

Datenschutz im Unternehmen

oder: wie Sie es vermeiden, einen Big Brother Award zu gewinnen

Christian Mock

<cm@quintessenz.org>

5. 12. 2006, MQ Wien

Über die Big Brother Awards

- “You name them, we shame them”
- Negativpreis für Datenschutzverletzungen und sonstige Schnüffeleien
- In Österreich seit 1999, jeweils am 25. Oktober
- Weltweit in 13 Ländern

Die Veranstalter

- q/uintessenz, Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter
- VIBE!AT, Verein für Internet-Benutzer Österreichs
- LUGA, Linux User Group Austria

Wieso eigentlich?

- Öffentlichkeitsarbeit
- Bewußtsein für die Problematik schaffen
 - inzwischen ausführliches Medienecho
- Die Preisträger zum umdenken motivieren
 - ist in einigen Fällen schon gelungen
 - in vielen Fällen zumindest eine Reaktion oder Pressemeldung

Beispiel 1: EDV HAK Grazbachgasse (2006)

- Einführung der “educard” (Smartcard mit RFID)
 - Login
 - Zutrittskontrolle
 - Bezahlung am Buffet
- Personenbezogene Daten:
 - wer/wann/wo
 - was gekauft am Buffet
 - wann von zuhause online

Der ganz normale Wahnsinn

- Keinerlei Problembewußtsein
 - kein Eingehen auf mögliche Probleme in den Jubel-Aussendungen
 - kein Verständnis für Problematik in Reaktionen von Direktor und Schulsprecher
- Technologie “aufs Auge drücken”
 - Stellungnahmen von Schülern: die angeblich breit diskutierte Einführung der educard wurde in Wirklichkeit einfach ohne Info und Diskussion durchgezogen

Solution in search of a problem

- Existieren die angeblich gelösten Probleme überhaupt?
- z.B. Login: sicherer als User/Paßwort
 - aber: hat es damit überhaupt Probleme gegeben?
 - wenn ja: ist Smartcard die richtige Lösung?
- z.B. Zutrittskontrolle
 - zentral steuerbare und nachvollziehbare Zutritte – nötig?

Technologie verstanden?

- www.microsoft.at:

Durch die enge Integration des .NET-Frameworks mit dem Betriebssystem benötigt man als Entwickler genau eine Zeile Code, um die Smartcard-Authentifizierung für seine eigenen Anwendungen zu benutzen

- Ob die Entwickler dann wissen, welche Daten wo gespeichert werden?

Mißbrauchspotential

- Der Glaube an die technische Sicherheit
 - wenn mir die Card gestohlen wurde, glaubt mir das wer?
- Zentrale Datensammlung
 - Zutritt
 - Login im Haus und extern
 - Bezahlung: “du nascht zuviel”
- Gewöhnung an Hochsicherheitstrakt-Feeling in einer Schule!

Beispiel 2: die Post (2003)

- Nachsendeauftrag:

Ich erteile meine Zustimmung, dass die Österreichische Post AG die oben angeführten Daten an die Postadress Austria GmbH bzw. andere zur Ausübung des Gewerbes der Adressverlage und Direktwerbeunternehmen berechtigten Unternehmen weitergibt.

- Auftrag wird sonst nicht akzeptiert
- Verschiedene Versionen des Formulars im Umlauf

Der Kunde ist Sklave

- Um eine jahrzehntealte Dienstleistung zu benutzen, muß auf einmal Werbung in Kauf genommen werden?
- Oder sind die Mitarbeiter nicht darüber informiert, daß man die Zustimmung verweigern kann?
- Kennt sich in der Organisation überhaupt jemand aus?
- Der Kunde kommt sich gepflanzt vor...

Beispiel 3: “3”/Hutchinson und der FriendFinder (2004)

- Lokalisieren von “Freunden” über Handy + GPS
- muß am Handy des zu Lokalisierenden **einmalig** bestätigt werden

Der Mißbrauch ist einkalkuliert

- Aus einer “3”-Presseausendung:
*3FriendFinder ist auch als virtueller
"Babysitter" einsetzbar – die Eltern
wissen jederzeit, wo sich ihre Sprösslinge
gerade befinden.*
- Oder: Handy kaufen, FriendFinder
aktivieren, dem Ehepartner im Auto
verstecken und selbst Detektiv spielen

Und wo sind die Daten sonst noch überall?

- Hutchinson muß die Location des gefundenen ja auch kennen
- Wo und wie lange wird das gespeichert?
- An wen und unter welchen Umständen wird's weitergegeben?
- Könnte vielleicht gar ein Mitarbeiter sich ein Zubrot verdienen?

Beispiel 4: EU-Kommission, IP Enforcement Direktive (2003)

- vulgo: Ihre Daten an die Musik- und Filmindustrie...
- Provider speichern oft trotz Flat-Rate die IP-Adressen der User
- Datenschutzkommission: Adressen sollen nicht gespeichert werden
- OGH: Daten müssen herausgegeben werden (wenn vorhanden)
- Fazit: Datensparsamkeit!

Beispiel 5: “Gratis”-Dienste / Outsourcing

- Ist (z.b.) Google Analytics ein Wohltäter der Menschheit?
- Kann Userverhalten über viele Websites hinweg korrelieren
- Daten liegen in den USA (oder wo auch immer – Google China?)
 - Welches DS-Recht gilt? Behördenzugriffe?
- Enduser bekommt oft nichts mit davon

Datenvermeidung ist Datenschutz

- Daten, die nicht anfallen oder gespeichert werden, brauchen nicht geschützt werden
- Positiver Eindruck beim mündigen Kunden
 - Werben Sie damit!
- Fallen einem selber nicht in den Rücken
 - USA: diverse Prozesse mit Herausgabe von Emails und anderen Daten als Beweismittel gegen den “Eigentümer”

Was ist eigentlich das Problem?

- Oft technische Lösungen für organisatorische/menschliche Probleme
 - Lassen sich auf der richtigen Ebene besser (in jeder Hinsicht) lösen
- z.B. Paßwort-Probleme, Smartcard als Lösung?
 - auch Smartcard kann an Kollegen weitergegeben werden
 - oder am Schreibtisch liegengelassen
 - und mit PIN “1234” versehen

Technologien verstehen Folgen abschätzen

- Verstehen Sie, was Sie verwenden!
- Spielen Sie Szenarien durch, die passieren könnten
 - Mitarbeiter
 - Mitbewerber
 - Cracker
 - Kunden

Aber wenn der Kunde will...

- z.B.: “Kopie aller Mails von/an X auch an Geschäftsführung”
- Versuch, dem Kunden das auszureden, keine Chance
- Schlußendlich implementiert
- Hinweise in Vertrag, README, Konfigurationsdatei, daß es nur gesetzeskonform genutzt werden darf

Danke!

und verdienen Sie sich keinen Big Brother
Award :-)

www.bigbrotherawards.at