

IT - Security Forum #3

Schutz der Privatsphäre aus Benutzersicht

Dr. Marc Rennhard
Dipl. El.-Ing. ETH, CISSP
Zürcher Hochschule Winterthur
Marc.Rennhard@zhwin.ch






IT - Security Forum #3

Ziel / Überblick

- Ziele
 - Antworten auf folgende Fragen:
 - Wie können Sie als Internetbenutzer Ihre **Privatsphäre besser schützen?**
 - Welche **Methoden/Technologien** gibt es dazu, die über Datenverschlüsselung hinausgehen?
 - Sensibilisierung
- Überblick
 - Schutz der Privatsphäre heute... und die Limitierungen
 - Platform for Privacy Preferences Project (P3P)
 - Techniken zur Anonymisierung
 - Zusammenfassung

2

ZHAW Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT IT-SECURITY HOSTING

ca Computer Associates®

SECLUTIONS

IT - Security Forum #3

Schutz der Privatsphäre Heute

Gesetzliche Vorschriften

Privacy Policies

↓

- Bestimmt, welche Information ein Unternehmen sammelt und was es damit macht, zum Beispiel
 - Verwendung der Kundendaten für personalisierte Angebote im e-Commerce
 - Weitergabe der Kundendaten an andere Unternehmen

Technologische Mittel

Datenverschlüsselung

↓

- Gewährt die Geheimhaltung der Daten auf dem Übertragungspfad, zum Beispiel
 - Zum Schutz der Kundendaten im e-Commerce (SSL/TLS)

3

ZHAW Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT IT-SECURITY HOSTING

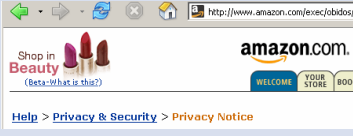
ca Computer Associates®

SECLUTIONS


IT - Security Forum #3

Limitierungen

- **Kaum jemand liest Privacy Policies:** sie sind mühsam zu lesen, schwierig, zu verstehen, können jederzeit ändern



Platform for Privacy Preferences Project (P3P)
- **Keine Anonymität:** jeder, der ein IP-Paket einer Kommunikationsbeziehung beobachtet, weiss, wer mit wem spricht



Techniken zur Anonymisierung

4

P3P – Was ist das?

- Ein World Wide Web Consortium (W3C) Standard
 - P3P 1.0 Spezifikation: 16. April 2002
- Idee: benutzerfreundlicher, automatisiert, mehr Transparenz
 - Der Benutzer spezifiziert seine **Privacy Preferences**
 - Websites spezifizieren ihre **Privacy Policies**
 - Der Webbrowser lädt die Policy **jedesmal** zusammen mit dem Inhalt der Website herunter und **vergleicht** diese Policy mit den Privacy Preferences des Benutzers
 - Sind die Preferences restriktiver als die Policy, so wird dies vom Webbrowser **optisch/akustisch mitgeteilt**
 - Automatisierung: P3P spezifiziert einen standardisierten Satz von **Attributen**, Speicherung im **XML-Format**

5

P3P – Browser Support

- Aktuelle Browser:
 - Zukünftige Versionen mit vollem Support
- Es gibt frei verfügbare Browser-Plugins von Dritten
 - Am bekanntesten: **AT&T Privacy Bird**
 - Plugin für Internet Explorer
 - Erlaubt einfaches Setzen der Benutzer-Preferences
 - Liest die P3P-Policies, Vergleich mit den Preferences
 - Zeigt mit einem Bird-Icon an, ob die Policy den Preferences entspricht



6

IT - Security Forum #3

Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT
IT-SECURITY HOSTING

Computer Associates*

SECLUTIONS

P3P – Privacy Bird (1)

The screenshot shows the 'Privacy Preference Settings' dialog box. The 'FINANCIAL OR PURCHASE INFORMATION' section has a red circle around the checkbox 'For analysis, marketing, or to make decisions'. The 'PERSONALLY IDENTIFIED INFORMATION' section has a red circle around the checkbox 'To share with other companies (other than those helping the site provide services to you)'. An overlaid code window shows the following P3P policy snippet:

```

...
<p3p:POLICY>
  <p3p:STATEMENT>
    <p3p:RECIPIENT appel:connective="or">
      <p3p:unrelated required="always" />
      <p3p:same required="always" />
    </p3p:RECIPIENT>
    ...
  </p3p:STATEMENT>
  <p3p:DATA-GROUP>
    <p3p:DATA>
      <p3p:CATEGORIES appel:connective="or">
        <p3p:purchase />
        <p3p:financial />
      </p3p:CATEGORIES>
    </p3p:DATA>
  </p3p:DATA-GROUP>
</p3p:POLICY>
...

