"Novejše" metode nepooblaščenega dostopa do vaših podatkov

MARKO SMID

Digitalno podpisal MARKO SMID
DN: cn=MARKO SMID, c=si, o=state-institutions, ou=sigen-ca, serialNumber=2462005216010
Razlog: Potrditev dokumenta
Lokacija: Astec d.o.o., Ljubljana
Datum: 2009.10.30 09:33:35 +01'00'

E-Poslovanje

VARNOST IN ZASEBNOST NA INTERNETU (in v LAN-u)

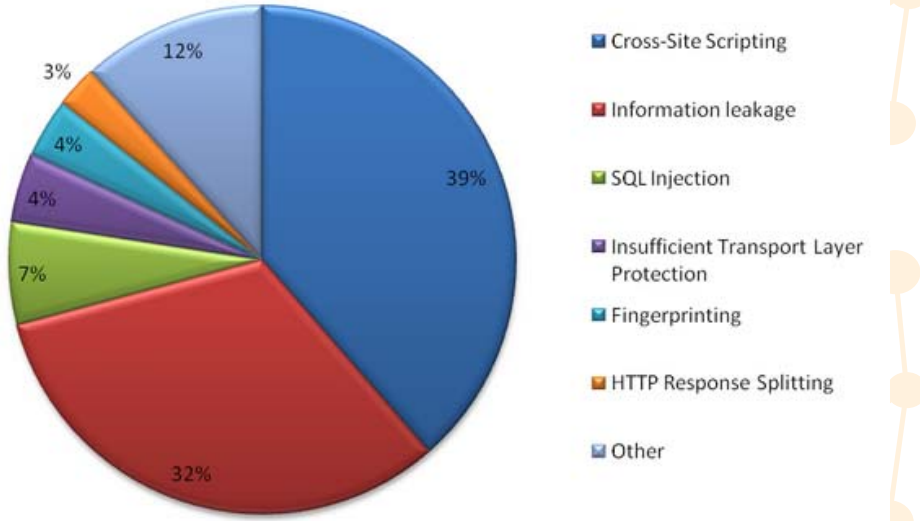
Marko Šmid

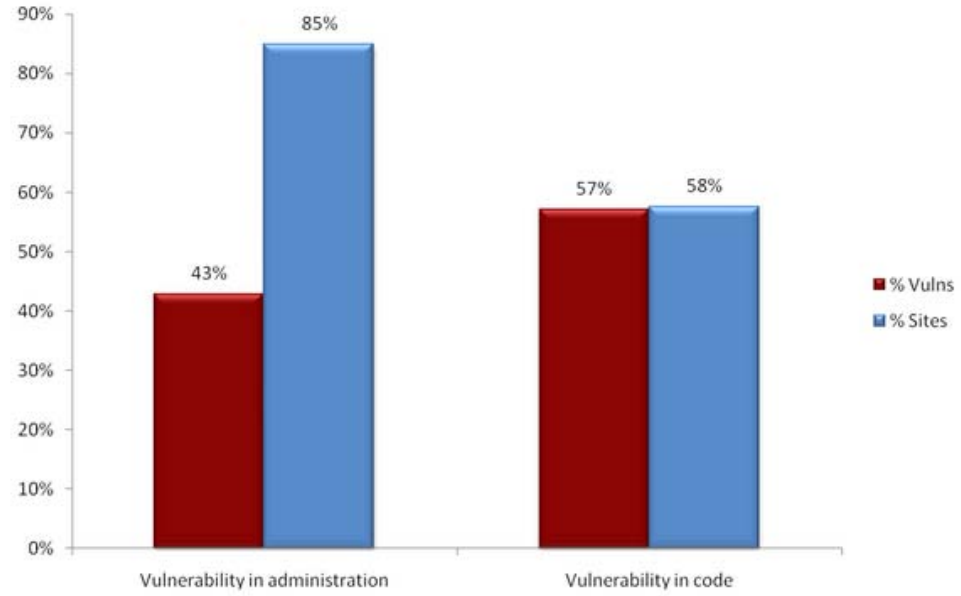
Kaj želi povedati predstavitev?

