INFORMATIKA V JAVNI UPRAVI 2015

15. - 16. december 2015
Kongresni center Brdo pri Kranju

Informatika v javni upravi 2015

"Odprimo digitalni potencial javne uprave"

TVEGANJA PRI UPORABI TISKALNIKOV IN VEČFUNKCIJSKIH NAPRAV

Franc Močilar, MZZ
Franci Mulec, MZZ
Samo Maček, GSV

16.12.2015

slovensko društvo informatika

www.iju2015.si

UVOD

Kaj so tiskalniki in multifunkcijske naprave

So:

- kompleksne omrežne naprave,
- dostopne preko lokalnih omrežij, iz interneta, preko WiFi,
- imajo operacijski sistem,
- množico storitev,
- možnost hranjenja podatkov.


© blogs.which.co.uk

Običajno so to spregledane naprave, ki predstavljajo mnoga tveganja za odtekanje podatkov!

TVEGANJA VEČFUNKCIJSKIH NAPRAV

Raziskava - Ponemon Institute The insecurity of Network Printers: Executive Sumary

- 44% organizacij ima te naprave obravnavane v svoji varnostni politiki.
- Več kot polovica zaposlenih te naprave ne prepozna kot tvegane, še najmanj vodilni, tržniki in kadroviki.

Nekaj tveganj:

- lažno predstavljanje (spoofing),
- spreminjanje podatkov (tampering),
- tajitev (repudiation),
- razkritje podatkov (information disclosure),
- preprečevanje storitve (denial of service),
- dvig privilegijev (elevation of privilege),
- nepooblaščen fizični dostop do naprave,
- prestrezanje podatkov.

© null-byte.wonderhowto.com

PRIPOROČILA ZA VARNO NASTAVITEV

- vzdrževana evidenca naprav,
- nastavljena gesla,
- nadzorovan fizični dostop,
- varno sprotno brisanje podatkov,
- redno nameščanje varnostnih popravkov,
- primerne klavzule v najemnih pogodbah,
- vzpostavljeni postopki za servisiranje naprav,
- brisanje in odstranjevanje medijev ob prenehanje uporabe,
- pravilno konfiguriran oddaljen dostop,
- postavitev statičnih IP naslovov,
- nepotrebne komunikacijske protokole je treba onemogočiti, potrebne pa pravilno nastaviti,
- brezžične vmesnike je treba onemogočiti oziroma varno nastaviti,
- če je možno, uporabiti tiskanje ob prisotnosti uporabnika,
- vključimo shranjevanje sistemskih dnevnikov,
- usposabljanje uporabnikov.

