

2007 metų grėsmės

Pranešėjas: Audrius Lučiūnas

UAB „Informacijos saugos sprendimai“

www.isec.lt



Prezentacijos turinys

- Phishing ir XSS
- CSRF arba XSRF
- P2P Botnet'ai
- Windows Vista pažeidžiamumai
- Google pažeidžiamumai
- Naršyklių pažeidžiamumai
- Interneto naršyklių istorijos verslas
- Plačių galimybių tinklalapių pažeidžiamumai
- Web sistemų modifikacijos
- Kas dar?
- Saugumas Lietuvoje
- Ką daryti?

Phishing ir XSS (1 iš 2)

Wikipedia: Cross-site scripting (XSS) - IT sistemų pažeidžiamumas, dažniausiai aptinkamas tinklalapiuose, kuris leidžia įterpti papildomą programinį kodą į vartotojų peržiūrimą puslapį.

Esaugumas.lt: Duomenų vagystė „phishing“ - sukčiavimo forma prieš asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti konfidencialius duomenis.

- XSS - senai žinomas pažeidžiamumas, tačiau anksčiau retai buvo naudojamas rimtai dėl ribotų galimybių.
- XSS išnaudojimas stipriai patobulėjo 2006 metais.
- Dabar galima tikrinti vidinio tinklo struktūrą, fiksuoti vartotojo spaudžiamus mygtukus, nuskaityti interneto naršyklės lankytų tinklalapių istoriją ir t.t.
- Vartotojui atvertus tinklalapį, XSS pažeidžiamumo išnaudojimas gali būti vizualiai nematomas.

Phishing ir XSS (2 iš 2)

- XSS pažeidžiamumas nukreiptas prieš tinklalapio vartotoją.
- Apjungus su „phishing“ metodais, gali būti labai pavojinga ataka išvagiant duomenis iš vartotojo, nes vartotojui sunku ją atpažinti, kadangi nėra klastojamas visas tinklalapis. Interneto adresas, kaip ir visa sistema, išlieka originalus ir t.t.
- Norint išnaudoti šį pažeidžiamumą, reikia priversti vartotoją nuspausti atitinkamai suformuotą tinklalapio adresą.
- XSS gali būti atpažintas pagal ilgą ir neįprastai suformuotą tinklalapio adresą.
- XSS pažeidžiamumą turi didžioji dalis sudėtingesnių Lietuvos tinklalapių.

CSRF arba XSRF

Cross Site Request Forgery – XSS priešingybė, nukreipta ne prieš vartotoją, bet prieš jo naudojamą sistemą, kuri pasitiki vartotoju.

Išnaudojimo pavyzdys:

Antanas prisijungia prie elektroninės akcijų biržos (toliau – EAB). EAB sistema pasitiki Antanu kaip vartotoju, nes jis nurodė tinkamą prisijungimo vardą bei slaptažodį ir priima visus jo atliekamus veiksmus (užklausas). Antanas sėkmingai perka ir parduoda akcijas. Lygiai tą patį sėkmingai daro ir Antano kompiuteryje esanti kenksminga programa, siųsdama sistemai užklausas, kurios nukeliauja į ją, tarsi būtų siųstos Antano vardu. Antanas “prisiperka” netinkamų akcijų.

Tokiu būdu dirbtinai sukeliama akcijų paklausa ir jos pabrangsta. Pabrangimą sukėlę sukčiai išperduoda pabrangusias akcijas. Išaiškėjus apgavystei akcijų kaina labai greitai ir stipriai krinta, o Antanas EAB sistemos savininkams negali įrodyti, jog jas pirkto ne savo noru.

- Seniai žinomas pažeidžiamumas.
- Sunkiau aptinkamas nei XSS.
- Gali būti išnaudojama kartu su XSS ar kitais pažeidžiamumais.
- Manoma, kad šį pažeidžiamumą turi beveik 100% sudėtingesnių internetinių sistemų.
- 2007 m. prognozuojamas šio pažeidžiamumo išnaudojimo padidėjimas.

P2P Botnet'ai

Botnet – žalinga programine įranga valdomi kompiuteriai be tikrųjų savininkų sutikimo, kurie gali būti naudojami nelegaliai veiklai vykdyti, pvz. nepageidaujamų laiškų siuntimui.

- Iki šiol buvo įprasta, kad tokie užvaldyti kompiuteriai būtų valdomi iš centrinės vietos (pvz. IRC kanalo).
- Panaikinus centrinę valdymo vietą, botnet'as tapdavo neaktyvus.
- Pritaikius P2P programų (Kazza, Emule, BitTorrent) funkcionalumą, nebelieka centrinės valdymo vietos, dėl ko tokių užvaldytų kompiuterių tinklą daug sunkiau panaikinti.
- 2007 m. dar nebus P2P botnet'ų piko, bet tokių tinklų kiekis pradės didėti.

Windows Vista pažeidžiamumai

- Ypač didelis dėmesys naujai operacinei sistemai.
- Didelis susidomėjimas iš vartotojų – įdomu kas nauja ir taip reklamuota.
- Didelis susidomėjimas iš hakerių – garbė pirmam įveikti Microsoft apsaugą.
- Tinkamas laikas pasiruošti kitų metų atakoms (2008 Vista bus labiau išplitusi).