- Varnost se ne začne in konča pri požarnih pregradah
- Varnost je celovit proces, ki ga je potrebno stalno vzdrževati
- Izkušnje, ki smo si jih pridobili pr izvajanju varnostnih pregledov kažejo, da večina še vedno ne verjame, da se nepooblaščen dostop do podatkov, njim lahko zgodi
- Beseda "Varnost" ni le propaganda prodaje

12186 spletnih aplikacij s 97554 zaznanimi ranljivostmi

- http://projects.webappsec.org/Web-Application-Security-Statistics





Zakaj prihaja do nepooblaščenega dostopa?

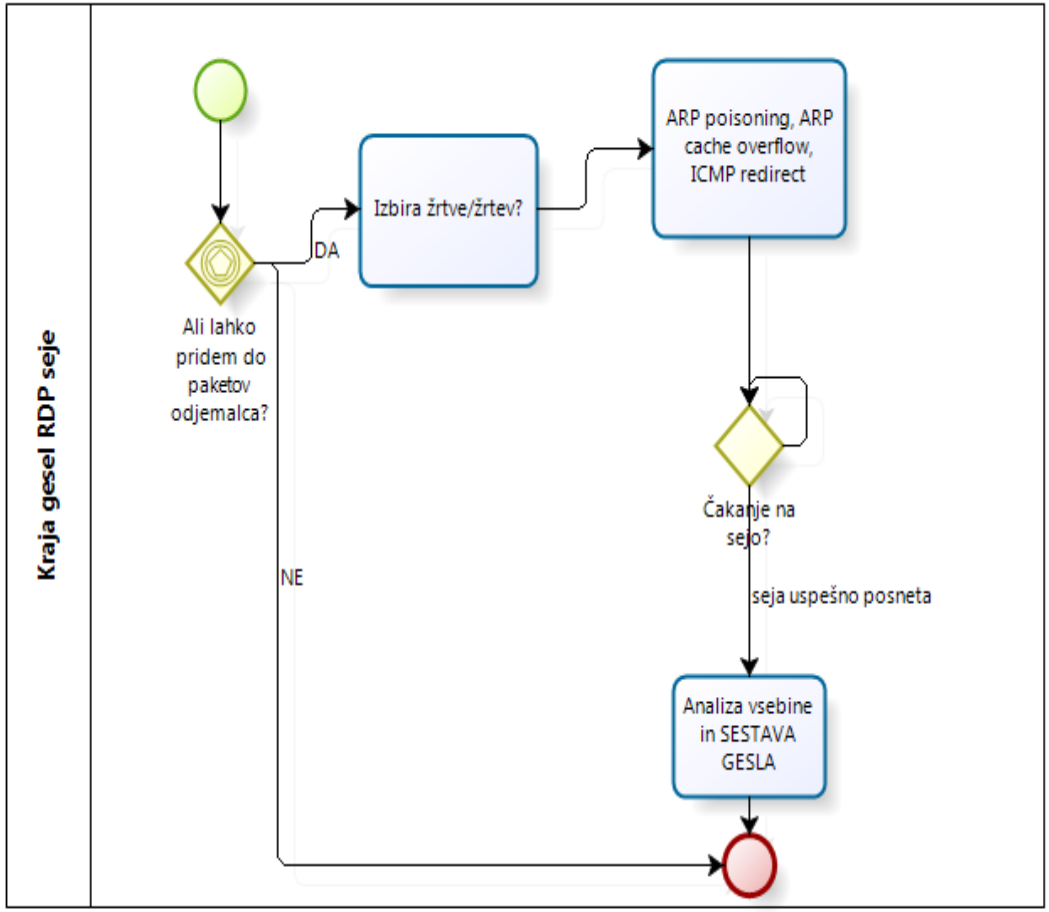
- Najbolj pogosti vzroki
  - Nespoštovanje osnovnih priporočil
    - delo pod administratorskimi pravicami;
    - gesla, gesla...;
    - možnost fizičnega dostopa do računalnika;
    - neizvajanje nadgradenj programske opreme;
  - Napake programske kode proizvajalca
  - Napake razvoja aplikacij
    - Predvsem spletne aplikacije
  - Nezadostna varnostna infrastruktura, oziroma postavitev infrastrukture z neizdelanimi cilji in načrti
    - Skrbništvo storitev: upravljanje in zagotavljanje delovanja
  - .....

