DUM č. 18 v sadě

36. Inf-12 Počítačové sítě

Autor: Lukáš Rýdlo

Datum: 06.05.2014

Ročník: 3AV, 3AF

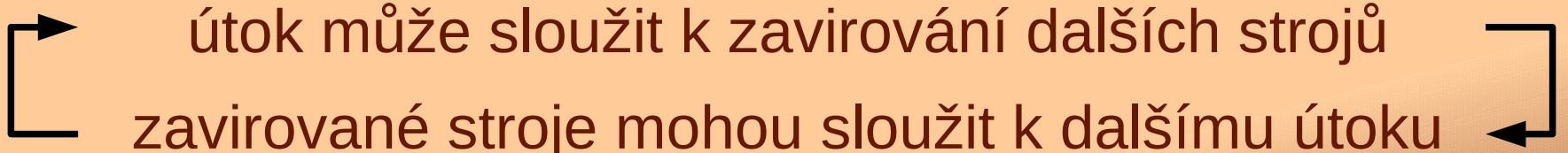
Anotace DUMu: bezpečnost v síti - typy útoků, DDoS, MiM, podvržení DNS, cross site scripting, clickjacking

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Počítačové sítě
Bezpečnost – útoky

Příklady útoků v počítačových sítích

- počítačové sítě jsou nebezpečné, nikdy nevíme, kdo nás může sledovat
- sítě nejsou zcela anonymní (uchovávají se data o navštívených stránkách a adresách)
- nelegální činnost lze anonymizovat pomocí zavirovaných počítačů



DDoS

- Distributed Denial of Service
  - rozložené blokování služby
- způsob jak vyřadit služby (web) jejich přetížením
- útočník používá velké množství různých (zavirovaných) počítačů (botnet) k opakovanému dotazování se serveru
- server tak velké množství dotazů nezvládá a „spadne“
- lze těžko rozlišit, kdo je útočník a kdo má opravdu o službu zájem
  - např. při slevové akci na e-shopu mohou „DDoS“ způsobit zákazníci
- je nutné hlídat, že náš počítač není zavirovaný, aby se nestal účastníkem DDoS

MiM

- Man in the Middle
  - útok podvržením prostředníka
- oblíbené např. při šifrované komunikaci
- stačí podvrhnout certifikát a uživatel zdánlivě zabezpečeně komunikuje ovšem se zcela jiným serverem, který ale dotazy přeposílá dál a odpovědi přeposílá zpět
- veškerá komunikace je odposlouchávána prostředníkem
- obrana:
  - používat vlastní techniku, neprovádět důležité činnosti v knihovně, kavárně apod.
  - nikdy neschvalovat neznámé certifikáty, nereagovat na phishing
  - hlídat si aktuální antivirový program, aktualizovat prohlížeč

Podvržené DNS

- jednoduchý způsob, jak získat citlivé údaje je vytvořit kopii cílové stránky a donutit uživatele domnívat se, že je na správné stránce
- „přesměrovat“ uživatele na podvrh lze podvržením falešné IP adresy
- počítač použije falešný DNS server, který vrací na požadované DNS adresy falešné IP adresy
- obrana:
  - používat vlastní, správně nastavené počítače
  - hlídat si, jaké DNS jsou použity v nastavení sítě

Clickjacking a skriptové útoky

- clickjacking je založený na provedení nějaké neočekávané akce po kliknutí
  - např. otevření nechtěných vyskakovacích oken, odeslání údajů na server apod.
- skriptové útoky se snaží pomocí skriptů (JavaScript na webu) provést nějakou škodlivou činnost
  - např. skript blokuje zavření okna, nechává neustále vyskakovat chybové hlášky apod.
- obrana:
  - vypnutí JavaScriptu, instalace doplňků jako adBlock, firebug a znalost JavaScriptu pro jeho obejití

Cross site scripting

- narušení webových stránek z jiné stránky
- je-li webová stránka špatně naprogramovaná, lze do ní např. vložit kód JavaScriptu, který pak odesílá data ze stránky (login, heslo, adresáty mailů…) útočníkovi
- obrana:
  - nemít na různé stránky stejná hesla
  - nepřihlašovat se na neprofesionálně vytvářené stránky

Sociální manipulace

Největší hrozbou je hloupý uživatel.

- velká část útoků je založená na neznalosti uživatelů
- příklady
  - ochota odkliknout přílohu, která se tváří jako obrázek, ale má koncovku „exe“ na Windows systémech
  - odklikávání odkazů s divnou adresou (místo DNS jen IP, zkomolenina adres, adresy v pochybných oblastech .ru nebo .cn apod.)
  - důvěřivost a nepozornost k divnému chování
  - ochota povolovat bezhlavě přístup k osobním údajům hrám neznámých autorů apod.

Útok „po domácku“ – příklad

- ukázka, jak ukrást hesla k facebooku
- na svůj počítač nainstaluju webserver (XAMPP) a umístím na něj kopii úvodní stránky Facebooku s cílem pro odeslání hesla na skript, který jej zobrazí (odešle mailem?)
- v souboru c:\windows\system32\drivers\etc\hosts (v Linuxu /etc/hosts) přidám záznam „127.0.0.1 www.facebook.com“
- díky tomu se po zadání adresy FB zobrazí stránka webserveru mého počítače
- stačilo se dostat k souboru hosts a mít někde webserver…

Zdroje

- http://cs.wikipedia.org/wiki/DDOS
- http://cs.wikipedia.org/wiki/Clickjacking
- http://www.krypta.cz/articles.php?ID=94
- http://cs.wikipedia.org/wiki/Cross-site_scripting