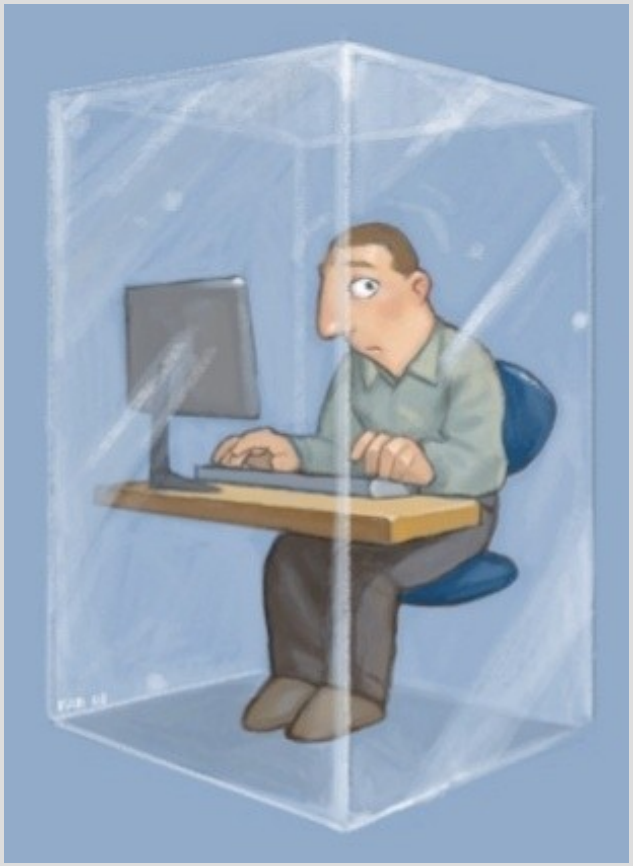
Wie funktioniert das WWW?



Sicher im WWW

Der normale Aufruf

1. Browserprogramm starten
2. Adresse eintippen, z.B. :
   ich-hab-doch-nichts-zu-verbergen.de
3. Der Browser ändert die Adresse auf:
   http://ich-hab-doch-nichts-zu-verbergen.de/
4. Der Browser fragt nach der IP des Servers
5. Der Browser fragt bei der IP nach der gewünschten Webseite
6. Das Serverprogramm liest die Seite von der Festplatte, schickt sie und trennt die Verbindung

Was kann schief gehen?

1. Tippfehler aller Art
2. Der DNS-Server antwortet nicht
3. Der DNS-Server liefert gefälschte Antworten
4. Der Server liefert die falschen Seiten aus
5. Die Datenpakete werden auf dem Transport verändert oder gelöscht
6. Programmfehler auf beiden Seiten – die Webseite kommt nicht ganz, oder der Browser schafft es nicht sie anzuzeigen

•

•

Was speichert der Server?

1. Den Namen des Clients laut DNS
2. Die IP Adresse des Clients
3. Die angefragte URL
4. Informationen über den Browser
5. Die Webseite, von der aus der Besucher kommt (Referrer)
6. Eingaben in Formularen etc.

•

•

Was speichert der Client?

1. Alle eingetippten Adressen (URL)
2. Die angeschauten Webseiten komplett
3. Formulardaten
4. Alle Daten, die von der Webseite nachgeladen werden
5. Textdateien, um den Client zu identifizieren (Cookies)

Was macht HTML dabei?

1. Webseiten sind in HTML geschrieben
2. HTML beschreibt das Aussehen der Seite
3. Bilder und andere Daten werden einzeln – mit eigener URL – heruntergeladen, die URL's der Bilder stehen in der Seite die man aufruft
4. Diese URL's können auf andere Server verweisen – auf einen Werbeanbieter z.B.
5. Über Javascript und ActiveX können Programme auf dem Client gestartet werden

Was davon ist problematisch?

1. In Suchmaschinen sind Suchanfragen in der eingetippten URL zu erkennen
2. Diese Anfragen werden mit gespeichert
3. Objekte können im Browser unsichtbar sein, werden aber dennoch geladen
4. Fremde Server verfolgen die Seitenaufrufe über die Anzeigen
5. Über Session-ID's oder Cookies verfolgt der Server die Verweildauer und Klick-Folge

Was davon ist problematisch?

7. Über Skripte können fremde Server Programme zur Ausführung bringen
8. Die Browseroberfläche kann von Webseiten geändert werden
9. Der Browser wird in anderen Programmen im Hintergrund aufgerufen (Email z.B.)
10. Das Browserprogramm hat ein Sicherheitsloch, über das eine Webseite einen Trojaner oder Virus einspielt
11. Die Website täuscht vor, eine andere zu sein – eine Bank z.B. (Phishing)

Abhilfe!

1. Browser so einstellen, das Skripte unterbunden oder geprüft werden
2. Browser auf dem neuesten Stand halten
3. Browser-Erweiterungen zum Schutz einsetzen (Plugins)
4. Keine verräterischen Adressen, Suchanfragen oder Formulardaten eingeben
5. Cookies und Zwischenspeicher (Cache) regelmäßig überprüfen und/oder löschen
6. Anonymisierungsdienste verwenden

Denken Sie dran...

Was immer Sie eingeben wird für alle Zeit weltweit lesbar gespeichert!

Abfangen von Daten (Phishing)

1. Tippfehler ausnutzen, ähnliche Namen sind oft böse Websites
2. DNS manipulieren
3. In Emails gefälschte Links unterjubeln
4. Zugangsdaten und persönliche Daten werden so per „Passwort fischen“ abgefangen
5. Abhilfe: Links überprüfen in der Statusleiste
6. Service von Google in Firefox 3 einschalten – aber: Google speichert alle aufgerufenen Webseiten?

Web 2.0 als Datenschutzalptraum

1. Websites binden Inhalte von anderen Websites nahtlos ein
2. Das wird über Programmierung gemacht
3. Man kann „böse“ Software schreiben
4. Auf harmlosen Seiten können so „böse“ Inhalte auftauchen
5. Bei Programmierfehler auf dem Server: sogenanntes Cross-Site-Scripting
6. Service von Google in Firefox 3 einschalten – aber: Google speichert alle aufgerufenen Webseiten?

Die Identität des Servers

1. Man verwendet dazu Verschlüsselungstechnik (X 509 Zertifikate)
2. Das Protokoll dafür ist https
3. Die Verbindung zwischen Webserver-Software und Browser ist abhörsicher
4. Das Zertifikat des Servers bestätigt dessen Identität
5. Einkäufe und Banking immer über https machen!
6. Zertifikate prüfen!

Https im Detail

1. Client fragt Server-IP nach Crypt-Methode
2. Server sendet Zertifikat
3. Ein Sitzungsschlüssel wird vereinbart
4. Die Webseitenanfrage wird verschickt (abhörsicher)
5. Die Seite kommt (abhörsicher)
6. Für jede IP gibt es nur 1 https-Server
7. Die Zertifikate müssen von einer „Authority“ unterschrieben werden, um die Identität zu beweisen

Https hacken

1. Sie können selber ein „Authority“ erstellen
2. Damit bestätigen Sie die Echtheit der https – Server
3. Vertrauen Sie dem Aussteller des Zertifikats?