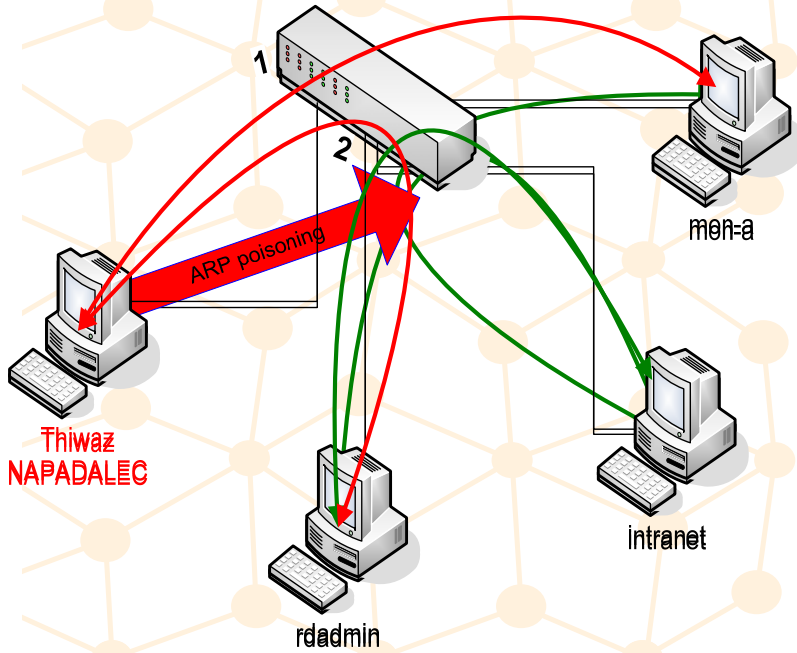
astec

Kaj sledi?

- Praktična predstavitev
  - Kraja gesla vzpostavitve RDP seje?
  - Kraja seje spletne aplikacije?
- Opis novejših metod dostopa do podatkov
  - Bootkit, SandMan
  - NULL-prefix SSL attack
- Kako ukrepati?

Prikaz varnosti gesel RDP seje



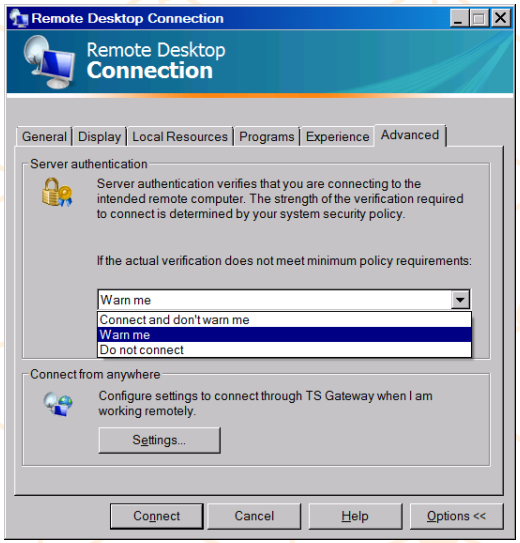


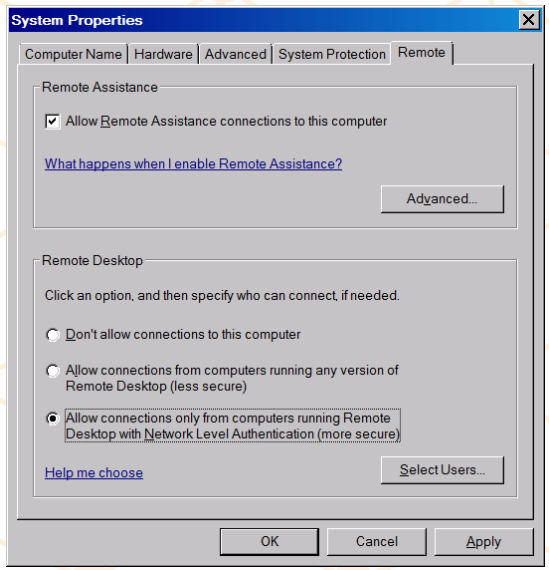
powered by BizAgi Process Modeler

astec

Kako preprečiti krajo RDP seje?

