Informationspflicht für Behörden und Unternehmen bei Datenpannen

fukami @ DS07, 6. Mai 2007

Agenda

- Was sind “Datenpannen”?
- Probleme
- Beispiele aus der Vergangenheit
- DLDOS
- Derzeitige Situation
- Forderungen
- Offene Fragen

Was sind “Datenpannen”?

- Servereinbrüche, Einbrüche in Netzwerke, Infektionen mit Malware
- gestohlene Laptops oder Smart Devices
- versehentlich veröffentlichte Daten auf Web- oder FTP-Servern, in Mails usw.
- Ausdrucke, die im Müll landen
- *(Merger, bei denen immer grössere Datensammlungen entstehen)*

Die Probleme (I)

- Alle möglichen Entitäten sammeln alle Arten persönlicher Daten (CC#, Email- und Wohnadressen, Telefonnummern, Verbindungsdaten, IP-Adressen, Positioning Data, Gesundheitsdaten, sexuelle Vorlieben, Lebensläufe ...)
- Sicherheitsrelevante Vorkommnisse werden meist nicht publiziert, Betroffene oft nicht informiert
- Viele Unternehmen sehen in solchen Vorfällen vor allem einen PR-GAU

Die Probleme (2)

Aber: User eines gehackten Systems können leicht Opfer weiterer Angriffe werden (z.B. durch ein Passwort für verschiedene Dienste, Single Sign-On Systeme oder Phishing und Identitätsdiebstahl etc.)

Beispiele aus der Vergangenheit (I)

- T-Hack: Im Provisionierungssystem der Telekom (OBSOC) konnten über Jahre Daten manipuliert werden (Logins, Routing Informationen ...).
- Beim Einbruch in Server von Guidance Software werden 3800 Kundendaten gestohlen.
- Angreifer hatten bei T-Mobile in den USA Zugriff auf 16,3 Million Datensätze (Zugang, persönliche Daten, Positioning, SMS, ...).

Beispiele aus der Vergangenheit (2)

- Durch einen Einbruch bei CardSystems werden 263.000 CC# gestohlen. Durch falsche Informationspolitik kommt es zu hohen Schäden (mind. 40 Mio US$).
- Bei Hotmail werden durch ein XSS-Problem 71.000 Accounts ausgespäht. Das Ganze fällt erst nach einem Jahr auf.
- Servereinbruch beim CCC: Eine spanische Hackergruppe kann die Anmeldedaten des Camps 2003 kopieren.

DLDOS

Data Loss Database - Open

- Projekt von attrition.org
- Grundlage: Security Breach Information Act (Kalifornien) vom 1. Juli 2003
- Öffentliche Mailingliste, CSV zum Download
- DLDOS trackt vor allem Vorkommnisse in Nordamerika
- Mehr Infos: http://attrition.org/dataloss

Derzeitige Situation (I)

- Vorgänge werden vertuscht (und oft auch nicht zur Anzeige gebracht)
- Es gibt in Deutschland (und Europa) unzureichende oder keine gesetzliche Regelungen, die Firmen oder Behörden zwingen, sicherheitsrelevante Probleme öffentlich zu machen
- In .de Fachausschuss eingerichtet
- Es gibt keine Behörde analog GSA in den USA (U.S. General Service Administration)

Derzeitige Situation (2)

- Behörden und Unternehmen sind oder werden hochgradig miteinander vernetzt - gleichzeitig wird Wissen um Schutz von Netzwerken und Rechnern kriminalisiert (Stichwort: Verbot von Hackertools).

Forderungen

- Verpflichtung zur Veröffentlichung von Vorkommnissen, bei denen der Diebstahl persönlicher Daten nicht ausgeschlossen werden kann. Die Art der kompromitierten Daten soll dabei angegeben werden.
- Verpflichtung zur Benachrichtigung der Betroffenen.
- Strafen für die Nicht-Benachrichtigung vorsehen.

Offene Fragen

- Welche Art Unternehmen sollten verpflichtet werden? Bei welchen Vorkommnissen? Wie ist es mit privaten Vereinen usw.?
- Wie soll die die Übermittlung der Daten aussehen, wie deren Publikation?
- Wie soll man Informationen von “Whistleblowern” behandeln? Wie verhindert man üble Nachrede?
- Wie soll man die tatsächlichen Probleme und das Datenleck von aussen richtig einschätzen?

Die Diskussion

- Mailingliste: dataloss@koeln.ccc.de
- https://mail.koeln.ccc.de/cgi-bin/mailman/listinfo/dataloss

Links

- Mailingliste des Dataloss-Projekt des C4
  https://mail.koeln.ccc.de/cgi-bin/mailman/listinfo/dataloss
- DLDOS
  http://attrition.org/dataloss
- Security Breach Information Act
  http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/
  sb_1386_bill_20020926_chaptered.html
- Stenografischer Bericht der 54. Sitzung des Deutscher Bundestags
  http://dip.bundestag.de/btp/16/16054.pdf
- T-Hack
  http://www.ccc.de/t-hack/
- Diebstahl der Daten vom Camp 2003
  http://ccc.de/updates/2004/camp-server-hack
- Einbruch bei Guidance Software
  http://www.heise.de/newsticker/meldung/67568
- Chaos Computer Club: Gesetzentwurf gefährdet die Computersicherheit
  http://www.ccc.de/press/releases/2006/20060925/