Grundlagen der Informationssicherheit/Datensicherheit, Blatt 0

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

24. Oktober 2017

Problem 1

- Datenbank der türkischen Staatsbürger:
  `https://www.databreaches.net/turkish-citizenship-database-leak/`
  Hierbei wurden Daten von 49,611,709 Bürgern aus der Türkei, die 2008 wählen waren, nicht sicher verschlüsselt. Die Daten stammen aus der zentralen Einwohnermelde-Datenbank. Es wurde nur ein Bitshift angewendet, der aber nahezu keiner Verschlüsselung entspricht. Mittels der Daten ist es sehr einfach Identitätsdiebstahl zu begehen.

- Dropbox:
  `https://blogs.dropbox.com/dropbox/2016/08/resetting-passwords-to-keep-your-files-safe/`
  Hierbei wurden 68,680,741 Account-Infos veröffentlicht. Diese beinhalten Login-Namen und die Passwort-Hashes(sha256+salt). Die Daten stammen aus dem Jahr 2012, der Hack wurde aber er 2016 entdeckt. Da User häufig das gleiche Passwort für alle Services nutzen, ist die Wahrscheinlichkeit hoch, dass man sich auf anderen Webseiten damit einloggen kann. Dazu muss man aber erstmal noch die Passwörter entschlüsseln. Es ist nicht veröffentlicht worden, wie die Daten gestohlen werden konnten.

- Thumblr:
  `https://thehackernews.com/2016/05/tumblr-data-breach.html`
  Hierbei wurden 65,469,298 Account-Infos von Thumblr gehacked(Thumblr hat mehr Nutzer). Dies beinhaltet Email-Adressen und Passwort-Hashes (hash+salt). Die Daten sind allerdings nicht hoch aktuell, da sie aus der Zeit vor der Übernahme von Yahoo stammen. Es ist nicht veröffentlicht worden, wie die Datengestohlen wurden. Es ist aber sehr gut möglich, dass diese von einem Insider kommen.

Problem 2

Password-Manager:

- Confidentiality:
  Niemand sollte es möglich sein, meine Passwörter auslesen zu können, da sonst der Sinn von Passwörter nicht mehr vorhanden ist. Daher sollten Passwörter in einem Passwortmanager immer verschlüsselt sein.

- Integrity:
  Die Passwörter sollten ohne das Nutzer etwas verändert, selbst auch nicht verändert werden können, da man sonst sich möglicherweise ausschließt. Und somit nicht mehr den Service nutzen kann, für den die Passwörter sind.

- Availability:
  Die Passwörter sollten immer verfügbar sein. Falls man keinen Online-Zugang hat, sollte es trozdem möglich sein, die Passwörter angezeigt zu bekommen.

- Authentication:
  Es sollte gewährleistet werden, dass nur authorisierte Personen Zugriff haben. Dies wird meistens durch einen Master-Key/Passwort sicher gestellt.

- Accountability:
  Wenn die Passwort-Datenbank online syncronisiert wird, sollte der Sync-Provider auf jeden Fall sehr seriös/professionell sein.