus noch weitere Daten anfordern.

Was muss gemeldet werden?

Mindestens wird gefragt

- Wie viele sind betroffen?
- Welche Daten sind betroffen?
- Kontaktdaten
- Welche Folgen lassen sich ableiten?
- Welche Maßnahmen wurden ergriffen?
- Wurden die Betroffenen benachrichtigt nach Art. 34?

Was kann folgen?

- Bei nichteinhaltung der Fristen
- Bei nichteinhaltung der Benachrichtigung
- Dann kann ein Bußgeld möglich sein.

Warum gibt es dann so selten Bußgelder?

- BDSG §43 Abs. 4
- Verbietet ein Bußgeld bei Art. 33 meldungen.
- Deswegen gibt es in Deutschland keine Bußgelder bei Meldungen solange diese Art. 33,34 einhalten

- Der einzige Streitpunkt ist Art. 34
- Wurden alle benachrichtigt?
- Reicht die benachrichtigung?
- Ist diese auffindbar?
- Ist es ein hohes Risiko für die Betroffenen?

Sorry wir wurden gehackt. Nächstes mal passiert es hoffentlich nicht.

Die Benachrichtigung

- Welche Informationen wurden falsch bearbeitet?
- Wie kann ich mich schützen?
- Wurde ich rechtzeitig gewarnt?
- An wen kann ich mich wenden bei Fragen über den Fall?

Die Rolle der Ethical Hacker

- Wenn man eine Lücke melden möchte?
- Die Firma reagiert nicht
- Oder ihr merkt, die Firma macht keine korrekte Benachrichtigung
- Gerne auch an die Landesdatenschutzbehörden. Das erhöht den Druck.

Das brauchen Behörden von Ethical Hackern

- Wann wurde die Firma kontaktiert?
- Sind personenbezogene Daten betroffen?
- Wie wurde die Firma kontaktiert?
- Wie kann die Lücke nachgestellt werden?
- Setzt bei der Kommunikation die Firma in CC.

Was wir nicht gebrauchen können.

Hallo, Wir haben gerade eine kritische Schwachstelle in Ihrem System entdeckt, die es Angreifern ermöglicht, vertrauliche Daten abzugreifen. Da wir Ihnen helfen wollen, das Problem schnell zu beheben, benötigen wir Ihre Unterstützung. Bitte überweisen Sie uns sofort 500 USD per PayPal, damit wir das Exploit-Patch für Sie bereitstellen können. Sobald die Zahlung eingegangen ist, senden wir Ihnen die vollständigen Details und das Gegenmittel. PayPal-Link: [paypal.me/secure-fix-12345] Vielen Dank für Ihr schnelles Handeln! Beste Grüße, Der Sicherheitsexperte

— Random Sec

Behörden haben auch die Ransomwaregangs im Blick

- Beziehen Daten aus z.B. ransomware.live
- Aus den Nachrichten
- Nach Hinweisen und auch eigene untersuchung

Was kann ich tun wenn ich betroffen bin?

- Verbraucherschutz hat eine gute Anleitung
- Vergleicht die Information die Ihr bekommen habt.
- Solltet Ihr ummstimmigkeiten sehen. Beschwerde bei der Aufsichtsbheörde.
- Versucht immer das was beim Databreach dabei war zu sperren.

Die häufigsten Databreach

- Im moment werden alle Firmen durch Phishing gehackt
- Ransomware ist auf Platz zwei
- Aufwendige Hacks sind die außnahme
- Klassischer IDOR wird am meisten gemeldet als Hinweis

Das Problem

- Der große anteil an Phishing
- Art. 34 bringt den Betroffenen wenig
- Es werden nicht weniger Datenpannen sondern nur mehr.
- Die EU möchte wegen LLMs Datenschutz eh abschaffen