Google pažeidžiamumai

- Google - jau ne tik paieškos sistema.
- Google tampa “mikrosoftu” internete, todėl yra puikus taikinys dėl vis didėjančio naudotojų rato.
- Google paieškos sistemoje jau anksčiau buvo rasta pažeidžiamumų (daugiausiai XSS), tačiau kitos Google sistemos yra daug sudėtingesnės.
- Sudėtingos sistemos – didesnė klaidų tikimybė.
- Aptikus ir išnaudojus Google aplikacijos klaidą galima iš karto užvaldyti daug jos naudotojų sistemų.
- Nepageidaujamų laiškų platintojai jau spėjo sėkmingai pasinaudoti Google SMTP tarnybine stotimi spam plaitinimui.

Naršyklių pažeidžiamumai

- 2005 pasirodė pirmasis tinklalapių kirminas.
- 2005 ir 2006 buvo atrasta daugybė įvairių naršyklių pažeidžiamumų. Ypač daug kritikos sulaukė FireFox naršyklė, kuri iki tol buvo laikyta viena saugiausių.
- 2007 prognozuojamas ir tinklalapių, ir interneto naršyklių pažeidžiamumus išnaudojančių kirminų plitimas. Galim sulaukti Nimda kirmino analogo veikiančio web ir naršyklių terpėje.
- 2007 susidomėjimas naršyklių pažeidžiamumais išliks ir bus atrasta naujų jų trūkumų. Pažeidžiama naršyklė, tai galimybė lengvai pasiekti vartotojo kompiuterį apeinant standartines ir labiausiai paplitusias apsaugos priemones, pvz. ugniasienę.

Interneto naršyklių istorijos verslas

- Išnaudojant tinklalapių ar naršyklių klaidas galima surinkti informaciją kur dažniausiai žmonės naršė, kaip jie į tuos tinklalapius pateko, kokius puslapius atvertė ir t.t.
- Šią informaciją sudėtinga gauti legaliai, bet ji ypač įdomi marketingo specialistams ir “phishing” sukčiams.
- Turint tokią informaciją daug paprasčiau ką nors parduoti arba apgauti vartotoją, pvz., “phishing” sukčiai tokiu būdu gali identifikuoti kokius tinklalapius ir kokias jų dalis labiausiai verta padirbinėti norint išvogti naudotojų duomenis.

Plačių galimybių tinklalapių pažeidžiamumai

- Plačių galimybių interneto tinklalapiai (Rich Internet Applications) – tinklalapiai, kurie galimybėmis ir funkcionalumu prilygsta tradicinėms programoms. Tai dažniausiai tokie tinklalapiai, kurie atsinaujinant duomenims, keičiantis elementų išdėstymui ir pan. nereikalauja viso tinklalapio atnaujinimo naršyklėje.
- Didelis didžiųjų kompanijų dėmesys šiai technologijai, didėjanti konkurencija, naujos galimybės internete.
- Nors paplitimas nėra didelis, bet tai nauja ir pakankamai sparčiai plintanti technologija, todėl kyla ir įsilaužėlių dėmesys.
- Šiomet jau pasirodė AJAX sniferis, gebantis perimti keliaujančius duomenis tarp tinklalapio klientinės ir serverinės dalies.

Web sistemų modifikacijos

- Dažniausiai dėl klaidų web sistemose vagiama įvairi informacija, kreditinių kortelių duomenys, į serverį diegiamos kenksmingos programos, keičiama tinklalapių išvaizda ir t.t.
- Naujas klaidų išnaudojimas: internetinių sistemų modifikavimas išlaikant pradinį jų funkcionalumą.
- Naudojama vartotojų šnipinėjimui
- Siekiama detaliau išsiaiškinti kaip veikia sistema ir tai panaudoti kitais tikslais, pvz. finansinėms machinacijoms.
- Įprasta, kad tinklalapiai būtų gan dažnai modifikuojami, todėl tokias modifikacijas tampa pakankamai sudėtinga pastebėti ir sukontroliuoti.

Kas dar?

- Visi iki šiol naudoti pažeidžiamumai išliks ir bus aktyviai naudojami toliau.
- Kai kurie jų persikels į naują terpę, pvz., mobilius įrenginius.
- Kai kurie jų bus apjungti sukuriant naujo tipo atakas.
- Daugės manipuliavimo žmonių pasitikėjimu (socialinės inžinerijos) atveju.

Saugumas Lietuvoje

- Saugumo mitas: antivirusinė sistema + ugniasienė = vaistas nuo visų pažeidžiamumų.
- Vidiniai tinklai prastos architektūros – puiki terpė plisti virusams ir kitoms nekontroliuojamoms programoms.
- Koncentruojamasi tik į tinklo apsaugą iš išorės (internetu).
- Pažeidžiamumų turi virš 80% sudėtingesnių lietuviškų tinklalapių. Trūkumų pastebėta ir bankinėse sistemose.
- Įmonės neskiria lėšų darbuotojų švietimui saugumo tema, todėl puikiai veikia socialinės inžinerijos metodai ir manipuliuoti žmonėmis yra paprasta.
- Dažnai įmonės saugumas priklauso tik nuo IT ūkį prižiūrinčio žmogaus iniciatyvos ir jo žinių.
- Mažai kas suvokia saugumą įmonės procesuose.

Ką daryti?

- Pradėti kreipti dėmesį. 😊
- Naudoti papildomus trečiųjų šalių saugumo sprendimus (pvz. web ugniasienes).
- Mokymai įmonės darbuotojams IT saugumo tema.
- Kartais pravartu žingsniu atsilikti nuo naujausių technologijų.
- Reikalauti vietinių sistemų autorių atitikti tam tikrus saugumo reikalavimus.
- Kitos priemonės ir būdai (organizacinės).

Klausimai ?

UAB „Informacijos saugos sprendimai“

www.isec.lt

Audrius Lučiūnas

Mob. tel.: +370 615 20288

El. paštas: audrius@isec.lt