- Uporaba dodatnih ali prenovljenih varnejših protokolov
  - Uporaba varnih rdesktop odjemalcev (61, 7.0)
  - Višja verzija RDP procesa na strežniku (RDP >=6.X), ki onemogoča hibo neidentifikacije obeh strani v procesu izmenjave šifrirnega ključa seje. (NLA)

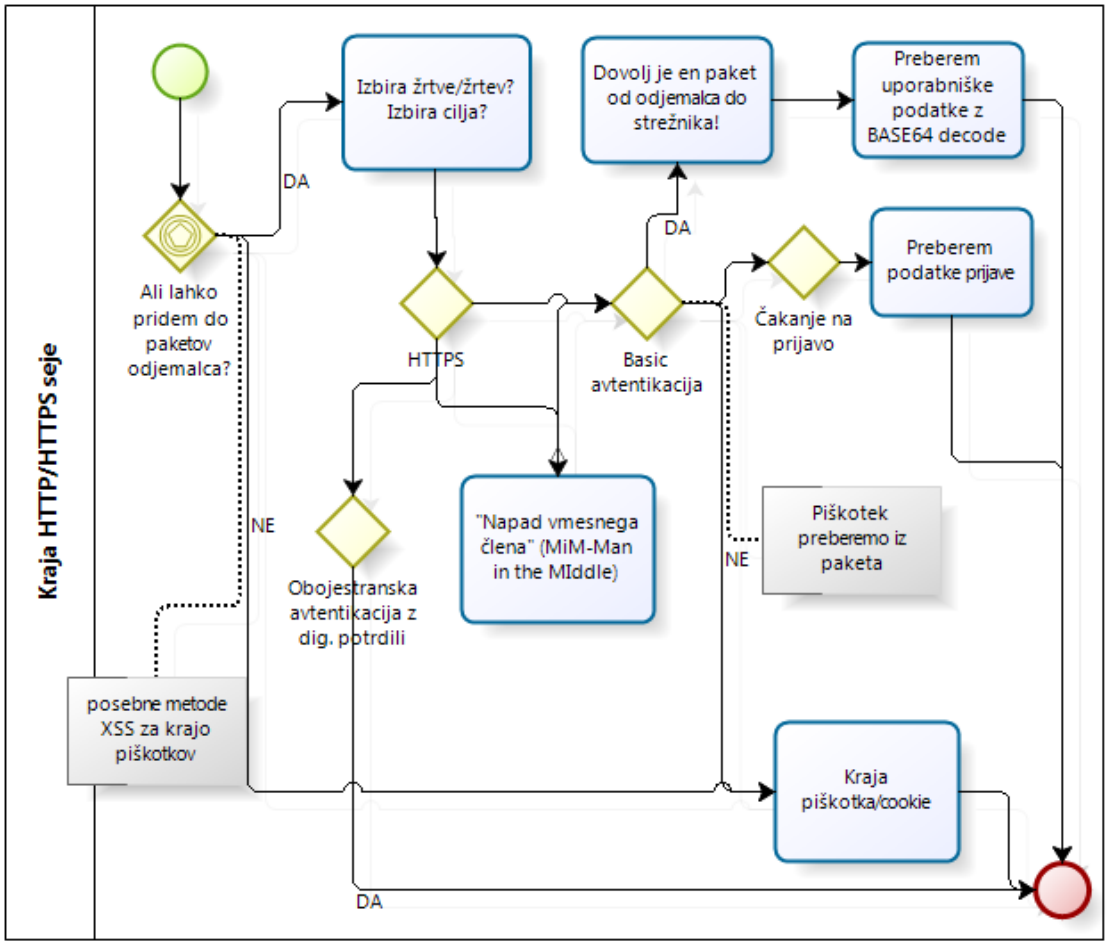




Kako preprečiti krajo RDP seje?