```

7

IT - Security Forum #3

Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT
IT-SECURITY HOSTING

Computer Associates*

SECLUTIONS

P3P – Privacy Bird (2)

The screenshot shows Microsoft Internet Explorer displaying the Microsoft Corporation website. A red circle highlights the privacy icon in the address bar. A 'Policy Summary' dialog box is open, showing the following information:

Microsoft Corporation Privacy Practices

Privacy Policy Check

- Microsoft Corporation's privacy policy *does not match your preferences:*

- Site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
- Site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Privacy Policy Summary

- + Policy Statement
- Access to your information

8

z:W Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT
IT-SECURITY HOSTING

ca
Computer Associates®

SECLUTIONS

IT - Security Forum #3

P3P – Privacy Bird (3)

p3policy.xml von Microsoft.com:

```

...
<STATEMENT>
...
  <RECIPIENT>
    <same />
    <ours />
  </RECIPIENT>
</DATA-GROUP>
...


```

(cont'd)

```

...
  ...
  <CATEGORIES>
    <purchase />
  </CATEGORIES>
  ...
</DATA-GROUP>
</STATEMENT>
...

```



Auszug aus der Privacy Policy von Microsoft.com:

We may use your personal information to provide you with important information about the product or service that you are using, including critical updates and notifications. Additionally, with your permission, we may send you information about other Microsoft products and services, and/or share information with Microsoft partners so they may send you information about their products and services.

9

z:W Zürcher Hochschule Winterthur
Department Technik, Informatik und Naturwissenschaften

GO OUT
IT-SECURITY HOSTING

ca
Computer Associates®

SECLUTIONS

IT - Security Forum #3

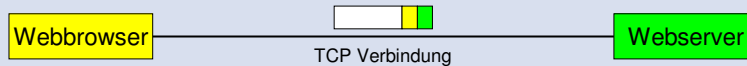
P3P – Quo vadis?

- Aktueller Stand:
 - Mai 2004: **33% der Top 100** Domains und **24% der Top 500** Domains haben eine P3P Policy, stetig zunehmend
 - Full P3P Support in IE/Netscape/Mozilla „wahrscheinlich“
- Ausblick/Potential
 - Studien zeigen: P3P Policies bringen einem Unternehmen einen **Mehrwert**; Benutzer bewerten P3P-enabled Browser **positiv**
 - Wird sich „vermutlich durchsetzen“
- Tipp für Sie als Benutzer:
 - Installieren, verwenden und beachten Sie den Privacy Bird (<http://privacybird.com>)

10

Anonymität – Überblick

- Auch mit P3P und Verschlüsselung bietet das Internet **keine Anonymität**
 - Jedes IP Paket enthält die IP-Adressen beider Kommunikationsendpunkte



- Jeder auf dem Übertragungspfad weiss, wer mit wem kommuniziert (lokaler SysAdmin, ISP, Server, Eavesdropper)
- Die Feststellung der Identität aus der IP-Adresse ist meistens möglich (Trend zu statischen Adressen, Access-ISP kennt Mapping zwischen Benutzern und dynamischer Adresse...)

11

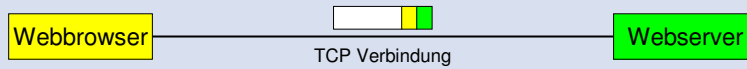
Anonymität – Brauchen wir das?

- Ich hätte **gern Anonymität** beim:
 - Zugriff auf eine Seite mit medizinischer Information
 - Zugriff auf eine Online-Job-Börse vom Arbeitsplatz aus
 - Durchstöbern eines e-Shops
 - Gebrauch von Search Engines (überlegen Sie sich, was Google über Sie weiss...)
- *Datenverschlüsselung nützt meist nichts*
- *Im „richtigen Leben“ sind vergleichbare Aktivitäten anonym*

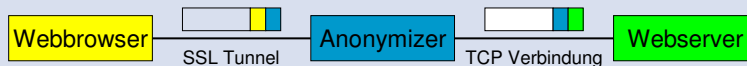
12

Anonymität – Techniken

- Problem: Direkte Client-Server Kommunikation



- Abhilfe: Proxy zwischen Client und Server
 - Bekanntestes Beispiel: The Anonymizer



- Details zum Anonymizer (<http://www.anonymizer.com>):
 - Seit 1996, 30\$/Jahr, eine Million Benutzer
 - Gute Performance (kleine Einbusse)
 - Aber: Der Anonymizer „weiss alles“ ☐ der Benutzer muss ihm vertrauen!
 - Forschungsprojekte mit mehreren Zwischenknoten



13

Zusammenfassung

- Limitierungen heute:
 - Privacy Policies sind mühsam zu lesen, schwierig, zu verstehen, können jederzeit ändern ☐ sie werden ignoriert
 - Keine Anonymität: Jeder entlang des Übertragungspfades weiss, mit wem ich kommuniziere
- Besserer Schutz der Privatsphäre ist möglich:
 - P3P erlaubt den automatischen Vergleich der eigenen Privacy-Preferences mit der Policy einer Website
 - Anonymisierungstechniken geben dem Benutzer die Wahl, wann er anonym sein will und wann nicht
- Probieren Sie diese Techniken selbst aus!

14