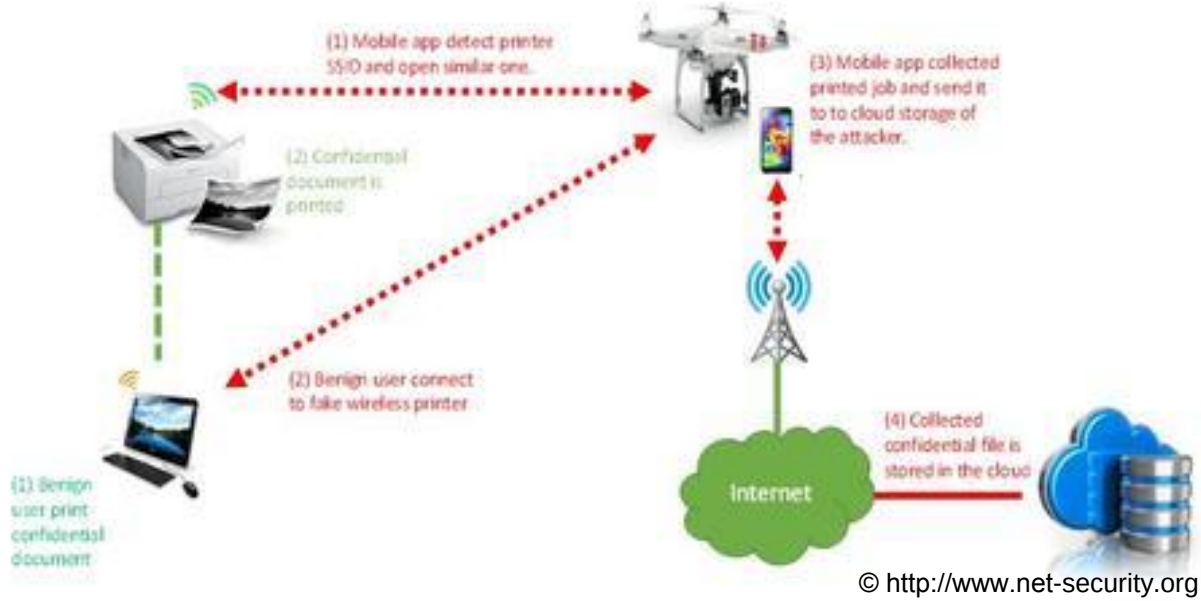
© reprage.com

KONKRETEN PRIMER

- vzpostavitev tovarniških nastavitev (factory reset),
- nastavitev sistemskih gesel, na primer: administrator, User administrator, Machine administrator, Network administrator, File administrator, PJL-geslo, Bootloader geslo, Root geslo, geslo za spletno upravljanje tiskalnika;
- pravilno nastavimo storitve DDNS, Bonjour, WINS,IPP authentication, IPP-tiskanje, LPR, SSH, RSH/RCP, LDAP, DIPRINT, USB, FTP, File transer, SFTP, WS-Device, Ws Printer, IPP, RHPP, IP v6 in vse storitve, Netware, SMB, SNMP ver 1/2/3 »pogojno«, SSDP, RCFG, Telnet, LLMNR, IPPS-tiskanje, LPD, Multicast Ip v4, SLP, WS discovery, TFTP, LexLink, DLC/LLC, Apple Talk, NetBeui, Web Proxy, Ipsec/Firewall, Service Announcement Agent, zunanji dostop do lokalnega diska prek PJL, PML, NFS, CIFS, PostScript oziroma ga zaščitimo z geslom, onemogočimo USB in paralelna vrata, če je to mogoče;
- nastavimo mrežne storitve:
  - TCP/IP naslov in gateway, DNS in proxy ne vpisujemo, določimo 9100 Printing; 802.1x, če ga uporabljamo,
  - nastavitev šifriranja za Web upravljanje, uporabimo lahko HTTPS, ustvarimo in namestimo digitalni certifikat naprave,
  - ravnanje ob napakah, npr. lahko shrani dump ob sistemskih napakah, običajno tega ne potrebujemo,
  - stopnjo nadzora nad upravljalno ploščo tiskalnika (uporabniku omogočimo osnovne funkcije kontrolne plošče),
  - šifriranje diska, če ima naprava disk,
  - odjemalec za elektronsko pošto, če ga potrebujemo, in nastavitev naslova elektronske pošte za pošiljanje sporočil,
  - MAC-filtriranje, če to potrebujemo, običajno pa tega ne vpisujemo,
  - politika zaklepanja gesel,
  - nastavitev sistemskih dnevnikov glede na to, kaj želimo spremljati, in glede na možnosti, ki jih naprava ponuja (logs). Naprave razlikujejo od 5 do 20 različnih vrst dogodkov.

ZAKLJUČEK

- **Naprave je treba obravnavati kot strežnike!**
- **Naprave morajo biti umeščene za požarne pregrade!**
- **Naprave moramo preučiti in za njih skrbeti!**
- **Spremljati ranljivost protokolov in nove grožnje.**
- Pen-testing drone searches for unsecured devices (video) http://www.net-security.org/secworld.php?id=18950



© http://www.net-security.org

Hvala za vašo pozornost !

Vprašanja?

Pripombe?

Predlogi?