- Zaščita omrežja
  - Uvedba zaščite proti onesnaženju z MAC naslovi na stikalni opremi
  - Uvedba dodatnega varnega tunela
    - IPSEC med odjemalcem in strežnikom
    - SSH tunela med odejmalcem in strežnikom
- Upoštevanje varnostnih priporočil
  - Ne dovoljujejmo oddaljene prijave na strežnike z uporabo Administratorske skupine (Deny Logon Through Terminal Services)
  - Politika gesel
  - Uporaba varnejših metod avtentikacije (enkratna gesla, digitalno potrdilo,biometrična prepoznava)
  - Uporaba varnejših avtentikacijskih protokolov (ukinitev uporabe LM povzetka)

Prikaz kraje spletne seje (npr. spletno bančništvo) XSS



- Ena sam napaka XSS ranljivosti lahko ogrozi celotno aplikacijo ali celo domeno
- http://xssed.com/
- http://xss-proxy.sourceforge.net/
- DOM based XSS:
  - /attachment.cgi?id=&action=foobar#<script>alert(document.cookie)</script>
  - Demo: q.astec.si/domxss.html
- Flash
  - Client Side Authentication (Google Search: filetype:swf inurl:login OR inurl:secure OR inurl:admin)
  - ClickTag: googleSearch → filetype:swf and inurl:ClickTag

astec

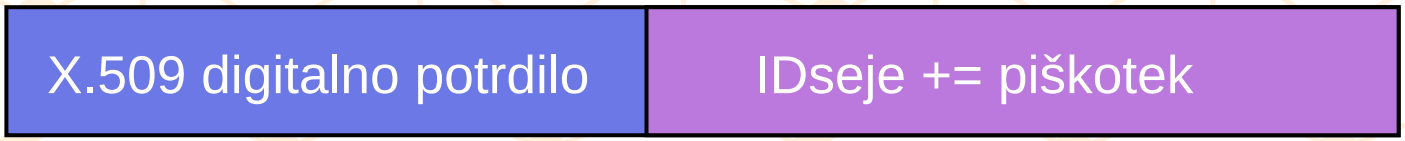
Glavne napake, ki povzročajo XSS ranljivost

- Vhodni podatki se prikažejo na izhodu
  - Brez preverjanja vsebine
  - S preverjanjem, vendar obhod strežniške ali odjemalčeve kode preverjanja
- Napaka programske kode
  - Napaka obravnavanja prejete vsebine,
  - Spreminjanje vsebine na odjemalcu s podatki odjemalca,
  - DOM XSS napad (document.location),
  - XCSS ranljivost (Mozzila binding document),
  - AJAX CSRF,
  - Flash, PDF

SKUPNI CILJ VSEH XSS napadov: Dostop do občutljivih podatkov (največkrat podatkov seje)

Kako preprečiti izrabo XSS ranljivosti?

- XSS ranljivost je znana že od začetka spletnih aplikacij, pa vendar je danes še vedno glavni vzrok kraje podatkov
- Želimo preprečiti krajo seje
- Priporočila
  - Preverjanja vnosa, posebne programske knjižnice, ki preverjajo izstopno vsebino, ...
  - vendar se pojavljajo nove in nove oblike napadov
- Razvijalci morajo zagotoviti povezavo med avtentikacijskim sredstvom in sejo
  - Najbolj uspešna kombinacija: "SSL seja z odjemalčevim X.509 digitalnim potrdilom in kodo, ki pri vsakem dostopu preveri digitalno potdilo in preveri katera seja pripada digitalnemu potrdilu"



SSL – vezava seje na potrdilo

- SSL avtentikacijo odjemalca zavrnemo, če nima potrdila ustreznega CA-ja
- Na vsakem dostopu preverimo veljavnost digitalnega potrdila in če je povezan s pravim piškotkom

```
Session=invalid;
if (X509cert.verify (PublicKey CApubKey) ) {
     select user_id, session_cookie, bankaccount from
   active_sessions where cert_hash=x509cert.hashCode ;

     if (request_cookie == session_cookie)
         Session=valid;
}
if (not Session) {
  log_data (cookie, certificate,...)
  redirect (login_page)
}
```

Novejše metode

- Pass The Hash
  - Vrinemo LSA hash uporabnika v prijavljeni Windows seji in nadaljujemo delo pod novimi uporabniškimi privilegiji (lokalni administrator → domenski administrator)
  - http://oss.coresecurity.com/projects/pshtoolkit.htm

- SandMan: http://sandman.msuiche.net/ (http://www.darknet.org.uk/2008/05/sandman-read-the-windows-hibernation-file/)
  - Prebere windows datoteko hibernacije hiberfil.sys
    - Lahko izluščimo vsebine shranjene v pomnilniku (naredimo izpis vsebine pomnilnika)
    - Orodje pa omogoča tudi obratno: spremeniti vsebino hiberfil.sys

Novejše metode

- BootKit=MBR rootkit
  - Poseben virus, ki okuži MBR; ob zagonu popravi in naloži svojo kodo v Windows "kernel" in pridobi nenadzorovan dostop do celotnega računalnika
  - Zaobide celo enkripcijo diskov
  - Ima vgrajene FAT in NTFS gonilnike
  - Celovito okolje za dodatne vtičnike in zagonske aplikacije
  - http://www.stoned-vienna.com/ (http://www.darknet.org.uk/2009/08/stoned-bootkit-windows-xp-2003-vista-7-mbr-rootkit/)

Kaj je skupen predpogoj vsem prejšnim grožnjam za uspešno izkoriščanje?

- Administrativni dostop do vašega računalnika, ki je lahko omogočen
  - Ker uporabniki opravljajo vsakdanje delo pod uporabnikom z administrativnimi privilegiji
  - Zaradi "luknje" operacijskega sistema
  - Zaradi luknje aplikacije, ki teče pod administrativnimi privilegiji
- Protiukrepi?
  - Račune z administrativnimi privilegiji uporabljajmo le ko je potrebno (dvonivojska prijava)
  - Redne nadgradnje operacijskega sistema in aplikacij s popravki kode

.... nadaljevanje

- SSL NULL-Attack = SSLsniff = SSL MITM Tool
  - Orodje omogoča izvesti napad vmesnega elementa, ki ob preusmeritvi paketov, sprejema odjemalčeve pakete, jih dešifrira in vzpostavi sam SSL sejo s pravim strežnikom
  - Orodje je bilo najprej napisano, da izkoristi napako Microsoft kode, ko ni preverjala, da je podpisnik digitalnega potrdila strežnika, potrdilo končnega subjekta in potrdilo CA-ja
  - Po zaprtju Microsoft "luknje" pa orodje izrablja NULL-prefix napako (NSS, MS Crypto API, GnuTLS knjižnice)
    - www.paypal.com\0.astec.si
    - arpspoof + sslsniff = neopaženo prestrežena SSL seja (brez opozorila odjemalčevega brskalnika)
  - http://www.thoughtcrime.org/software/sslsniff/

V Astecu vam omogočamo "Celovito upravljanje z varnostjo"

Nadzor in protiukrepi
- Spremljanje, Zaznavanje, Ukrepanje (SIEM)
- Tehnične analize
- IDS in A/V
- DLP,....

Preverjanje varnosti (skladnost)
- Zunanji in notranji ISO pregledi
- Varnostni pregled
- Postavitev varnostne ocene (ARAT)
- Izobraževanje

Upravljanje z varnostjo
- Varnostna politika
- Varnostna arhitektura
- Upravljanje s tveganji (ARAT)

Izvedba varnih rešitev
- IDM sistemi
- Varni prehodi
- Varnost končnega odjemalca

Pomoč svetovanja, načrtovanja in ocene
- Analiza tveganja
- Svetovanje pri razvoju
- Načrtovanje varnih aplikacij in varne infrastrukture

Izvedba varnih rešitev
- Požarne pregrade in IPS sistemi
- Varna strežniška infrastruktura
- Varnost omrežja (NAC, 802.1X)

astec

Vprašanja?

marko.smid@astec.si

Kupujmo kvalitetne slovenske storitve.